JIMMA UNIVERSITY

JIMMA INSTITUTE OF TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS

Performance Enhancement of Channel Aware Based Message Verification Scheme Using Trust and Reputation Model in VANET.

BY

Dagim Asfawu

Advisor: Mr. Kebebew Ababu (Ass.Prof.)

Co-Advisor: Mr. Getamesay Haile (M.Sc.)

THESIS SUBMITTED TO SCHOOL OF COMPUTING OF JIMMA UNIVERSITY IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE DEGREE OF MASTERS OF SCIENCE IN COMPUTER NETWORKING

November 22, 2021

Jimma University

Approval sheet

This Independent Research entitled “***Performance enhancement of channel aware based message verification scheme using trust and reputation model in VANETs***” has been read and approved as meeting the preliminary research requirements of the School of Computing in partial fulfillment for the award of the degree of Master in Computer Networking, Jimma University, and Jimma, Ethiopia.

Principal Investigator: Mr. Dagim Asfawu Sign ________________________________

Mr. Kebebew Ababu (Assist. Professor)
Principal Advisor

Sign________________________________

Mr. Getamesay Haile (MSc.)
Co-Advisor

Sign ________________________________

External Examiner

Name:________________________________

Sign:________________________________

Internal Examiner

Name:________________________________

Sign:________________________________

Chair Person

Name:______________________________________

Sign:___________________________________

Abstract

One of the main goals of vehicular ad hoc networks (VANETs) is to increase road safety and traffic efficiency, by using information that is shared among vehicles in a wide range of Intelligent Transportation Systems (ITS) applications such as crash warning, sudden-brake warning, and lane-change warning. Safety messages are transmitted from each vehicle at a fixed rate such as ten messages per second. In high dense VANET scenario, vehicles have similar motions, that nearby vehicle's BSM gets verification time redundantly due to consecutive broadcasting and then other vehicle's BSM in communication range but distant couldn't get enough verification time.

Each safety message must be verified by a time-consuming cryptographic operation before its information can be reliably utilized. This leads to a problem since the rate that messages are received can be much higher than the verification rate. This problem could be serious with closely occupied roads and when ITS applications require a high transmission rate of safety messages. To solve the raised problem, we proposed a novel trust and reputation model to enhance the performance of the Channel Aware-based message verification scheme in VANETs. For we proposed work the verification time minimizes, that is to skip one BSM without verification process (i.e. one BSM verification processes to take an averagely of 5ms) for the valid vehicles with the help of RSU and increases awareness of the vehicle according to the WAVE standard the result our proposed work trust and reputation model in average 82.28% and when we compare to the existing work of MLPQ-Ch in average 70% within the same distance of 100m. We used some simulation software such as NS3 and SUMO for the produced results.

Keyword: TRM, RSU, SUMO**,** VANETs, WAVE, ITS, basic safety message, nearby vehicles, faraway vehicles, and verification

Dedication

First of all, I dedicate this thesis to the Almighty God, thank you for the guidance, strength, power of the mind, protection, and skill for giving us a healthy life. All of these I offer you.

This study is wholeheartedly dedicated to our beloved parents, who have been our source of inspiration and gave us strength when we thought of giving up, who continually provide their moral, spiritual and emotional.

And Lastly, I dedicate this thesis to our brothers, sister, relatives, mentor, friends, and teachers who shared their words of advice and encouragement to finish this study.

Acknowledgment

First, I would like to thank the almighty GOD, who helped me in every aspect of my life. I am extremely thankful to my main advisor Assistant Prof. Mr. Kebebew Ababu and My co-advisor Mr. Getamesay Haile, whose sincerity and encouragement I will never forget. They have been an inspiration as I hurdled through the path of this Master's degree. Each of the members of my Thesis Committee has provided me with extensive personal and professional guidance and taught me a great deal about both scientific research and life in general. This thesis would not have been possible without the guidance of all teachers and friends. I am thankful for the extraordinary experiences they arranged for me and for providing opportunities for me to grow professionally.

I am grateful for my parents whose constant love and support keep me motivated and confident. My accomplishments and success are because they believed in me. Deepest thanks to my siblings, who keep me grounded, remind me of what is important in life, and are always supportive of my adventures. Finally, I owe my deepest gratitude for all supporting me in my thesis. I am forever thankful for the unconditional love and support throughout the entire thesis process and every day.

By: Dagim Asfawu

List of Figure

List of Table

Acronyms, Abbreviation, and Terminology

AC: Access Categories

AIFS: Arbitration Inter-Frame Spacing

AU: Application Unit

BSM: Basic Safety Message

CALM: Continuous Air-interface Long and Medium range standardization

CCH: Control Channel

CSV: Comma-Separated Values

CW: Contention Window

DSRC: Dedicated Short-Range Communication

ECDSA: Elliptic Curve Digital Signature Algorithm

EDCA: Enhanced Distribution Channel Access

EDR: Event Data Recorder

ETSI: European Telecommunication Standards Institute

EU: European Union

FCC: Federal Communication Commission

FCFS: First Come First Served

FIFO: First-In-First-Out

GNU: GNU's Not Unix

GPS: Global Positioning System

GUI: Graphically User Interface

HRTZ: History Relative Time Zone

IPv6: Internet Protocol version Six

ISO: International Organization for Standardization

ITS: Intelligent Transportation System

IVC: Inter-Vehicle Communication

LLC: Logical Link Control

MAC: Medium Access Control

MANET: Mobile Ad hoc Network

Mbps: Megabits per second

MHZ: MegaHertZ

MLPQ: Multi-level priority queue

MOVE: Mobility model generator for Vehicular networks Environment

NHTSA: National Highway Traffic Safety Administration

NS2: Network simulator Version two

NS3: Network simulator Version three

OBU: On-Broad Unit

OFDM: Orthogonal Frequency Division Multiplexing

PLCP: Physical Layer Convergence Procedure

PMD: Physical Medium Dependent

PSID: Provider Service Identifier

RCP: Resource Command Processor

RSA: Ron Rivest, Adi Shamir, and Leonard Adleman

RSU: Road Side Unit

RTZ: Relative Time Zone

SAE: Society of Automotive Engineers

SAQ: Safety Area Queue

SNAP: Sub-network Access Protocol

SUMO: Simulation of Urban Mobility

TCL: Tool Command Language

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

UI: Unnumbered Information

V2I: Vehicle to Infrastructure

V2V: Vehicle to Vehicle

V2X: Vehicle to Exchange

VANET: Vehicular Ad-hoc Network

WAVE: Wireless Access in Vehicular Environment

WHO: World Health Organization

WSM: WAVE Short Message

WSMP: WAVE Short Message Protocol

XML: extensible markup language

Table of Contents

CHAPTER ONE

INTRODUCTION

1.1 Background

The arrival of VANET in the transportation area is a great step forward. It allows vehicles to instantly send messages to other vehicles or infrastructures. One of the main objectives of VANETs is safety message dissemination which relies on broadcast communication, among vehicles. However, the main challenge in transportation is how to improve road safety. The report in 2018 by World Health Organization (WHO) shows that the road traffic death number globally has reached 1.35 million per year and injured people are 25 to 60 million[1]. Road traffic damages are now the foremost killer of people aged 5-29 years. According to[2], 95% of accidents occurred because of poor or wrong decision-making of drivers. In general, 85% of drivers did not pay attention within a few seconds of an accident.

Experts in the transportation industry have been searching for services to increase safety and provide information to vehicles. To accomplish this goal, ITS have proposed to exchange information among vehicles and infrastructure such kind of network is known as VANETs. Many researchers and companies in different countries like the US and Europe are trying to address challenges in the VANETs environment. In the US and EU, the results of projects are mainly used for standardization bodies in ITS. In the US, the research mainly focused on the protocol suite IEEE 1609 which enables vehicles to communicate wirelessly. In the EU, they are contributing to European Telecommunication Standards Institute (ETSI) ITS, and International Organization for Standardization (ISO) CALM (Continuous Air-interface Long and Medium range) standardization[3].

Every vehicle in VANETs is commonly equipped with necessary sensors such as GPS and compass, a transceiver, and an On-Board Unit that is used for processing and storing necessary information. Another infrastructure of VANETS that is fixed around along the road is called Road Side Units (RSUs). The main function of RSU Vehicles may communicate with other vehicles, directly or indirectly that to create a large-scale network for sharing necessary information. The requirement to share messages about traffic conditions that each receiving vehicle needs to verify the messages to identify whether it‘s from valid or invalid sources. The approach is as follows working principles of signature and verification for the transmitter and receiver vehicles[4] [5] [6]and [7].

Wireless Access in Vehicular Environment is one of the standards that allow vehicles and the infrastructure to communicate and share information wirelessly at a distance of 300 meters [3]. This is mainly to improve awareness in a vehicle about its neighboring vehicles, traffic efficiency, and increase safety, WAVE standard suggests vehicles should broadcast Basic Safety Messages (BSMs) in the above distance range that include vehicles' status (such as position, velocity, heading, etc.) every 100ms or 300ms to the one-hop communication range. Received BSMs to verified, for the safety applications [4][5][6]and [7] and also use the verified information in BSMs to grow traffic efficiency and restrict vehicles from impossible safety problems (incidents) by sending warnings messages to the drivers.

But in highly dense VANETs, a vehicle may receive thousands of BSMs from neighboring vehicles. Due to the message verification process involving a time-consuming cryptographic operation; it makes it impossible for a vehicle to verify all messages[3][8][9][10][11][12][13]and [14]. According to [15][16], it could take at least 4.97ms on average for one message to be verified. So, the BSM receiving rate is usually higher than the verification rate. To cope with this problem, many studies [8],[9],[14] have proposed verification prioritization schemes to selectively verify messages based on their potential relevance to safety applications. The first method can impact safety applications [15] to miss relevant and important information. So the best approach is to develop an algorithm for a vehicle to selectively verify messages based on their potential relevance to the safety applications.

Different papers have been proposed on receiver side safety message prioritization schemes to verify the message based on different approaches. Currently, in [8] [10] [11][12]and [13] there are two main safety message approaches vehicle status-based prioritization schemes and a channel-aware-based prioritization scheme. Existing vehicle status-based prioritization schemes completely rely on mobility information within BSM (i.e. speed, direction, acceleration, headings, etc.). Therefore, it can impact the safety of the end-to-end ITS application, when undeserved priority can be served during zone creation. However, still, the messages within each safety area need to be prioritized to satisfy the demands of the ITS application which recommends that nearby vehicles' BSM need to get verification time before faraway vehicles even within their corresponding zones. To verification delay, increase awareness in the suggested communication range, there is still work to be done.

Mostly, in traffic congestion, vehicles move with similar motion [14], in existing prioritization schemes, always nearby vehicle’s BSM get verified redundantly due to consecutive broadcasting and then those in communication range but distant vehicles couldn’t get enough verification time. This will impact the awareness between vehicles significantly, as the verification delay is still high. According to the WAVE in [1] standard, every vehicle within a distance of 300m communicates with each other. The existing system mentioned above is not enough to fill the WAVE standard. The awareness vehicles measure after their communication with receiving vehicles. To solve the specified problem of the existing scheme, we proposed a novel Performance enhancement of channel aware-based message verification scheme using trust and reputation model in VANETs.

1.2. Statement of Problem

As the WAVE standard [3], discuss each vehicle is recommended to periodically broadcast safety messages to its one-hop neighbors at an interval of 100 ms or 300 ms. The large number of BSM disseminated from the transmitter to receiver vehicles; the small number of safety messages to be verified. For instance, on a dense highway with a broadcast interval of 100 ms and assuming 300 vehicles in its one-hop receiving range (which is reasonable for multi-lane road, counting vehicles in both directions), a receiving vehicle may receive 3,000 safety messages per second.

Nevertheless, confirming an elliptic-curve-based digital signature takes around 4.97 ms on average [14]. Thus, the verification rate is only 500 messages per second, which is much lower than the rate that messages are received [8-14]. To solve this problem, many papers have proposed, verification prioritization schemes to selectively verify messages based on their potential relevance to the safety applications.

Frequently, in high-dense VANET scenarios, vehicles have similar motions [14]. In the case of existing schemes, most of the time, nearby vehicles’ BSM get verification time redundantly due to consecutive broadcasting, and then, unfortunately, other vehicle’s BSM which are in communication range but distant couldn’t get enough verification time. To solve the raised problem, we proposed a novel *trust and reputation model to enhance the performance of the Channel Aware-based message verification scheme in VANETs*.

Our scheme works to use the trust and reputation model counting the list of valid BSM depending on the direct experience of the sender and receiver vehicle to provide recognition of this vehicle is called trusted vehicle. We aim to allow BSM of trusted vehicles to be accepted without verification, with help of RSU based on the trust/reputation value of transmitting vehicles. Hence the faraway vehicle's BSM will get verification time. During that number of verification, delays will be minimized and awareness in communication range will be improved in advance.

Generally, the following research questions are to be answered in this thesis:

- ❖ How to decide the trustworthiness of vehicles to accept its message without verification?
- ❖ How to design an efficient algorithm to decide that count valid BSM transmitting vehicles is trusted?

1.3. Objectives of the Research

1.3.1. General Objective

The general objective of this thesis is to enhance the performance of channel aware-based message verification scheme using trust and reputation model in VANETs.

1.3.2. Specific Objective

To accomplish our general objective, we have the following specific objectives:

- ❖ Investigate and recognize the current safety message verification schemes
- ❖ Design architecture for our new proposed safety message verification scheme
- ❖ Implement the proposed solution in the highway scenario on the simulator VANET environment.
- ❖ Test and Evaluate through simulations the performance of the proposed solution to demonstrate that it enhances the existing system verification scheme
- ❖ Compare and contrast the new scheme with existing schemes.

1.4. Scope and Limitation of the study

The scope of this thesis is delimited on designing based trust and reputation model for receiver side safety message verification for VANET in highway scenarios to enhance the performance of existing prioritization schemes. The proposed solution allows the receiving vehicle to accept the message of the trusted vehicle without verification for a given round based on the trust/reputation value of transmitting vehicles. So that it will improve the vehicle’s awareness in its communication range, and minimize the verification processing delay.

This thesis will not cover the following issues:

- Multi-hop broadcasting issues
- Malicious vehicles detection that denies verifying received message

1.5. Methodology

1.5.1. Literature Review

To achieve the objectives of this thesis various resources that are related to the work such as published international journals, conferences, workshops, articles, books, related websites, and other vital documents are explored to fully understand the VANET system and existing receiver side prioritization safety message verification schemes.

1.5.2. Design and Implementation

In the design phase, proposed solutions in highway scenarios that are specified in the objectives of this thesis are designed. Due to prohibitive costs of employing VANETs, different wireless access technologies, and vehicles in real-world testbeds, we have been implemented the proposed solution using a simulation VANETs environment.

1.5.3. Evaluation of the Proposed Work

The experiment was conducted to test the usefulness of the proposed schemes in the highway scenario and evaluated in terms of their objective and contribution in comparison to what is already done in the simulation environment.

1.6. Significance of the study

VANETs have a lot of potentials for many applications to be developed for ITS. Different types of data are monitored with VANETs applications. For instance, vehicle conditions, surrounding roads, were neighboring vehicles, the surface of the road, and weather. The data is available for different purposes [14]. Based on their purposes, the VANETs applications can be divided into non-safety applications and Safety applications. Non-safety applications provide comfort for road travelers and also make the journey more enjoyable. Some examples are Infotainment, Payment Services, and Traffic/route optimization. Safety applications have the focus on decreasing the probability of traffic accidents and loss of life [15]. Some of the road safety applications which use V2V communication are cooperative forward collision warning, lane change warning, blind-spot warning, and visibility enhancement applications.

Hence, the contribution of this work will improve the BSM waiting time to get verification time and also enhance the awareness of faraway neighboring vehicles. Since WAVEs recommend that for every vehicle, they should broadcast BSM up to 300 meters, we want to also ensure or achieve this (by increasing awareness between vehicles up to 300 meters (300m) as much as possible). So, our goal is to increase awareness between vehicles within their transmission range (300m). Therefore, this satisfies the demands of ITS in VANETs safety applications which suggests in the scenarios of the high-density network not only nearby vehicles but also faraway vehicles of the safety messages need to get verification time.

CHAPTER TWO

LITERATURE REVIEW

2.1. Basic Overview of VANETs

During 1980, the infrastructures of vehicular ad hoc networks change suddenly, in which vehicles connected through wireless communication [22].   Recently, VANETs are used in increasing every traffic safety and driver direction [23]. In VANETs the way of flow diagram that displays the vehicles' communication can be described into V2V and V2I communication, roadside units (RSUs), and onboard units (OBUs). This communication standard that achieved through via wireless technology called WAVE (wireless access in the vehicular environment). The main system components are the application unit (AU), OBU, and RSU.

Generally, the RSU hosts an application that offers services and the OBU is a peer device that uses the services delivered. The application may occupy the RSU or the OBU; the device that hosts the application is called the provider and the device using the application is described as the user. Each vehicle is equipped with an OBU and a set of sensors to collect and process the information then send it on as a message to other vehicles or RSUs through the wireless medium; it also carries a single or multiple AU that uses the applications permitted for the provider using OBU connection capabilities. The RSU can also associate with the Internet or to another server which allows AU's from multiple vehicles to connect to the Internet.

The WAVE architecture describes [24] the communications that ensure the safety of passengers by amending vehicle information and traffic flow. This application guarantees pedestrian and driver safety and also improves the traffic flow and efficiency of the traffic management system. Additionally, TA is responsible for maintaining all components of the VANETs[25]. The several elements of VANETs detail explain below:

I. Roadside Unit (RSU):-

RSU has been considered to support the Vehicle-to-Infrastructure (V2I) communication and to increase the vehicle-to-vehicle (V2V) communication connectivity. It's a computing device that is fixed beside the road. VANET is developing technology for future road applications.

Additionally, it specified locations such as parking areas or at the intersection [26] and was also used to provide local connectivity to the passing vehicles. The RSU contains network devices for dedicated short-range communication (DSRC) based on IEEE 802.11p radio technology.

Generally, RSUs can also be used to communicate between other network devices within the other infrastructure networks [27]. The vehicle connects with the internet through RSU (Road-Side Unit) directly or indirectly. The communication between vehicles and fixed RSUs is used in Intelligent Transportation System (ITS) to allow the vehicle to amend their knowledge about the traffic status.

II. Onboard Unit (OBU):-

OBU is a GPS-based tracking device that is commonly equipped in each vehicle to exchange vehicle information to RSUs and/or other OBUs. OBU contains different electronic components such as resource command processors (RCP), sensor devices, user interface, and read/write storage for recovering storage information. The main important function of OBU is to connect with RSU and other OBUs through the wireless link of IEEE 802.11p [28] and also the responsible for communication with other OBUs or RSUs in the form of messages. In addition, OBU accepts input power from the car battery, and every vehicle contains the sensor type such as; global positioning system (GPS), event data recorder (EDR), and forward and backward sensors which are used to supply input to OBU[29].

III. Application unit (AU):-

The AU is the device equipped within the vehicle that uses the applications provided by the provider using the communication capabilities of the OBU. The AU can be a dedicated device for safety applications or a normal device such as a personal digital assistant (PDA) to run the Internet, the AU can be connected to the OBU through a wired or wireless connection and may reside with the OBU in a single physical unit; the distinction between the AU and the OBU is logical. The AU communicates with the network only via the OBU which takes responsibility for all mobility and networking functions

VANETs are vehicular ad hoc networks that are a collection of a wireless node that forms a fleeting network to communicate between vehicles. The two main component application uses of VANETs are safety and comfort application. The moving vehicles on the roadside are considered as nodes/vehicles and that nodes/vehicles can communicate with each other and also communicate with infrastructure such as RSUs. These vehicles are equipped via wireless devices to connect with the other vehicles during that the vehicle communicates and transfers much useful information. Reliability value is computed by gathering some information like node location, direction, and the velocity of the node. VANETs are different from other wireless networks in the way that they have high transmission power, high computational capability [29].

Vehicular Ad Hoc Networks (VANETs) are made by utilizing the principles of mobile ad hoc networks (MANETs) - the self-generated introduction of a wireless network for data exchange - to the domain of vehicles. They are a key component of intelligent transportation systems (ITS)[29]. The most common types of communications methods in VANETs are:

- ❖ **Vehicle to exchange (V2X):** V2X communications play a crucial role in the ITS to improve traffic efficiency, traffic safety, and driving experiences by providing real-time and highly reliable information such as collision warning, road problem information, traffic over-crowding warning, emergencies, and other transportation services [26]. V2X communication can transfer the information between V2V, V2I, and vehicles to pedestrians (V2P).

- ❖ **Vehicle-to-Vehicle (V2V):** InV2Vcommunication, transmission medium is defined by high transmission rate and short-latency [30]. Its communications architecture provides interaction within vehicles that can broadcast important information such as emergency braking, collision detection, and traffic conditions among each other.

- ❖ **Vehicle-to-Pedestrian (V2P):** It's a communication type in which vehicles share and communicate important information with the footer. It provides the connection between the vehicle and roadside users using the V2V application.
- ❖ **Vehicle-to-Infrastructure (V2I):**-is the infrastructure-based communication. Its communication type in which the information will be broadcast between the nodes (i.e.

vehicle) and the infrastructure to deal with important information such as road conditions and safety events that have been taken into an explanation. In this V2I, a vehicle (node) launches a connection between RSU and contact external networks which is the internet [31]. Figure 1 shows the architecture of communication in VANETs [32].

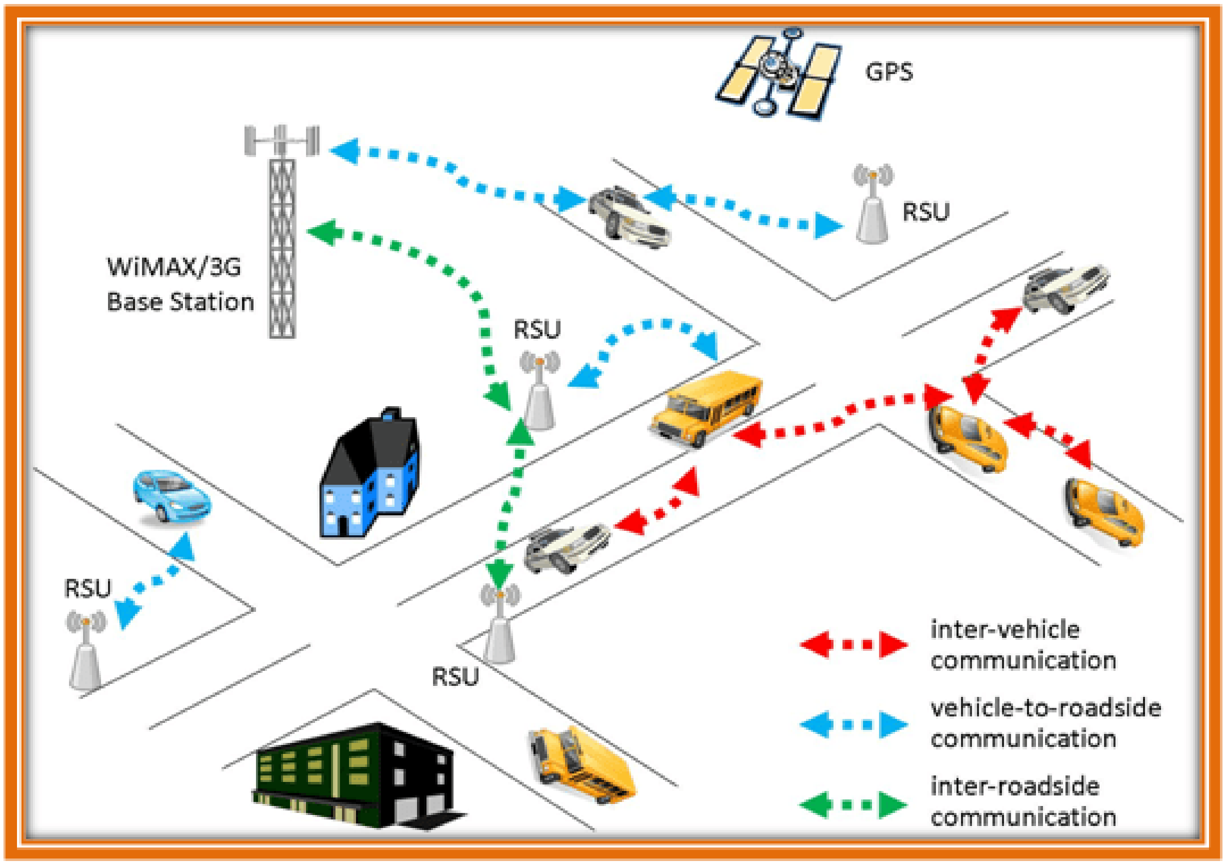

GPS
RSU
WiMAX/3G
Base Station
RSU
RSU
RSU
inter-vehicle communication
vehicle-to-roadside communication
inter-roadside communication

Figure 1:The Communication Architecture in VANETs

VANET Principle and Applications the communication in the VANET is broadly divided into two such as infrastructure-based communication (Vehicle to Infrastructure (V2I) communication) and (ii) direct communication between vehicles (Vehicle to Vehicle (V2V) communication) [29] according to the following Figures 2 VANET communication - infrastructure-based and without infrastructure [29].

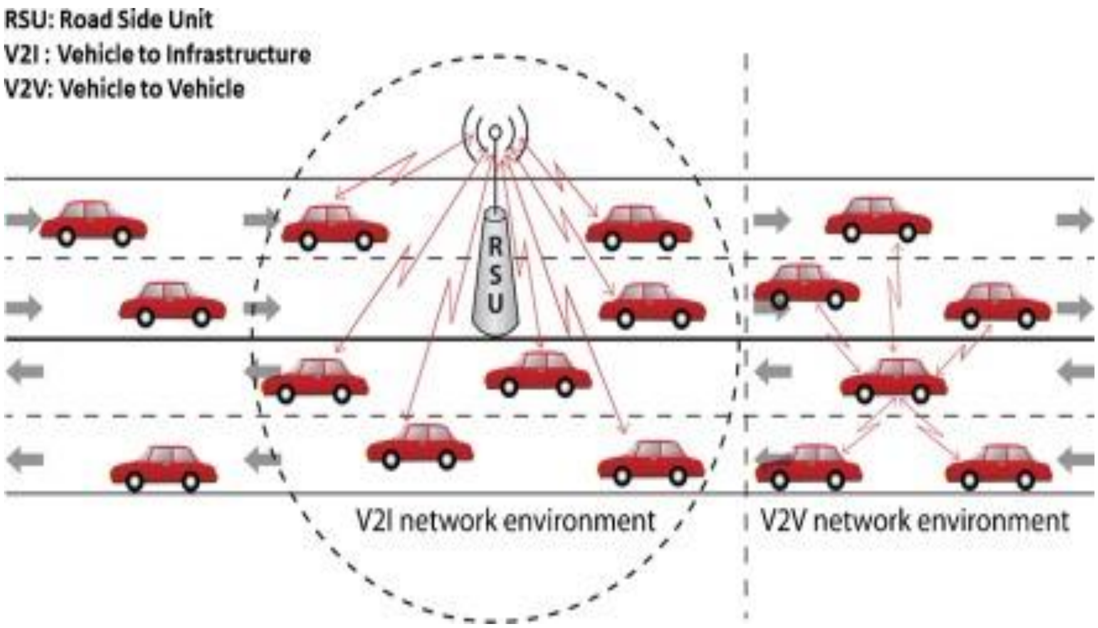


Figure 2:VANET communication - infrastructure-based and without infrastructure

2.2. Characteristics of VANETs

VANET is an application of MANET but it has well-defined characteristics [33]. We will discuss the unique characteristics and advantages of using VANETs over MANETs in terms of the following elements:

- **High Mobility:** The vehicles in VANETs commonly are moving at high speed. This makes challenging to predict a node's position and makes the protection of node privacy [33] quickly change.
- **Network topology:** for the reason of high node mobility and random speed of vehicles, the position of the node changes frequently. As consequence obtains from the network topology in VANETs tends to change frequently. The topology is dynamic and unpredictable. It facilitates the whole network attacks and makes it hard to find misbehavior in the network [12].
- **Frequent exchange of information:** The ad hoc nature of VANET encourage motivates the nodes to gather information from the vehicles and roadside units. Hence the information exchange among nodes becomes frequent [8], [19].
- **Unbounded network size:** VANET can be carried out for one city, several cities, or countries. This means that the network size in VANET is geographically limitless. The

general quality of the being needed this wireless transmission medium is a great advantage in Inter-Vehicle Communication (IVC), becomes the origin of some security issues, related to both the nature of transmission in a wireless environment and to the security of communications using open support [8][12].

- **Limited bandwidth:** In VANET, the standard DSRC set should be measured as restricted, the width of the DSRC band was 27 MHZ. The throughput was 27 Mbps which is a theoretical value [12].
- **Sufficient Energy:** The VANET nodes have no issue with energy and solving problem that involves quantities of resources. This allows VANET utilization of demanding mechanisms such as RSA, ECDSA implementation and also provides unrestricted transmission power [8] [12].
- **Time-critical:** Within the time, the information in VANET should send to the specific node. Therefore, the node will decide and execute action correspondingly [12].
- **Better Physical Protection:** In VANET the vehicle should be well protected physically. Therefore, physically compromising the VANET node will be difficult and it is very difficult to reduce the outcome of infrastructure attack [12] and[20].
- **Limited transmission power:** In the WAVE the transmission power should supply until the data is reached. The data reach-ability distance can be said to be 1000m. For crisis and any public safety such as accident problem or any traffic congestion problem, it is allowed to transmit with a high power [9]and [20].
- **Variable Network Density:** This depends on the density of traffic, which can be low, as in sub-urban traffic, and high during traffic jams [8] and [12].
- **Services of safe driving:** This is motivated by improving traveler gratification and improving traffic efficiency. The direct communications between mobile nodes are ensured by VANETs, hence enabling the usage of a set of applications that require direct communication between vehicles over the network. These applications offer warning information to passengers moving in the same direction concerning the urgency for swift hard breaking or about accidents, thus the driver needs to create a larger image of road topology ahead. Moreover, VANETs can also improve traveler gratification and improve traffic efficiency by providing information such as shopping malls, gas stations, weather, traffic flow, and fast food [9][12] and[19].

2.3. Communication Technology in VANET

Federal Communication Commission (FCC) in US government agency is established for regulation and licensing for 75 MHz spectrum ranges from 5.850 to 5.925 GHz band which is known as Dedicated Short-Range Communications (DSRC) service in ITS. The 75 MHz spectrum defined in Figure 3 Channel diagram of DSRC [34]and [35], is divided into 7 channels of 10 MHz and 5 MHz guard band. This channel (Ch) start from 172 up to 184 all the others are channel service except channel 178. Channel 178 is a managing channel that can help safety power application [36].

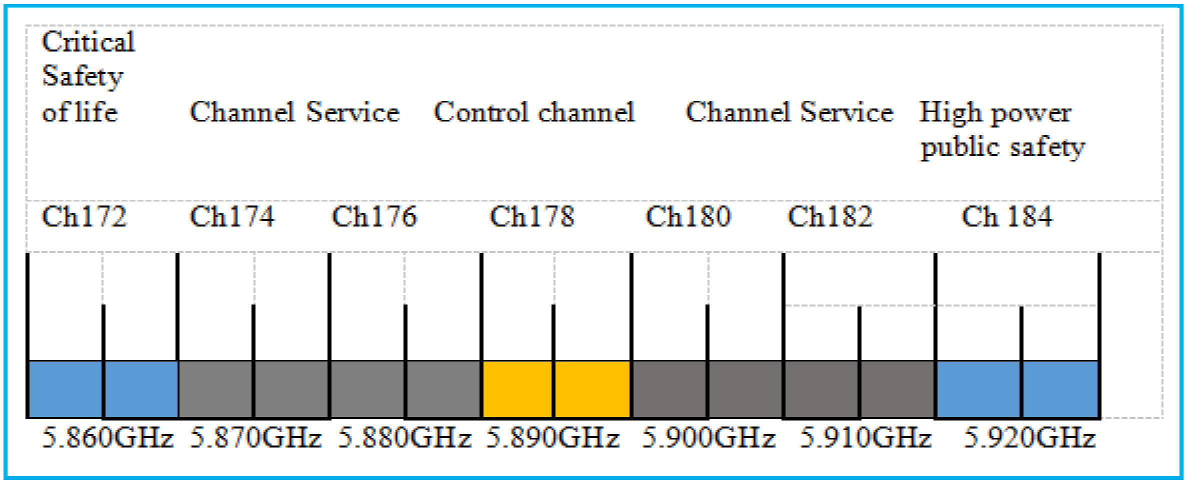


Figure 3:Channel diagram of DSRC

The Wireless Access for Vehicular Environments (WAVE) is the main protocol used to handle communication in VANET. WAVE is based on the Wi-Fi IEEE 802.11 used in Mobile Ad-hoc Networks (MANET) but since VANET is characterized as highly scalable networks with high mobility, new protocols were necessary. It’s the well-known communication standard in the ITS [3]. WAVE makes it possible for vehicles and infrastructures to communicate with each other. The protocol stack that supports the application layer is comprised of the WAVE 1609 standards family [3]. The main reason behind developing this type of standard is to increase safety on road by making possible communication between vehicles and infrastructures.

WAVE standard uses the DSRC frequency band for exchanging information between entities in the VANETs [35]. Since WAVE can offer low latency, wireless communication for safety applications makes it suitable to perform in a dynamic environment. In VANETs, the devices which use WAVE can have two categories: Onboard Units (OBUs) and Road-side Units (RSUs). OBUs are used in mobile stations (vehicles) and RSUs are used as base stations. OBUs and RSUs can communicate directly or indirectly with each other in VANETs. In our thesis, we assume that the architectural components of a VANET (such as On-Board Unit, Road Side Unit, and wireless interface) are Capable of being used with the IEEE 1609 family of standards for WAVE [3]. Figure 4 shows the protocol stack for WAVE in [13]. The main standards in use in the stack protocol of WAVE are summarized as follows:

- **1609.1, Core Systems:** Defines recommendations for the application layer to use the WAVE protocol correctly.
- **1609.2, Security:** Defines the layer that handles security over communication and application in VANETs.
- **IEEE 1609.3, Network Services:** (for network services including the WAVE Short Message Protocol): defines the layer that handles communication stacks and Transport and Network layers.
- **IEEE 1609.4, Channel Management:** Defines the layer that handles multi-channel communications and IEEE 802.11p for wireless MAC and PHY specifications. Indeed, multi-channel is available with two types of channel:

    1. **Control Channel (CCH):** Used for security matters, this channel offers low delay services and aims to transmit security messages to the network.
    2. **Service Channel (SCH):** Used for services such as entertainment or non-safety dedicated communication. Six SCHs can exist in parallel but each SCH

needs the establishment of a communication between vehicles over CCH before being used.

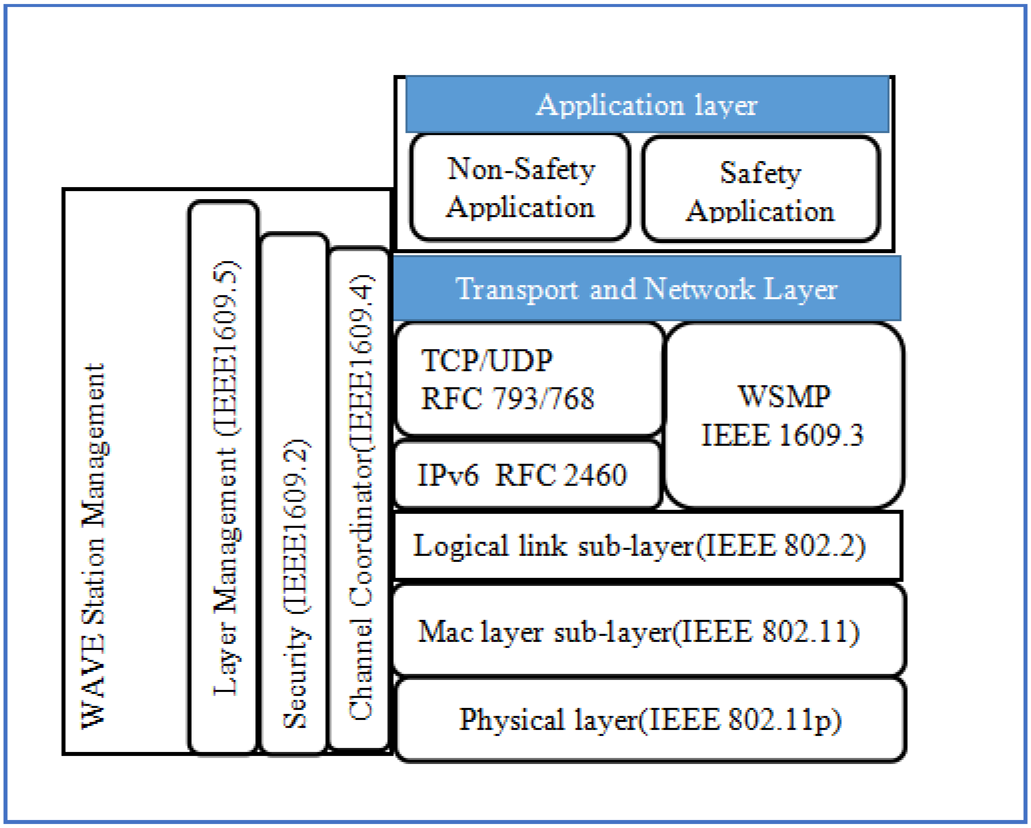

Application layer
Non-Safety Application
Safety Application
Transport and Network Layer
TCP/UDP RFC 793/768
IPv6 RFC 2460
WSMP IEEE 1609.3
Logical link sub-layer(IEEE 802.2)
Mac layer sub-layer(IEEE 802.11)
Physical layer(IEEE 802.11p)
WAVE Station Management
Layer Management (IEEE1609.5)
Security (IEEE1609.2)
Channel Coordinator(IEEE1609.4)

Figure 4:WAVE layouts

As shown in the Figure 4:WAVE layouts, WAVE uses 802.11p at the physical layer [40]. It‘s a modified version of the IEEE 802.11 standard that was divided into two sub-layers: Physical Medium Dependent (PMD) and Physical Layer Convergence Procedure (PLCP). The first one is to utilize the Orthogonal Frequency Division Multiplexing (OFDM) technique and the second one defines the mapping between the MAC frame and the basic physical layer data respectively [41]. IEEE 802.11p can transmit data at high rates from 3 to 27 Mbps in the 10 MHz bandwidth. It has the aim of providing communication between vehicles and infrastructures up to 1000 meters.

In WAVE, the Data Link layer has divided into two sub-layers: Medium Access Control (MAC), and Logical Link Control (LLC). The MAC defines how to access a common medium. MAC layer uses IEEE 802.11e to provide quality of service [36]. IEEE 802.11e uses Enhanced Distribution Channel Access (EDCA) mechanism to provide priority to more crucial services. EDCA is comprised of four separate FIFO buffers called Access Categories (AC) from AC0 to AC3 where AC0 has the highest priority. Therefore, AC0 has access to the channel more compared to other ACs. Figure5: ECDA prioritization mechanisms in WAVE [36] show the four different transmit buffers for each AC. Each AC buffer has a different Contention Window (CW) size and Arbitration Inter-Frame Spacing (AIFS). The smaller AIFS value for AC provides a higher priority chance to access the channel for transmitting the data.

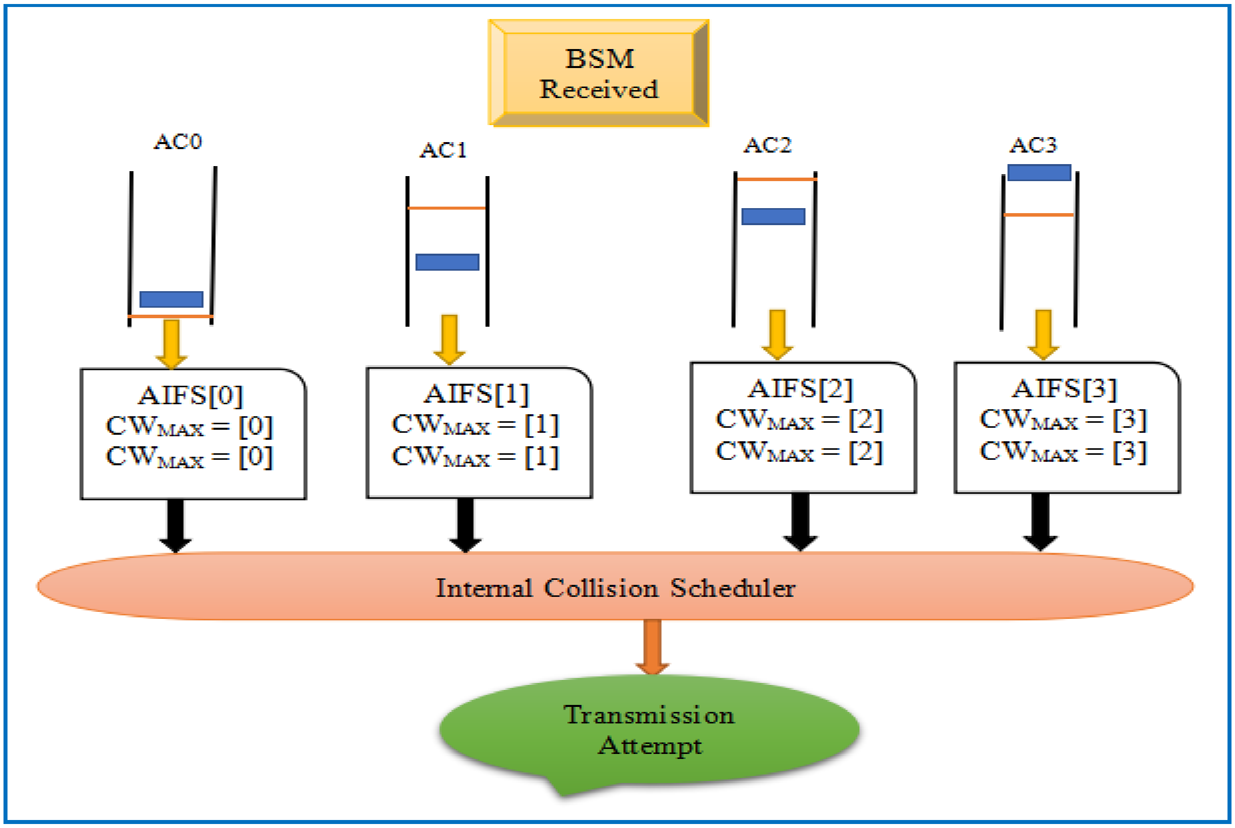

BSM Received
AC0
AC1
AC2
AC3
AIFS[0] CW_MAX = [0] CW_MAX = [0]
AIFS[1] CW_MAX = [1] CW_MAX = [1]
AIFS[2] CW_MAX = [2] CW_MAX = [2]
AIFS[3] CW_MAX = [3] CW_MAX = [3]
Internal Collision Scheduler
Transmission Attempt

Figure 5: ECDA prioritization mechanisms in WAVE

The Logical Link Control (LLC) uses IEEE 802.2 in cooperating with the Sub-network Access Protocol (SNAP) to support IEEE 1609.3 in [37],[38]. They require no-acknowledgment connectionless service with Unnumbered Information (UI) frames. In WAVE, the protocol associated with LLC payload is specified by Ether-Type which has the two known values are 0x88DC (WAVE Short Message Protocol) and 0x86DD (IPv6).

In WAVE, the network and transport layers are found above the LLC layer. They are classified into IP-based and non-IP-based data transmission. The non-IP-based data transmission uses IEEE 1609.3 standard [39] to define and transmit WAVE Short Message (WSM) via WAVE Short Message Protocol (WSMP) were primarily meant for safety applications in VANETs [39]. The IP-based data transfer uses traditional internet protocols, IPv6, UDP, and TCP. Generally, the services depend on their requirements by choosing to use either WSMP or IPv6 service for transmission of data. Most of the time; the overhead of the WSMP packet is 11 bytes less than UDP/IPv6 packets which have a minimum size of 52 bytes [40]. Figure 6 WSM packet formats show the format of WSM consisting of headers 'size and payload [13].

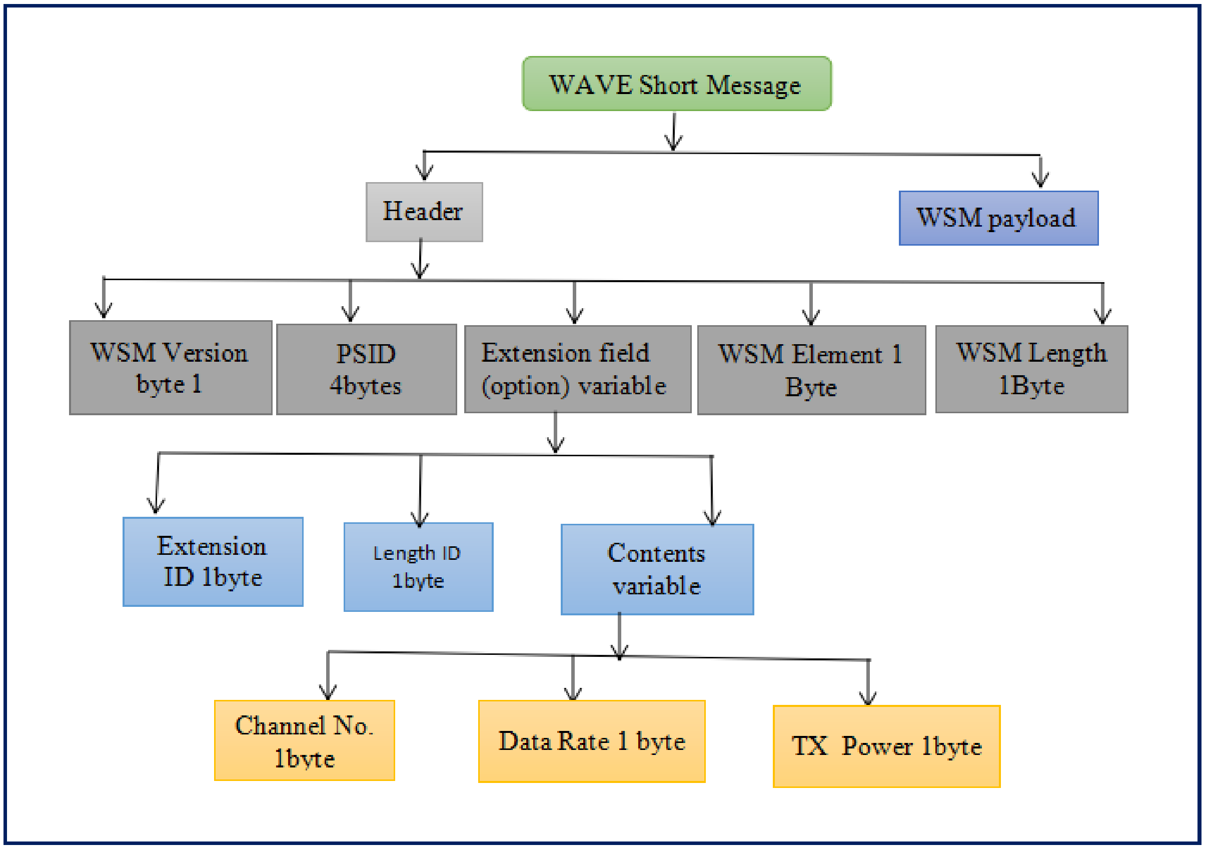


Figure 6:WSM packet formats

As Figure 6 WSM packet formats showed that the header of WSM is 1 byte which indicates the WSM version. WSM uses Provider Service ID (PSID) field with 4 bytes size to identify the applications. It has a similar function with TCP/UDP packet's port number. The Extension field is an optional field of 3 bytes size, which is used for flexibility in communication. WSM element ID indicates payload format and shows the end of Extension fields. WSM length field shows the size of payload which has 2 bytes size. The WSM payload field contains information that comes from the application layer.

In general, an On-Board-Unit (OBU) uses a First-In-First-Out (FIFO) buffer, at the network and transport layer, to handle receiving messages from entities in a VANET. Finally, applications can be classified into two categories at the application layer: non-safety and safety. Non-safety applications refer to those which are used for infotainments and advertisements. Safety applications refer to applications that are used to detect and prevent vehicles from having incidents such as accidents. A common message adjusts used by safety an application is defined by SAE J2735 [41].

2.4. Applications of VANETs

VANETs have a lot of potentials to develop many ITS applications. Protocol stack of VANETs provides applications requirement for vehicular environments and different types of data can be monitored using applications of VANETs. For instance such as traffic conditions, surrounding roads, neighboring vehicles, and weather. The data is available for different aims. The vehicle communicates with its neighboring vehicles to exchange the relevant information [42]. Based on their purposes, the VANETs applications can be divided broadly into two categories. These are non-safety applications and safety applications.

2.4.1. Non-Safety Application:

Non-safety applications refer to applications that provide comfort for road travelers and also make the journey more pleasant. In case of comfort for road traveling, it can refer to traffic efficiency and management applications to improve traffic flow, traffic coordination, and traffic assistance such as speed management, and co-operative navigations applications [43]. The other applications related to infotainment can be local services or global services. The local services which focus on local-based services are the following: Point of interest advertisements, Maps download, Parking payment, and automatic tolling services. The global services which mainly focus on data that can be obtained from the Internet are the following: Insurance, Parking zone management, financial services, web browsing, and Voice over IP [43].

2.4.2. Safety Application:

Safety applications are applications that have the main focus to decrease the probability of traffic accidents and loss of life [42] [43], and [44]. A significant number of accidents happening in the world every year are related to intersections, bind-spot, rear-end, and lane change collisions. Safety applications use information collected by vehicles from their neighboring vehicles to alert a driver to prevent such collisions with other vehicles. Some examples of safety applications are as follows**:**

- **Blindspot warning application:** This application is designed to alert a driver when there is a vehicle at the blind spot when a vehicle wants to change lanes.
- **Visibility enhancement application:** This application is used for alerting a driver when there is an unsafe situation occurring when there is low visibility due to heavy rain, fog, storm, or others.
- **Cooperative forward-collision warning application:** It is an application designed to alert a driver when there is a potential of rear-end collision to the vehicle ahead. In general, the application uses position, velocity, acceleration, heading, and yaw-rate to analyze unsafe situations.
- **Lane change warning application:** This application is used to alert a driver when there is a potential collision for changing lanes. When a driver wants to change lanes and uses a signal for changing lanes, the vehicle uses the information of other vehicles such as position, velocity, acceleration, and heading to analyze the situation such as calculating the gap between vehicles for safe lane changes.
- **Highway merging assistance application:** Alerts a driver when a vehicle at the blind spot or a vehicle is on a highway ramp trying to merge. The vehicle uses the heading, position speed of that vehicle to analyze the situation and alert a driver if there is an unsafe situation. In Table 1 we have summarized the requirements of safety application such as transmission mode, allowable latency, and the maximum range in [43].
- **Cooperative collision warning application:** It alerts a driver when there is a potential accident about to happen. The application uses the collected information of neighboring vehicles such as position, speed, acceleration, wheel angle to analyze them with its sensor information for a potential collision.

- **Pre-crash sensing application:** Far way vehicle becomes active when there is an accident about to happen with a vehicle. This application uses neighboring vehicle information to detect this kind of situation.

Application	Transmission Mode	Allowable Latency (s)	Maximum range (m)
Cooperative forward-collision warning	Periodic	100	150
Lane change warning	Periodic	100	150
Blindspot warning	Periodic	100	150
Highway merge assistance	Periodic	100	250
Visibility enhancement	Periodic	100	300
Cooperative collision warning	Periodic	100	150
Pre-crash sensing	Event-driven	20	50

Table 1:Safety applications and their specific requirements

2.5. Types of Message used for Safety Applications in VANET

SAE J2735 over Dedicated Short Range Communication (DSRC) is a standard for messaging in VANETs [34] and [45]. This standard defines fifteen types of messages used in VANET communications. Basic Safety Message (BSM) is an essential message type used by vehicle-to-vehicle safety applications or cooperative safety driving applications. For the rest of this thesis, a BSM is referred to as a safety message or message. Each safety message has the default size of 254 bytes.

Vehicles usually broadcast safety messages to inform neighbors about their statuses at either 100 milliseconds or 300 milliseconds intervals. During safety message delivery, to avoid delay, there is no acknowledgment or handshaking. They are broadcast to all one-hop neighbors.

According to the WAVE standard, vehicles can communicate up to the range of 1km. The maximum communication range can be used by vehicles for specific purposes such as sending emergency messages or routing messages. The National Highway Traffic Safety Administration (NHTSA) recommends an operational range of up to 300 m for vehicle-to-vehicle communication [46]. Each safety message incorporates information about the status of a vehicle, such as velocity, direction, acceleration, and optional information such as event flags. Periodically broadcasting safety messages by all vehicles permits other vehicles to be aware of nearby vehicles. Retrieved from US Department of Transportation, Washington:

Some safety applications are required to transmit messages periodically (for example, every 100 milliseconds), whereas other safety applications need message transmission when an event occurs [47]. Safety applications examine messages and provide essential action if needed to prevent or warn a driver from about to happen situation. Thus, in general, safety messages can be categorized into two groups. These are periodic messages (messages that are transmitted for awareness of the environment) and the other messages are event-driving messages (event messages which are triggered by unsafe situations).

Periodic Messages: This is an important type of message in safety applications. It is also known as Basic Safety Message (BSM) for V2V communications. Generated BSM is used for neighboring vehicles to have a clear and accurate awareness of potential threats/crashes 360 degrees around the vehicle. Vehicles notify the neighboring vehicles about their existence by transmitting this message. This message contains necessary sensor information of vehicles such as the speed of the vehicles, acceleration, heading, wheel angle. Usually, periodic messages are broadcast in a range of 300 meters radius around a one-hope distance of the vehicle. A vehicle can prevent an unsafe situation by processing these messages before it happens.

Event driving messages: This type of massage is also known as an emergency message. They are transmitted to neighboring vehicles if an incident/unsafe situation has been discovered. Thus, this type of message will not be generated, if there is no incident occurred. Event message has the highest priority for a vehicle to process and usually, it contains location, time, and event type.

2.6. Safety Messages Prioritization schemes in VANETs

According to [15] [16], safety message prioritization approaches can be categorized into transmitter side and receiver side safety message prioritization schemes for verification. Figure 7 BSM prioritization schemes categories show the classification of the two approaches [15]

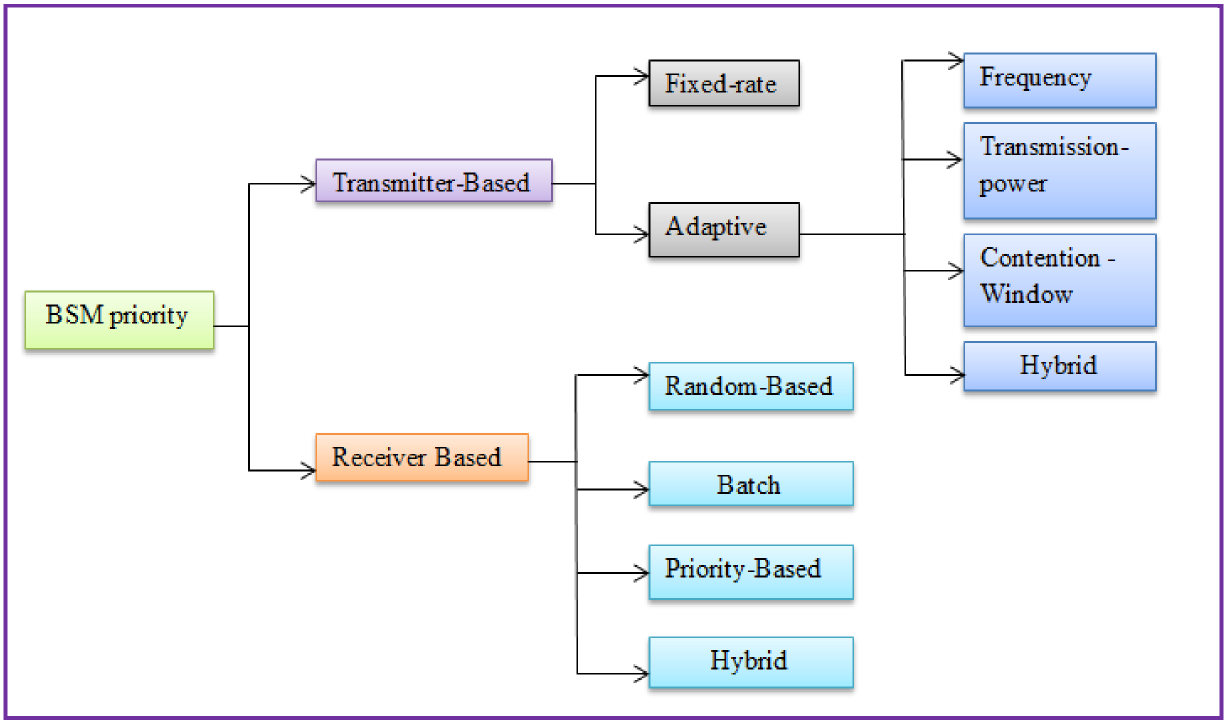


Figure 7:BSM prioritization schemes categories

Let us discuss the advantage and limitations of these two approaches one by one.

2.6.1. Transmitter-side Safety Messages Prioritization schemes

Safety message prioritization at the transmitter-side is performed based on transmission rate, transmission power, contention window size, or a combination of the aforementioned factors.

Fix rate transmission of safety messages: WAVE standard utilize a fixed rate to transmit safety messages in VANET (i.e.10 message/s) [44]. The WAVE protocol [3] gives the quality of service at the MAC layer by following the Enhanced Distributed Channel Access (ECDA) with four separate buffers (AC3, AC2, AC1, and AC0, in descending order of priority) to prioritize transmitting messages. Messages in the buffer with higher priority (i.e. AC3) will have more chances to access the channel. According to the Oldest Packet Drop (OPD) planned the buffering mechanisms at the transmitter to increase the freshness of the messages sent [48]. The OPD strategy is better than the prioritization strategy in the WAVE protocol, in which messages are transmitted in First Come First Serve fashion and new messages are dropped when the transmit buffer is full. However, with this strategy, in very dense traffic, the freshness of messages may be decreased at the receiver due to queuing and processing delays.

Adaptive rate transmission of safety messages: This scheme adjusts the adaptive rate of safety messages transmission based on the condition of the VANET. Paper in [49] proposed to use of clustering vehicles based on their mobility. Each cluster is assigned a cluster head based on its relative speed and distance to cluster members. The cluster head determines the data propagation inside and between clusters. In [50] proposed dynamically adjusting the beacon transmission rate based on current traffic density, Even though keeping appropriate accuracy to increase the performance of VANETs in a high-density traffic condition. The proposed mechanism uses the movement of neighboring vehicles such as velocity and acceleration to estimate the transmission rate of a beacon. However, the drawback of these schemes is that low rate transmission rates may cause inaccuracy in safety applications and reduce the awareness of the vehicle about the status of neighboring vehicles in the vicinity. ·

Safety messages' adaptive transmission power: This scheme adaptively adjusts the range of communication by increasing or decreasing transmitting power. The higher the transmitting power the farther range, a vehicle can broadcast messages. As a result, the lower transmission power can give the closest vehicles higher priority. In [51] proposed a delay-bounded dynamic interactive power control algorithm in which each vehicle iteratively uses a directional antenna to adjust the transmission power for neighboring vehicles [52] focused on increasing the probability that neighboring vehicles receive beacon at the maximum possible range of communication. Their scheme uses piggyback over beacon to share the transmission power control information with neighboring vehicles. In [53] used network topology persistent scheme based on the density of the network to adjust the transmission power with acceptable coverage percentage. However, the drawback of this scheme is reducing transmission power impact on the number of vehicles that can receive the message. This causes a significant reduction in the awareness of neighboring vehicles in the vicinity.

Adaptive contention window size for transmitting safety messages: This scheme adaptively adjusts the contention window size (CW) of MAC in the 802.11p WAVE protocol. As a result, reducing the CW parameter can provide higher priority to the applicable messages for transmitting which causes the reduction in transmission delay for these messages. In contrast, increasing CW provides lower priority to irrelevant messages for transmitting. In[54] proposed to adjust adaptively the parameter in the MAC layer such as CW and network layer to achieve the optimal value for VANET to transmit the message. In [54] used one-hop neighboring vehicles density and many vehicles that were aware of them at a time to estimate the value of CW. But, the drawback of this scheme is that increasing the CW harms transmission delay, and each time the transmission failed the value of CW will be doubled.

Hybrid adaptive transmitting safety messages: This scheme uses a combination of adaptive transmission rate, power, and contention window size for transmitting BSM. In [55] used traffic characteristics such as local vehicle density, traffic flow, and road segment size to determine the transmission range and then calculate the transmission power. The CW size is adaptively adjusted in EDCA to prioritize messages in the AC buffer.

2.6.2. Receiver-based Safety Message Prioritization Schemes

Even though safety message prioritization at transmitters can reduce the message arrival rate at receivers, it does not describe the receiver capability and neighboring vehicles' messages. Thus prioritization of safety messages at a receiver is needed to verify more BSMs from transmitting vehicles in the vicinity which are more likely to be involved in a safety incident. The receiver-based prioritization scheme can be categorized into three schemes: random-based, batch, priority-based schemes.

Random Based verification Scheme: To enhance the security and scalability of the system [9] proposed a verification scheme that chooses messages randomly from the buffer. Although this method has been used in several authentication schemes [19] due to its simplicity, the main drawback of this method is that some important messages may not get verification on time or not be verified at all.

Batch verification Scheme: In this scheme, a receiver collects arrival BSMs as a batch and then verifies them all at once[56]. So, this verification scheme minimizes the verification time per BSM. The disadvantages of this scheme are: i) collecting messages in a batch causes an additional delay for verification and ii) if a single BSM in the batch has a false signature, the batch may not be successfully verified.

Priority Based Verification Scheme: In this mechanism, the vehicle uses mobility information such as velocity, heading, and direction. In the BSMs received from neighboring vehicles to prioritize arrival BSMs in a buffer.

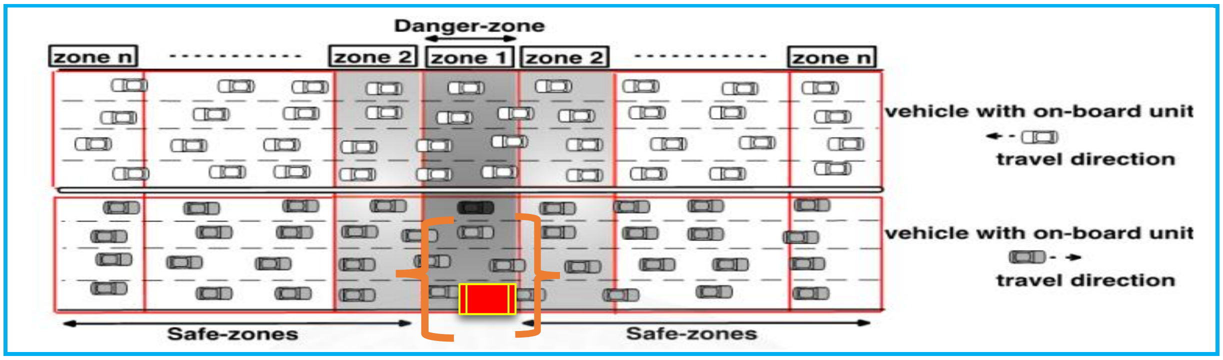
2.7. Broadcasting approaches in VANETs

As stated in the literature [40], and [57] safety message broadcasting approaches in safety application depends on their broadcasting techniques: one-hop broadcasting and multi-hop broadcasting.

2.7.1. One-hop Broadcasting Approaches

Periodically transmitted messages by neighbor vehicles and that are not forwarded to other vehicles used the one-hop broadcasting technique. The standard IEEE 1609.4 is based on the 802.11p update to control multichannel operations at the 5.9 GHz band. It divides the available band, specifically into seven channels of 10 MHz bandwidth. Particularly, there is a Control Channel, two channels used at the end of the frequency band, and four Service Channels ready for safety and non-safety applications [47]. One-hop safety messages used to this standard that generated periodically at the rate of 10 Hz to give the modified information about traffic conditions in VANETs.

Generally, one-hop-based safety messages broadcasting approaches provide local information. Therefore, the requirement of additionally feasible collection algorithms in safety applications that cover a wide area limits their functionality in such scenarios. These procedures increase the computational overhead of the applications, which may delay the detection and notification of dangerous situations, thus making them undesirable in many scenarios. Figure 8: One–hop data disseminating approaches [14].



🟥 =Receiver Vehicle

{ } = Assume transmitter vehicles in the parenthesis

Figure 8:One-hop data broadcasting approaches

The above figure shows that, if vehicles need to exchange data (messages) about their status (i.e. speed, direction, acceleration, etc.), without additional intermediates vehicles, they can accomplish their communication.

2.7.2. Multi-hop Broadcasting Approaches

In this kind of broadcasting approach, when an emergency is detected by a vehicle, the vehicle information to its neighbor vehicle and the message should be re-broadcasted farther to notify the other vehicles that are not in the transmission range of the first vehicle [40], [48], and [57]. Since VANETs are designed to support safety applications, the information is expected to be received by all vehicles.

In VANET, safety message broadcasting is a critical issue to inform vehicles quickly about the accidents that may affect them. Different broadcasting approaches are designed to prevent broadcast storms by choosing certain vehicles from rebroadcasting using different parameters, hence contention in the channel, message redundancy, and collisions are reduced.

- **Flooding:** It is one of the data broadcasting approaches in which vehicles simply rebroadcast when they receive the message. Here if there are k vehicles in the network, they simply rebroadcast for further coverage of messages. When vehicles or RSU receive a message which has to be broadcast, initially they check whether the packet is new. If it is new, they rebroadcast; otherwise, they discard it. Since every vehicle forwards the message, it leads to redundancy. But, the message redundancy depends on the density of the vehicles found in the transmission range.

- **Safety Messages (Beacons):** Safety messages are messages that are periodically broadcasted by every vehicle to exchange information about their status (i.e. direction, speed, and other basic information). These messages have low priority than the alert (event) messages and they are broadcasted in one hope manner to the neighboring vehicles. They are not encouraging rebroadcast by the neighbor nodes.
- **Store and Forward:** In this kind of broadcasting technique, when an alert message is received by a vehicle, the vehicle hold for some time until it gets other vehicles in its transmission range. According to this technique, a vehicle mostly waits to rebroadcast the message until a new neighbor is found. This way is mostly used in sparse network scenarios.
- **Probabilistic approach:** This technique depends on the probabilistic distributions to decide the probability of broadcasting the message, based on the conditions of the transmitting vehicle. Most of the broadcasting approaches that were studied based on this mechanism use the Gaussian (i.e. the uniform distribution to associate a probability) to each vehicle.
- **Distance-based approach:** According to this technique, the message rebroadcasting depends on the distance between the transmitting vehicle and the receiving vehicle. In this broadcasting technique rebroadcasting is not recommended if the distance between them is minimum, to cover large coverage.
- **Counter-based approach:** It is part of the flooding-based data broadcasting technique. According to this, if (counter greater than 5) for a received message, rebroadcasting then not allowed for that message. It is also known as limited flooding. Figure 9 demonstrates the multi-hop data broadcasting technique [40].

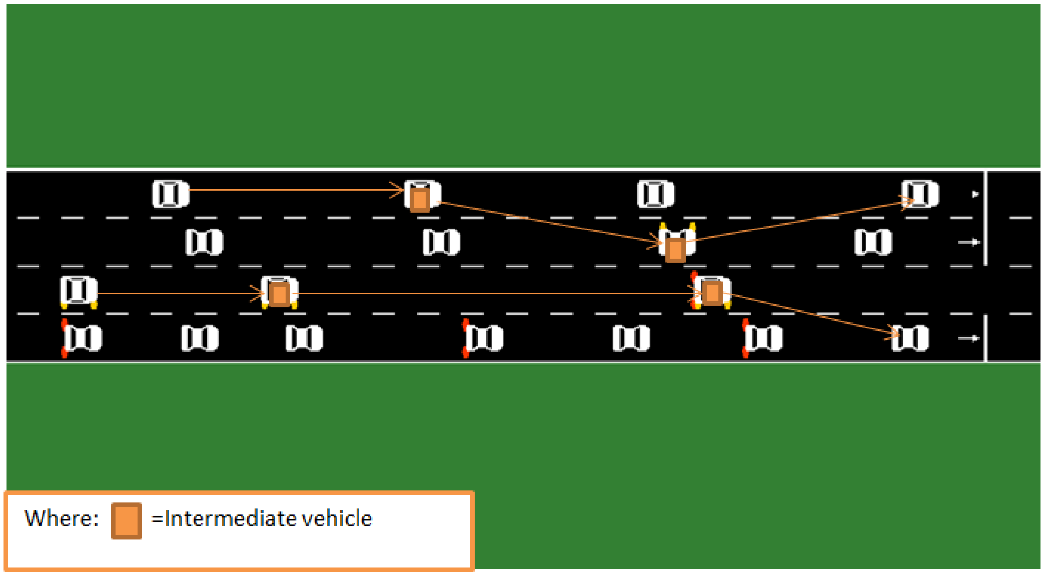


Figure 9:Multi-hop data broadcasting approach

In the above figure, the data is exchanged between source and destination through an intermediate vehicle which is orange colored.

2.8. Challenges in VANETs

As we expressed above, there are a lot of VANET applications in the ITS environment. However, to satisfy the demands of those applications effectively and efficiently, there are many challenges. The main requirements for VANET as explained in [47], [56] are packet loss reduction, bandwidth reservation, packet scheduling, and QoS control. Traditional approaches that are designed for MANET are not efficient and cannot be directly applied for VANET. As a reported survey in [40] and [57] the main challenges in VANET are the following.

- **Applications Heterogeneity:** VANET has various applications of safety and non-safety applications. These safety applications are time-sensitive that need low latency and high reliability while non-safety applications need low packet loss, better throughput, and higher utilization of the resource. Therefore, designing an efficient and effective communication technique that can satisfy the demands of applications requirements is a critical issue in VANET.
- **Frequently Link Disconnections:** As has been expressed above, vehicles have high mobility and travel at higher speeds (for example, over 100 km/hour) unlike nodes in

MANETs. This can result in the frequent change of network topology. Hence, there can be link failure from source to destination [40].

- **Disruptive Communications Tolerant:** At the moment there are problems such as lower reliability delivery and higher delay in low-density networks. To improve the delivery reliability, some solutions utilize the carry-and-forward technique, which in addition increases delivery time (i.e. high delay) of the information. Therefore, designing a mechanism without carrying- and –forward stratagem is needed in VANET.

- **Protocols Standardization:** In VANETs, there can be different kinds of vehicles such as trucks, cars, taxis, motorbikes, bicycles, and buses. In this kind of scenario, it‘s very indispensable that all of these vehicles can communicate with one another through the same protocol. Therefore, the challenging task here is creating a standard.

- **Broadcasting of Information:** Broadcasting emergency or alert information in VANET is a critical problem. The safety information in VANET requires broadcasting, different the other networks like the Internet, where data are typically unicasted [57]. Since safety messages can be broadcasted to many of its neighboring vehicles instead of a single vehicle, to create awareness about an emergency, broadcasting that information using the broadcasting technique is more comfortable than a routing approach which employs a unicasting approach. In the broadcasting technique, a vehicle does not require the address of the destination and the route to a particular destination.

Broadcasting reduces a lot of difficulties in VANET such as route discovery, address resolution, and topology management complexity. Even though this approach is a better option, it can also cause the problem of blind storms in a dense network environment [47]. Therefore, designing a broadcasting technique that is capable of solving those problems is a challenging task.

- **Security Threats:** VANETs may face many challenges in the field of communication security and also in a revolution for vehicular safety and comfort in road transport. In the aforementioned applications, messages can influence driver behavior and consequently road safety.

- Additionally, they can have economic consequences. During the deployment of VANET, it is important to consider the possible existence of adversaries or attackers who try to accomplish the different situations. For example such as injecting false, modifying, or repeating messages, and also impersonating vehicles. Therefore, the security of communications in VANETs is an essential cause in preventing all these threats. In general, in cooperative driving or awareness applications, where each vehicle transmits messages periodically (i.e. in the interval of 100 milliseconds or 300 milliseconds), the validation of the source of the received messages must be confirmed the truth instead of accepting it as it is [15].

- **Safety message arrival-to-verification rate:** Safety message processing or verification plays a significant role in securing VANETs. As safety messages are broadcasted several times per second in a highly dumb network, the message arrival rate can easily exceed the verification rate of safety messages at a vehicle. Therefore, scheming an algorithm for selecting and prioritizing important messages received to increase the awareness of vehicles in the locality is needed [14].

CHAPTER THREE

RELATED WORK

Many schemes have been proposed in the literature to decrease the verification processing time of BSMs [8–10] [14] [17] and [18], and [58]. We discussed above the two common ways of safety message prioritizing schemes for verification in VANET. They are transmitter-side and receiver-side safety message prioritizing schemes. But our research follows the receiver-based schemes. So that, we will focus on existing receiver-side safety message prioritizing schemes.

3.1 Safety Message Prioritization at Receiver

Prioritization of messages at transmitters can decrease message arrival rate at receivers even though, it does neither consider the neighboring vehicles' messages nor the receiver capability. As a consequence, prioritization of safety messages at a receiver is needed to verify more BSMs from the neighbor vehicle. The receiver-based prioritization scheme can be categorized into three schemes such as random, batch, and priority-based signature verification.

The random-based verification schemes select a few BSMs for verification to decrease the congestion at the security queue. Approving only random messages at the transmitter is proposed to decrease the security overhead [58]. Furthermore, random BSMs are selected at an OBU for the verification process to minimize the end-to-end delay. The scheme proposed in [8] uses off-line data given to the central authority to approve and confirm safety messages with a lower security overhead. The disadvantage of these random approves and a verification omission technique is that the authentication of crucial BSMs from nearby vehicles cannot be insured.

The batch-based verification techniques collect together some packets to verify them all at the same time. The protocol introduced in [18] proposes using the mechanism of a binary authentication tree-based batch verification scheme to verify some collection of the BSMs. Another same basic technique to [18] is to produce fake identities based on private keys and bi-linear mapping to assist active batch verification of the safety messages [17]. The drawback of the batch verification techniques is the loss of several packets for the mistake a single batch could not get authenticated.

The priority-based approach is based on the BSMs location information, GPS location, headings, etc. These prioritize the processing of the messages based on their relative closeness with the receiver vehicle. Resource aware verification of BSMs is based on the distance (closeness) between transmitter and receiver [10]. The using metric bloom filter to calculate the importance of the safety messages, [9] uses a priority-based BSM verification mechanism. In conclusion, [14] the priority-based verification of BSMs use separate geographical area into zones by an attractive description of the vehicle mobility. The disadvantage of the priority-based schemes is their dependence on transmitter-receiver closeness which could not be calculated before the packet is authenticated.

In the scheme probabilistic verification proposed in [10], the probability of a message being verified depends on its rank. This depends on distance and a fixed probability threshold to reduce the number of messages to be verified. In this scheme, messages from nearby vehicles to the receiver have a higher probability of being verified than messages from further vehicles. In the key limitation, verification based on probability in a high-density traffic area may cause some received BSMs even from nearby transmitting vehicles to be not verified because of the probabilistic nature.

The scheme prioritizes BSMs based on location and direction proposed in [13] the transmitting vehicle (quadrant), proximity (zones), and relative time, to prioritize applicable received BSMs in a receiving vehicle's buffer. The key design of RTZ uses adaptive discrete zones based on human reaction time and density of network where the received messages from the close zone with lower relative time have a higher chance to be verified. The key limitation complete reliance on mobility information will lead to security issues

To improve RTZ and better the functioning of safety messages verification [13][14], HRTZ is proposed. The key design of the enhanced HRTZ is they added the history of BSM to be stored to avoid duplication of message verification. So that only the most up-to-date message from each vehicle is kept in the receiver‘s buffer.

In the scheme channel-aware, ECDSA signature verification proposed in [12] the high-density VANETs. The approaches to prioritize the verification of BSMs based on the estimated safety areas that are calculated using the received signal strengths. From the ITS safety applications points of aspect, nearby vehicles to received vehicle get the opportunity of the higher safety. So, the BSMs received from the nearest vehicles should be verified in priority; whereas the verification of the BSMs generated by vehicles further away could be delayed. According to schemes [12], used received signal strength of BSM to cluster incoming messages into five fixed safety areas using the K-means clustering algorithm. Then assign BSM according to their safety areas and verify the messages depending on their arrival time. The below Figure 10 shows Multi-level priority queue for channel-aware BSM verification schemes in [12].

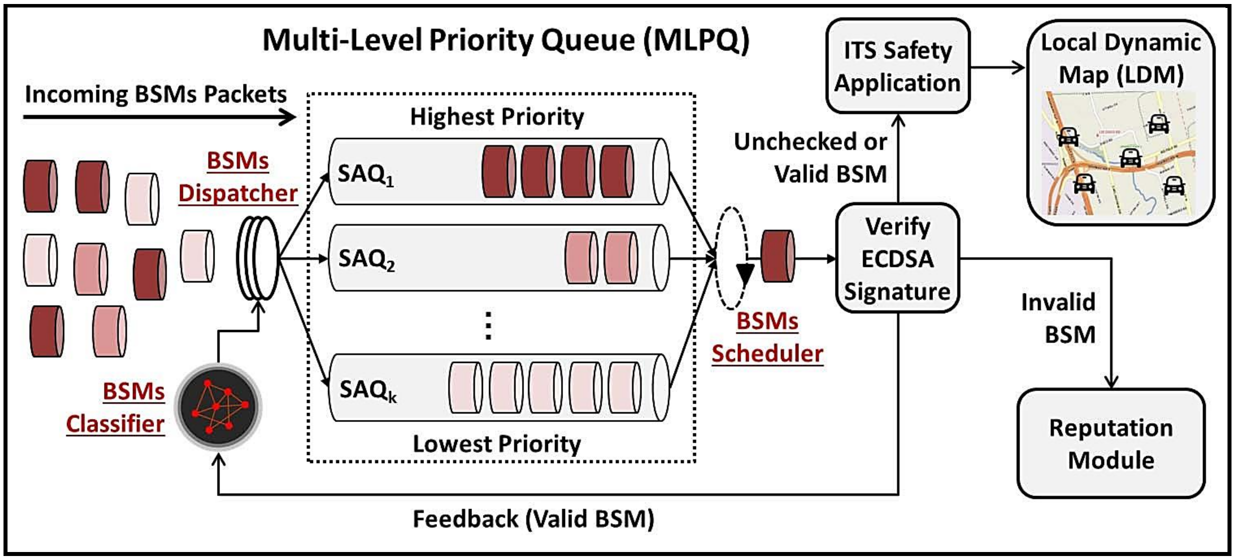


Figure 10:Multi-Level Priority Queue for Channel aware BSM verification scheme.

In the schemes, BSM scheduling for verification the last step BSMs extracted from the MLPQ to be verified by using the First Come First Served (FCFS) scheduling algorithm. The FCFS always checks the highest priority Safety Area Queue (SAQ) which is SAQl (i.e. l = 1) for BSMs stored in the ready queue within their assigned safety areas. If a queue is empty, it will check the immediate lower level queue, until a BSM is found and extracted. In general, however, scheduling techniques do not give priority to messages in the buffer according to the demands of ITS application which recommend that nearby vehicle‘s BSM need to get verification time before far vehicles even within their corresponding safety areas.

Year	Mechanism	Contribution	Limitation
2007	Batch	To produce fake identities from BSM use private key and bi-linear	From several the BSM for the mistake, a single batch couldn't get authenticated.
2010	Probability nature.	The probability of a message being verified depends on it ran. The messages from nearby vehicles to the receiver have a higher probability of being verified than messages from further vehicles.	The verification based on probability in a high-density traffic area may cause some received BSMs even from nearby vehicles cannot be verified
2012	Bloom filter BSM assigned to each rank verified randomly	Resource aware verification of BSMs uses priority-based.	Random verification of BSM in each rank-important BSM not verified
2013	Random	Reduce security overhead at transmitter vehicle.	Verification probability in a high-density traffic area in nature nearby vehicle crucial safety message not insured
2017	K-Means clustering algorithm. FCFS, MLPQ.	The takes into report the received signal strengths and application Dependent safety areas. Enhancement to achieve safety awareness.	According to WAVE standard, every vehicle within transmission range communicate with each other but nearby vehicle gets verification redundantly while distant couldn't enough verification.
2018	location and direction	Discrete zones based on human reaction time and density of the network.	In the density network, the Nearby vehicle drops important BSM for the reason, more wait for the

			buffer to get the opportunity of the verification.
2019	Location, velocity, direction, BSM history	To avoid duplication of message verification from the receiver buffer at a time.	Complete reliance on mobility information lead to security issues

Table 2: Summary of related work

In general, to overcome the specified problems of the existing prioritization scheme, all the papers mentioned above use approaches of nearby vehicle‘s BSM need to get verification than further away vehicle‘s BSM from the received vehicle. However, frequently, in high-dense VANET scenarios, vehicles have similar motions [14]. In the case of existing schemes, most of the time, nearby vehicle's BSM get verification time redundantly due to consecutive broadcasting, and then, unfortunately, other vehicle's BSM which are in communication range but distant couldn't get enough verification time. To improve the awareness between neighboring vehicles and reduce n BSM drop rates, by maximizing the number of BSM accepted by receiving vehicles, we proposed a novel trust and reputation model to enhance the performance of the Channel Aware-based message verification scheme in VANETs.

Our scheme work by classifying vehicles as trusted and untrusted vehicle depending on the direct experience of the sender and receiver vehicle. We aim to allow BSM of trusted vehicles to be accepted without verification, based on the trust/reputation value of transmitting vehicles. Hence those far away vehicles' BSM get verification time and that verification delay minimized and awareness in communication range improved in advance.

CHAPTER FOUR

DESIGN OF THE PROPOSED SOLUTION

As we discussed in chapter one about the problem in highly dense VANETs, a vehicle may receive thousands of BSMs from neighboring vehicles. Due to the message verification process involving a time-consuming cryptographic operation; it makes it impossible for a vehicle to verify all messages. However, still, the messages within each zona need to be prioritized to satisfy the demands of the ITS application which recommends that nearby vehicles' BSM need to get verification time before far vehicles even within their corresponding zones. To reduce verification delays, increase awareness in the suggested communication range, there is still work to be done.

In traffic congestion, vehicles move in similar motion. In existing prioritization schemes, always nearby vehicle's BSM get verified redundantly due to consecutive broadcasting, and then those in communication range but distant couldn't get enough verification time. This will impact the awareness between vehicles significantly, as the verification delay is still high.

In our new proposal, we consider this specific problem of the existing scheme. Regarding this we will achieve based on the ITS safety applications necessitate, vehicles can categorize the geographical region around them into several zones by using channel aware based BSM verification scheme of the BSM received signal strength, within their zone using transmitter-receiver trust and reputation mode direct experience communication.

We are going to design the trust and reputation model to enhance the performance of the Channel Aware-based message verification scheme in VANETs. We aim to allow BSM of trusted vehicles to be accepted without verification, based on the trust/reputation value of transmitting and receiving vehicles. In our proposed solution, we consider those far away vehicles' BSM will get verification time and such that the number of verification delays will be reduced; verification delay will be minimized and awareness in communication range will be improved in advance. Additionally, in our thesis, we have focused on two metrics such as the verification delay, and awareness in the communication transmission range. We will discuss in detail our work concerning the three metrics.

Hence, we have improved from the component of the existing scheme. This component was developed by trust and reputation modal to accept safety messages of faraway vehicles. To improve verification delay, and awareness in communication range, in the scenario of dense network nearby vehicle‘s BSM within their corresponding zones, we proposed the trust and reputation model used to count valid BSMs from the verification module (Verify ECDSA). Thus when counting BSMs verified greater than five, give the feedback to verify the signature of the next BSM jump without verification that depending on the direct experience transmitter and receiver communication before. We are going to introduce the general architecture of our trust and reputation model to enhance the performance of the Channel Aware-based message verification scheme in VANETs.

4.2. The Architecture of the Proposed Solution

In our new system solution, we improve BSM queuing within the zone for a Channel aware-based BSM verification scheme using the verification algorithm that accepts BSMs' trust and reputation model count valid BSMs greater than five depending on the trusted communication of the transmitter and receiver in the high-density network scenarios. The proposed solution‘s architecture shows the flow operations of the proposed work in detail. The operation includes level safety messages according to their assigned zones. Our new trusted and reputation algorithm uses direct experience of the transmitter-receiver communicates to jump one BSM without verification. In our proposed solution, to reduce in the scenario high dense network nearby vehicle‘s BSM communication with the receiving vehicles always get verification time before the farthest vehicles. Therefore, improve the metric of our proposed work in an advanced way than the existing system.

In general, our scheme work to count trusted vehicle depending on the direct experience of the sender and receiver vehicle. Our main objective is allowing BSM of trusted vehicles to be accepted without verification, based on the trust/reputation value of transmitting vehicles. Hence those unverified vehicles’ BSM will get verification time and that verification delay minimized and awareness in communication range improved in advance.

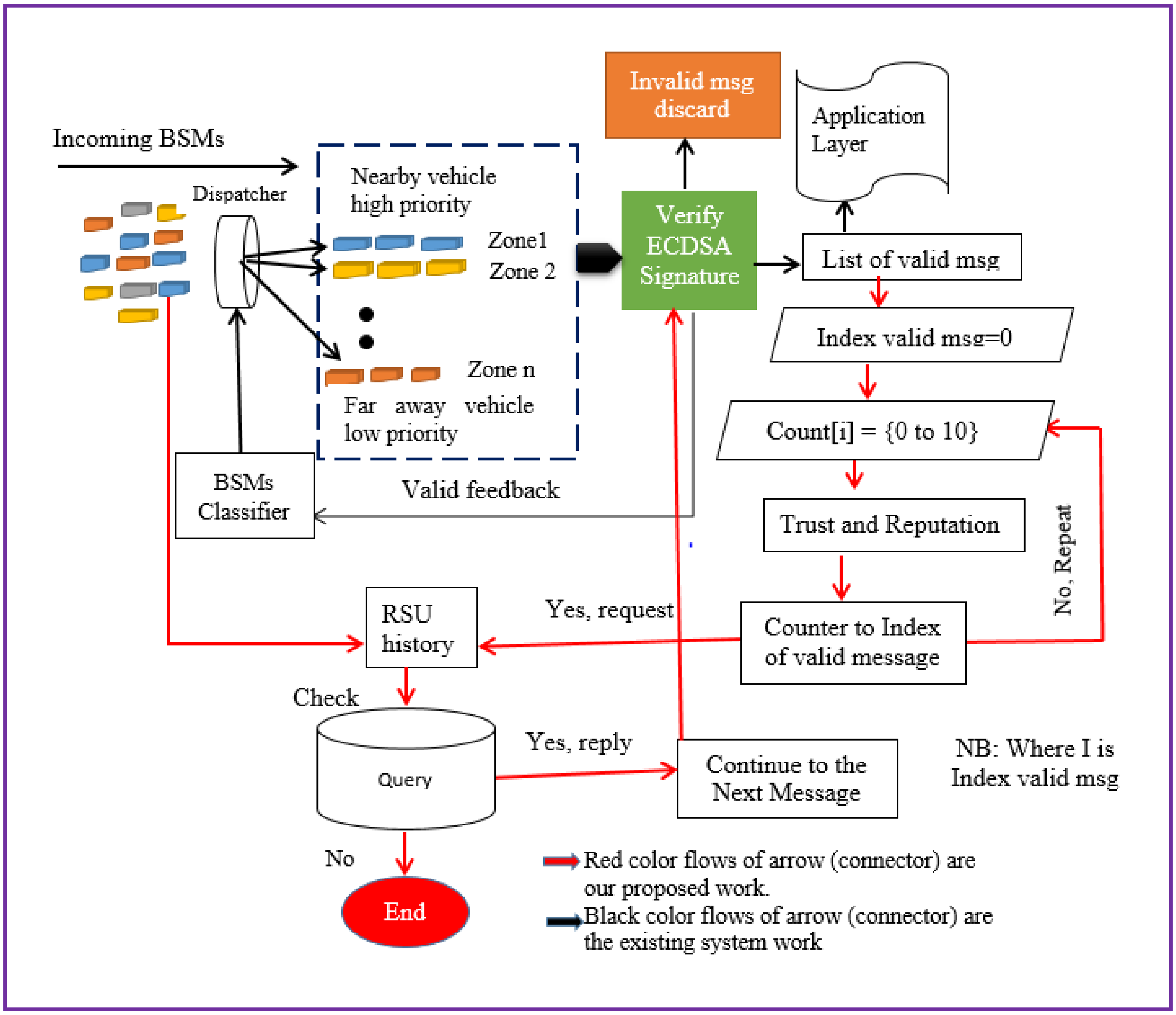

Invalid msg discard
Application Layer
Incoming BSMs
Dispatcher
Nearby vehicle high priority
Zone1
Zone 2
Zone n
Far away vehicle low priority
Verify ECDSA Signature
List of valid msg
Index valid msg=0
Count[i] = {0 to 10}
Trust and Reputation
No, Repeat
Counter to Index of valid message
BSMs Classifier
Valid feedback
RSU history
Yes, request
Check
Query
Yes, reply
Continue to the Next Message
NB: Where I is Index valid msg
No
End
Red color flows of arrow (connector) are our proposed work.
Black color flows of arrow (connector) are the existing system work

Figure 11: Architecture of the proposed solution

According to the proposed solution architecture, we are showing how our BSMs jump (continue to next message) without verification in the highway VANETs system. While our proposed system introduces the standard of the ITS work in VANETs networking system that uses the BSMs to communicate transmitting and receiving in the scenario of the high-density network. We have improved the way verify signature work in the VANETS system.

General Component shows the public information about the whole architecture of the proposed solution in the list below.

- **Incoming Basic safety messages: -** is the message that every transmitter vehicle broadcast within the range of communication in the VANET networking system.

- **Dispatcher: -** is controls the disseminated message from the transmitter and accepted the verified message from the basic safety message classifier. It is a communication that receives and transmits information to coordinate operations of vehicles carrying out a service.
- **Nearby vehicle high priority:-**is the transmitter vehicle closest to receiver vehicle within distance 0 up to50 meters of the first safety area (Zone1) [13] than the other mentioned in standard of WAVE communication range.
- **Far away vehicle low priority:-** is the transmitter vehicle far away to receiver vehicle within distance greater than 50 meters of the safety area (i.e Zone2-5) [13] that is according to the WAVE standard of the communication range (300 meters).
- **Verify ECDSA (**Elliptic Curve Digital Signature Algorithms**):-** it provides network security by engaging a digital signature for messages being transmitted over the network [14].
- **BSMs classifier: -** it's accepted feedback from the verification module and provides the feedback messages for the dispatcher.
- **List of Valid Message: -** is the list of the valid message obtained after the verification module identifies valid and invalid. The system invalid message discard and valid message to store in the list of valid message.
- **Reputation: -** is the direct communication transmitter and receiver that depending on the trust vehicle communication to provide the reputation for one BSM of the transmitter vehicles.

Generally, the old system, nearby vehicles in the scenarios of the dense network get verification redundancy unless within the same zone doesn't get verification that doesn't satisfy the demands of ITS safety application. Therefore, we have replaced that use trusted and reputation model count valid BSMs that greater than five asking the request to RSU history; Real_Id request by trust and reputation modal is equal to the real id RSU history if we get yes then reply display the message for the verify signature jump next BSM. During that unverified BSM get a chance to verification once. So that, this opportunity increases the awareness of unverified BSM one vehicle to get verification (increase awareness of far away from the receiver) and reduce the verification time. In the following subsection, we are going to elaborate on all the components explained above.

4.3. The Proposed BSM prioritization scheme

In our novel proposed system, from the existing system, different prioritization schemes use as input for our proposed work such as:

i. BSM-Classification and
ii. BSM-Ranking
iii. Trust and reputation model

4.3.1 BSM-Classification:

Since the classify BSMs use the approach using K-Means Clustering algorithm separated into five fixed zones with BSM‘s received signal strength, then BSM has been assigned according to zones which have nearby vehicle highest too far away lowest safety area priority queue. The most important clustering of the BSM as it is ordered for the safety of vehicle communicates in the VANETs networking system.

4.3.2. BSM-Ranking:

Another input of our proposed work is that rank basic safety messages within their assigned zones to extract them from the MLPQ module for verification, first, we accept the zones created by BSM-Classifier, then apply the ranking approach on coming BSMs corresponding to their zones. After the process of both BSM classifying and ranking processed their tasks to give according to the arrangement of the priority BSM that to provide for the verify ECDSA. After that, we applied to achieve a trust/reputation model counting the list of valid BSM that help to jump one BSM without verification.

4.3.3. Trust and reputation model

Like the dictionary, meaning trust is safe to believe in the reliability, truth, or ability of something or someone, in another word it is a directional relationship between two parties. Reputation is the belief or opinions that are generally believed about someone or something. When we are coming to our proposed work focus on trust and reputation model, as we introduce to accept the list of valid messages from the verification module (verify ECDSA signature) counting valid BSM depending on the trust communication of the receiver and transmitter in other words (i.e. direct experience of communication between sender and receiver). When we say trust vehicle, in our scenario the BSM verified more than five of the basic safety message get to ensure validity are called trusted vehicle. Since counting valid safety messages greater than five (count>5) reputation decision send the request (such as Is their this real ID?) ask to RSU history replay the feedback to reputation decision yes, then reputation decision the depend on the trusted sender and receiver tells the verification module next 6 BSM jump without verification after that continue to verification until another request get from the reputation model.

In general, our proposed workflow char to design is introduced below in Figure 12.

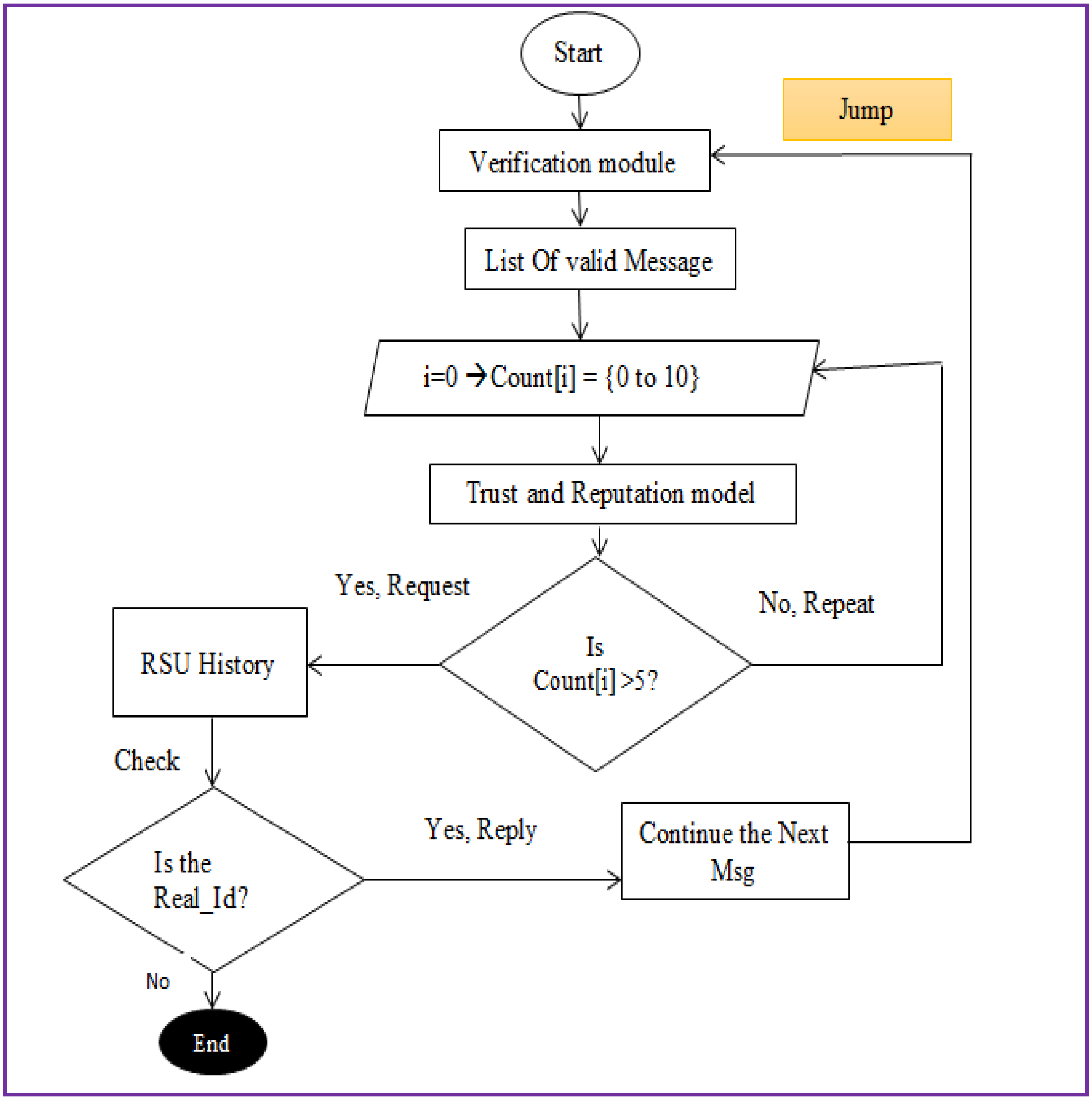


Figure 12: Flowchart of our proposed work

Algorithm: - Our proposed work algorithm

```
1.  Verification module
2.  List of valid message
3.  Procedure (List of ValidBSM)
4.  Begin
5.  For valid BSM  count [i]where i is 0 to 10
6.       Continue to iterate till to get the result
7.        If  count greater than  five
8.             RSU Check Real_Id  list from the old neighbor
9.      Else if get the Real_Id is matched Reply
10.            Display to jump and continue the next message back into step1
11.     End if
12.End for
13.Display stop
14.End Procedure
```

Verification module:- is used to check the validity of the transmitter vehicle at the receiver vehicle when the communication occurs in the highway scenario.

List of valid BSM: - is the collection of valid BSM from the valid vehicle obtained after the verification module.

For valid BSM Count[i]:- each vehicle in one second disseminates ten (10) BSM to the neighbor vehicles. During that use for loop count valid BSM from the valid vehicle using array count index of the valid message (i) that iterate till the value is greater than five (5).

If count greater than Five:- when array count value greater than five the trust and reputation modal send the request to ensure the reality of Real_Id of the valid vehicle that checks in the RSU history.

Else if get the Real_Id:- when the Real_Id request by trust and reputation modal is matched the Real_Id store in the RSU history reply to display the message for the verification module skipping one basic safety message for this valid vehicle Otherwise, end the process.

In general, the algorithm shows the steps for processing the arrival list of valid BSM from a transmitting vehicle at a receiving vehicle. One vehicle transmits in one second 10 (ten) BSM to the receiver vehicle BSM the receiving vehicle determines the trust and reputation scheme depending on the direct communication transmitter and receiver and with help of RSU jumping one BSM without verification.

4.4 Summary

In this chapter Four, we have presented the overall architecture of our enhancing of channel aware based message verification scheme using trust and reputation model that direct communication of sender and receiver to count valid BSMs after verification and jump to the next one basic safety message without verification. Initially, we described how our scheme incorporates the IEEE WAVE standard for safety application. Our scheme is based on IEEE 802.11p physical and MAC layer, which is specifically designed for VANET application. The IEEE 1609.4, used for channel assignment and the basic safety messages supported by the WAVE architecture. In the proposed scheme, we propose algorithms to generate a trust and reputation model scheme that counts a list of valid BSM. Generally, in this Chapter, we present the architecture of the proposed scheme and in the next chapter, we present the implementation.

CHAPTER FIVE

IMPLEMENTATIONS AND RESULT EVALUATION

5.1 Overview:

In the previous Chapters Four, we have revealed that designing enhancement of channel aware based message verification scheme using trust and reputation model in VANETs can solve the problem of verification delay and also improve awareness far away from the vehicle according to the ITS safety applications requirements. Therefore, to achieve this objective we have presented in Chapter 4, the enhancement of the design of channel aware based message verification scheme using trust and reputation model that direct communication of sender and receiver to count valid BSMs after verification and jumping to one basic safety message without verification for the valid vehicle with the help of RSU.

In our proposed solution, we have considered the highway scenario of highly dense VANET environments. Due to the excessive costs of VANET entities and the wireless access network technologies in real-world testbeds, our proposed solution using the trust and reputation model has been implemented and evaluated using a simulator. So, we have used the NS3 simulator to trace safety messages received by each vehicle in the network, within their WAVE standard transmission range. And for the trust and reputation model, we used Jupyter notebook (i.e. python platform). A detailed description of the implementation of our proposed work is presented under sub-sections of this Chapter. Section 5.2 describes the development environment employed to implement the scheme. In section 5.3, Prototype Implementation. Finally, in section 5.4 the simulation experiment and evaluation results are described.

5.2 Development and Simulation Tools

The selection of development environment and simulation tools that were used for the implementation and evaluation of our proposed solution is described below. We have used different simulation tools by assimilating them to implement our proposed solution. For VANETs that are simulator and Python platforms for data analysis (in our case, for trust and reputation model). We use different tools by adapting them to perform our trust and reputation scheme. VANETs simulation requires two types of simulation components those components are: Network and Mobility

5.2.1 Mobility Generators

A mobility generator is a kind of simulator that generates required realistic vehicular mobility traces to be used in the network simulator as input. The comparative studies on VANETs traffic mobility simulators are presented by different articles. One of the mobility generators is SUMO described in [59], which is one of the open-source simulators such as a highly portable, and microscopic road traffic simulation package designed to support different road networks. Their analyses are based on features like freeware, portability, XML-based trace support, GUI support, ease of use, user-defined map, and available as examples. From the different simulators tools in [59], SUMO and VanetMobiSim are recommended as the best choices when supporting all traffic models, and good software features are considered for research work.

Based on this evaluation, SUMO is highly portable, functional across various scenarios, designed for use in traffic strategies and enhancement of route layout. SUMO [60] stands for Simulation of Urban Mobility (SUMO), it is one of the open-source simulators which is a highly portable, microscopic road traffic simulation package designed to support different road networks in VANET. It can be used on most operating systems. Because of high portability and its GNU General public license, SUMO has become more popular and most widely used in vehicular ad hoc networks. It has progressed into a full-featured suite of traffic modeling utilities that uses its formats for traffic demand generation and road networks and routing utilities. MOVE (MObility model generator for Vehicular networks Environment) is also one of the mobility generators which is GNU based mobility generator and also generates the realistic mobility models for VANETs simulations. The main advantages of SUMO are that it is OpenGL GUI based; generates real traffic mobility, is highly portable, open-source, easy simulation set-up, portable libraries, collision-free movement, imports different formats, and a large number of the map defined for better understanding. Therefore, we have selected SUMO as a traffic mobility generator in our proposed work.

5.2.2. Network Simulators

The computer network regularly used for simulation is called a Network Simulator. These simulators are used for simulating the VANETs by determining the performance of network protocols for the mobility nodes. Another important technique is to calculate and create the required components in a network such as the detailed structure of all nodes (vehicles), sending and receiving packets roles, data traffic transmission, channels, etc. The comparative studies on many network simulators are presented by different scholars. In [61] the scholars described and examined network simulators like OPNET, NS-2, GloMoSim, and QualNet. The analyses for network simulators are done based on their features like GUI support, distributed simulation support, scalability, antenna support, and multiple wireless technologies support. Based on this evaluation, OPNET and QualNet have supported all the above-mentioned features though they are not free and do not support the real mobility pattern of vehicles.

However, NS-2 does not support multiple wireless technologies. The evaluations done for network simulators are depending on their features like language support, weaknesses, and strengths. The results of the examinations are almost similar to the general assessment outcomes mentioned in [62].

Another network simulator, NS-3 [63] is a discrete-event network simulator, directed primarily for educational and research use. It is free software, licensed under the GNU GPLv2 license (GNU General Public License version 2), and also publicly available for research, development, and use. The NS-3 project has started in 2006, it is not a backward-compatible extension of NS-2; it is a new simulator. Both simulators are written in C++ but NS-3 is a different simulator that does not support the NS-2 APIs and it allows coding in C++ and Python to simulate a simple and complex networking scenario. NS-2 some models have already been exported to NS-3 and the NS-3 project will continue to maintain NS-2 while NS-3 is being built, and will study transition and integration approaches. Therefore, a survey in [63] showed that NS-3 (Network Simulator version 3) can handle large-scale scenarios, with even 10,000 nodes, and support multiple wireless interfaces in a single node. Furthermore, it is open-source with GNU licensed. Based on our have observed from the comparative studies and analyses presented in [61] [62] [63] SUMO which stands for Simulation of Urban Mobility, is the best choice as a traffic mobility generator that provides a realistic mobility model, functionality in different scenarios and high portability of trace file for VANETs. While from VANETs network simulators, NS-3 is the preferred one regards to supporting multiple wireless interfaces in a single node and is freely available or non-commercial. In general, we have selected NS-3.29 as a network simulator for implementing vehicle communication and storing each vehicle‘s received packets as an input to our trust and reputation model scheme.

5.2.3. Data Processing Tools

As the relative studies have been introduced in [64] on the data processing and analysis platforms use both MATLAB and Python. This studies demonstration that MATLAB is widely known as a high-quality environment for any work that involves arrays, matrices, or linear algebra. Python language is one of the new languages in this area but is becoming increasingly popular for similar tasks. The mature language developed by hundreds of collaborators around the world is called Python. Both of them are interpreted language. This means that their code can be altered between all of the major operating system platforms and CPU architectures out there, with only small changes required for different platforms. According to a survey by [65], an important philosophical difference in the MATLAB and Python comparison is that MATLAB is protected by trademark, closed-source software. Additional the license to use MATLAB is quite expensive. On the other hand, Python is free and open-source software. This is one of the big advantages of Python because anyone can pick up the development of the language. A very popular Python distribution, particularly for math, science, engineering, and data science applications, is the Anaconda distribution. The main reasons for the popularity of Anaconda are:

I. Anaconda distributes pre-built packages for Windows, macOS, and Linux, which means that the installation process is really easy and the same for all three major platforms.

II. Anaconda includes all of the most popular packages for engineering and data science-type workloads in one single installer. Therefore, in our proposed solution, we have used python and its platform like Jupyter Notebook to general broad BSM channel aware based, trust, and reputation model analyzing of received basic safety messages by a particular jump one basic safety message without verification.

5.3. Prototype Implementation

In our proposed work that to generate mobility traces for vehicles by SUMO traffic simulator to model that assume to create Addis Ababa to Adam expressway scenario designed on Net Edit SUMO built-in network editor. A road network of 1km x 1km is used. The vehicle density is set to 200 vehicles per km to create a dense network. For a generation of mobility models, conventional vehicles have been used.

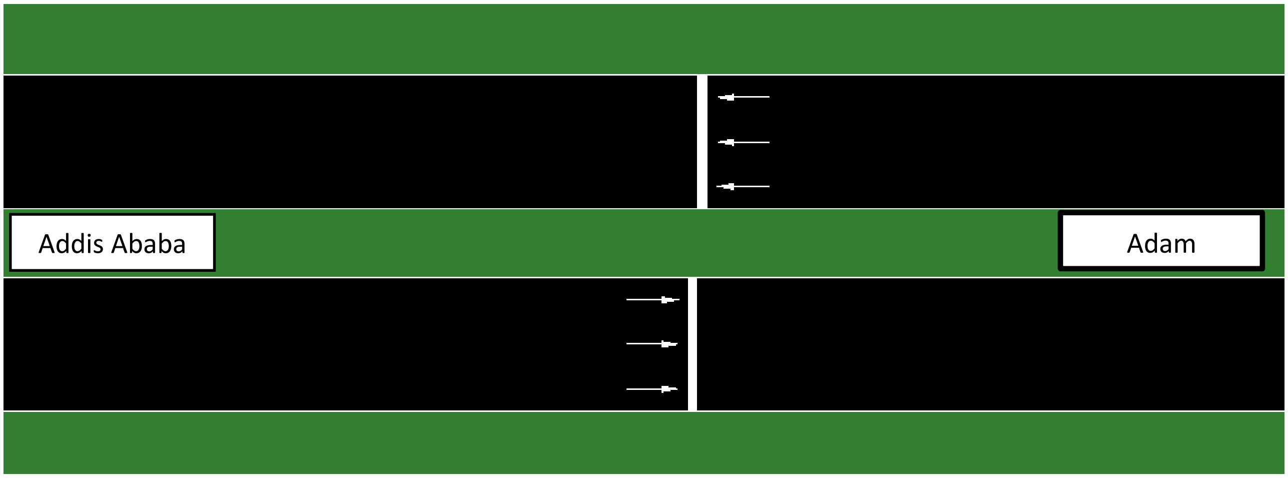


Figure 13: Design of the highway scenario

We consider then, after completion of our design; simulate on sumo-GUI to check the traffic flow on our road scenario. We have summarized the parameters of mobility generation (simulation variable) in Table 3 below.

Parameter		**Value**
Traffic	Type of street	Highway
	Road Area	1km x 1km
	Vehicles number	200perkm^2
	Vehicle Speed	23.6 m/s
	Number of lanes	3 (per direction)
BSM	Simulation time	200 seconds
	BSM interval	100 ms (millisecond)
	BSM lifetime	2 ms
	BSM processing time	5 ms
	BSM size	200 byte
	Data rate	6 Mbps

Table 3: Simulation parameters

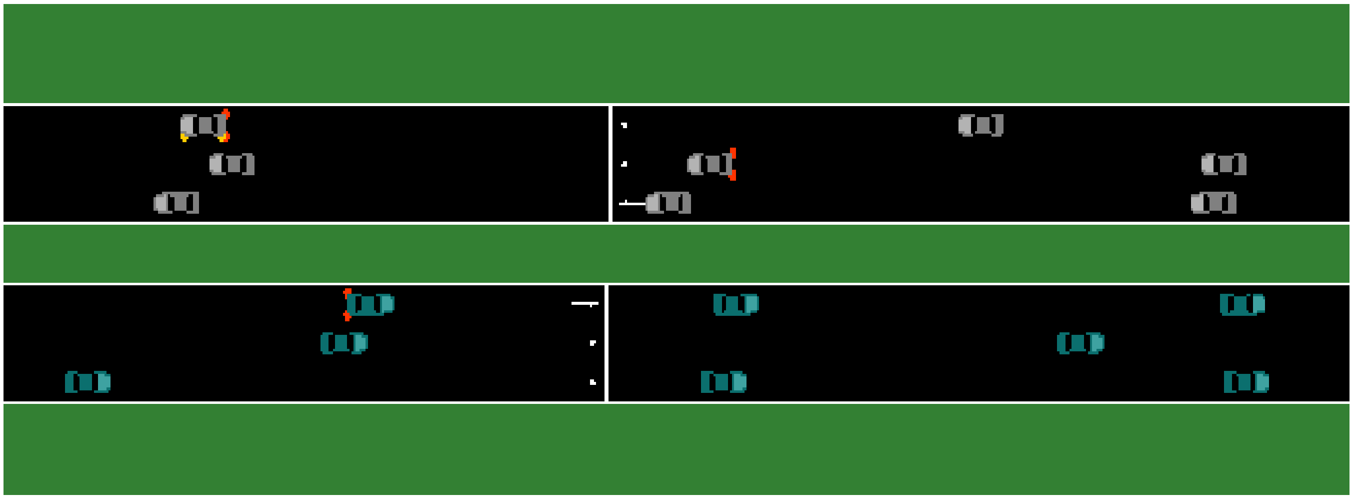
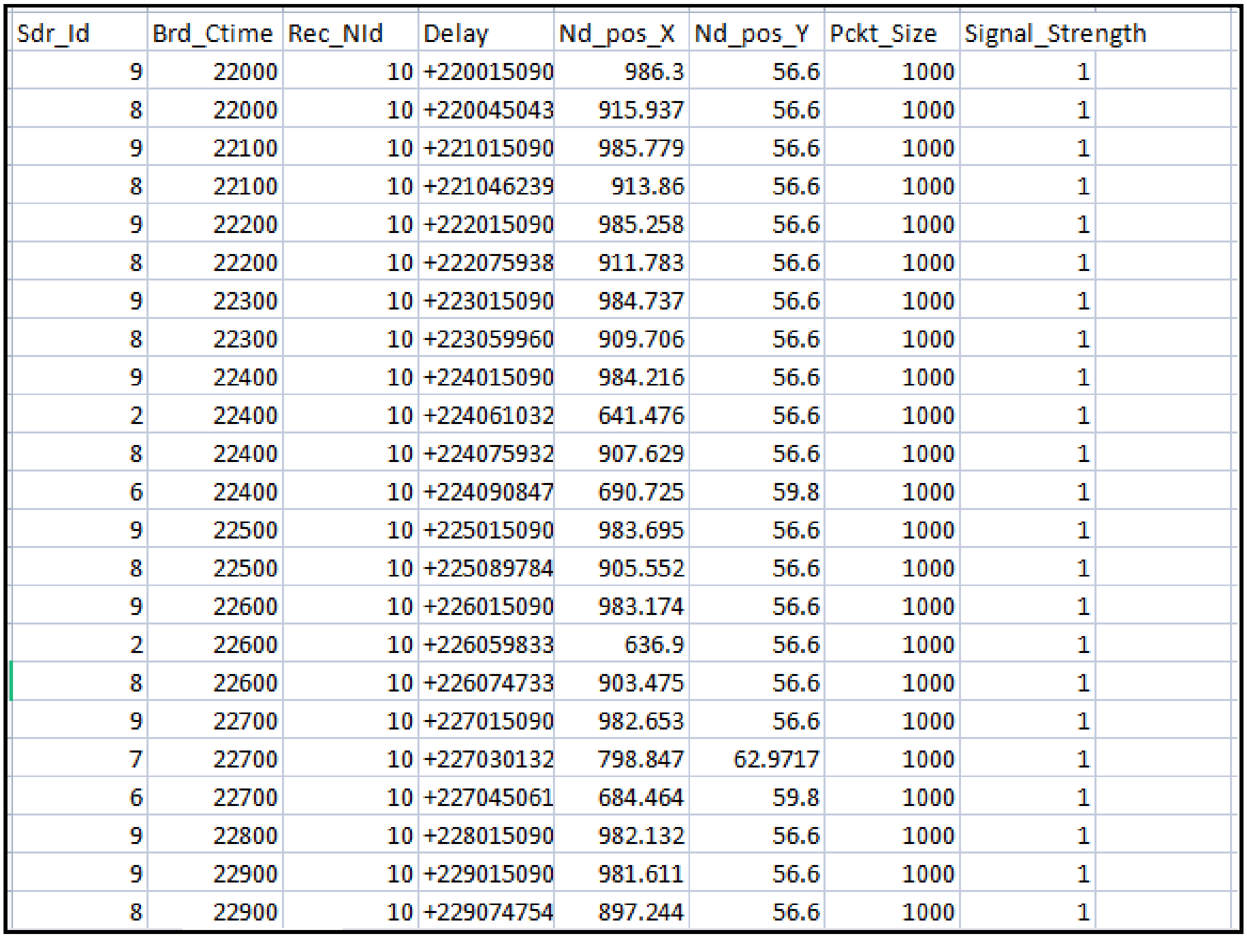


Figure 14: The sample of the traffic mobility model in our expressway scenario

As we introduced in the previous section design flow SUMO simulate in our proposed work that Trace files (.XML files) generated by SUMO can be exported to different network simulators such as NS-3. But, NS-3 is programmed with C++ and Python; therefore, it primarily used .tcl and. py extension files. General, before the actual network configuration of vehicles, we have converted the generated trace file of vehicles mobility model to (.tcl) file which supported by NS-3 network simulator.

In the next step, we are the configuration of the vehicles. We imported the mobility Tcl file to use the generated vehicle's mobility in the NS-3 simulator. Then we proceed to the configuration of WAVE Interface and BSM application on Vehicles. This step is the simulation of vehicle communication on NS-3. Each vehicle has a configured WAVE setup. We used Wave Helper and QosWaveHelper [66] of NS3 helpers are implemented on PHY and MAC layers of vehicles respectively. BSM applications are installed on devices like BSM format and information in the BSM. We have created our NS3 class to extend the built-in application class and program the way nodes broadcast and receive BSM accordingly.

In general, we are using NS-3 simulate in our proposed work is to get the status of the vehicle of the packet trace. Then we have stored the packet (BSM) that received from all transmitter nodes of their neighbor in the transmission range using the extension (.CSV) file. The sample of safety messages received by specific vehicles has been shown in Table 4.



Sdr_Id	Brd_Ctime	Rec_NId	Delay	Nd_pos_X	Nd_pos_Y	Pckt_Size	Signal_Strength
9	22000	10	+220015090	986.3	56.6	1000	1
8	22000	10	+220045043	915.937	56.6	1000	1
9	22100	10	+221015090	985.779	56.6	1000	1
8	22100	10	+221046239	913.86	56.6	1000	1
9	22200	10	+222015090	985.258	56.6	1000	1
8	22200	10	+222075938	911.783	56.6	1000	1
9	22300	10	+223015090	984.737	56.6	1000	1
8	22300	10	+223059960	909.706	56.6	1000	1
9	22400	10	+224015090	984.216	56.6	1000	1
2	22400	10	+224061032	641.476	56.6	1000	1
8	22400	10	+224075932	907.629	56.6	1000	1
6	22400	10	+224090847	690.725	59.8	1000	1
9	22500	10	+225015090	983.695	56.6	1000	1
8	22500	10	+225089784	905.552	56.6	1000	1
9	22600	10	+226015090	983.174	56.6	1000	1
2	22600	10	+226059833	636.9	56.6	1000	1
8	22600	10	+226074733	903.475	56.6	1000	1
9	22700	10	+227015090	982.653	56.6	1000	1
7	22700	10	+227030132	798.847	62.9717	1000	1
6	22700	10	+227045061	684.464	59.8	1000	1
9	22800	10	+228015090	982.132	56.6	1000	1
9	22900	10	+229015090	981.611	56.6	1000	1
8	22900	10	+229074754	897.244	56.6	1000	1

Table 4:CSV file storage

5.4. Simulation Experiment and Result Analysis

To test our scheme we use a simulation experiment according to different parameters. To implement our scheme initially we made a simulation set up to conduct the simulation. After that, we identify and define network parameters. Finally, we analyze and compare our scheme with the existing emergency dissemination schemes.

5.4.1. Simulation Setup

To generate mobility traces for vehicles, we use the SUMO traffic simulator to model a highway scenario. A road network of 1km×1km is used. The vehicle density is set to 200vehicles/km2 to create a dense network. The maximum vehicle speed is taken as 23.6m/s. The WAVE model in NS-3 is used for BSM transmission exchange between vehicles. Each vehicle generates 10 BSMs per second with a transmission range of 300m and 6Mbps of data rate. As we list in the simulation parameter in table 3.

5.4.2. Performance Evaluation Metrics and Results

To evaluate and compare our proposed Performance enhancement of channel aware-based message verification scheme using trust and reputation model in VANETs with MLPQ-CH for verification scheme, we use different metrics. The following metrics are used to study the performance of our scheme with other schemes:

Verification Time Minimize (VTM):- during the communication of the one vehicle in per second broadcast BSMs 10 BSM disseminated. Total Broadcast BSM every vehicle disseminated per second different one BSM.

VTM*=Total Broadcast BSM every vehicle per second – One BSM ------------- (Equation 1)*

Awareness Quality level increase for the far away vehicle (AQL):- the awareness of one vehicle measured when the transmitter vehicles communicate with the receiver vehicles. The total number of Broadcast Basic Safety messages is different from the total number of skipping BSM. For the verification message BSM to get from the total number of Broadcast Basic Safety messages divided by five (i.e. each message for verification use 5 milliseconds). AQL the addition of verification BSMs and jumped BSMs.

Verification BSM = *Total Broadcast BSMs / Five Milliseconds ---------------------- (Equation 2)*

Jumped BSM=*Total number of Broadcast Basic Safety messages – Total* number of skipping BSM -- *(Equation 3)*

AQL= *Verification BSM + Jumped BSM --- (Equation 4)*

5.4.2.1. Verification Time Minimize

Figure 15 shows the increasing probability distribution of the BSM arrival rate in a high-density network condition where each vehicle broadcasts BSMs every 100 ms. In every 100ms each vehicle broadcasts BSMs in a high-density network condition. Subsequently, the verification process of BSM’s signature takes around 4.97≈5ms per message a receiving vehicle can verify 200 messages per second on average. But, the message arrival rate is always greater than 200 messages per second. That means only 20 vehicles got the verification per second. Due to this, the faraway vehicles that disseminate many BSMs do not get verification for suffering the nearby vehicle gets redundantly verification time from the receiver vehicle. But, every vehicle needed to get verification from the receiving vehicle. For this reason, our proposed work uses a trust and reputation model that depends on their direct experience transmitter and receiver communication skipping one BSM without verification for the valid vehicles with help of RSU. During that, we proposed to provide the verification process BSM's 220 message or 22 vehicles got verification per second on average.

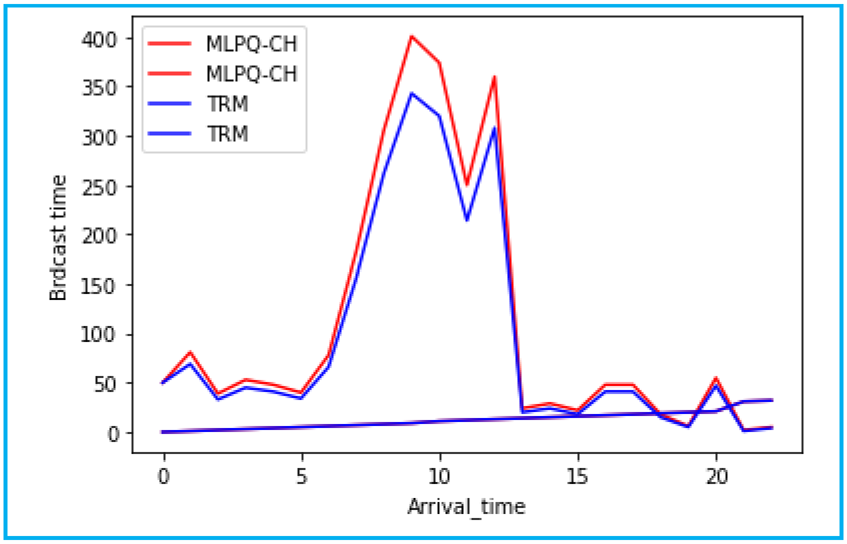


Figure15: comparison of verification time

5.4.2.2 Awareness Quality Level Increase for the far away vehicle

Provides information about how many of the actual neighbors a vehicle is aware of and gives a measure of application reliability. A higher AQL value implies a more reliable cooperative awareness application. We depict the cooperative awareness quality level (AQL) in Figure 16. According to the existing system, MLPQ-CH approaches to computing the AQL for safety areas less than 100m the vehicle awareness level 70%. As the vehicles that are in the closer locality are a higher safety concern, the improved vehicle awareness can improve the QoS of cooperative awareness applications. But the WAVE standard ever vehicle communicate with each other and get the opportunity of the quality of service within the distance 300m. This existing system MLPQ-CH approaches focus only within the distance of fewer than 100m, not enough AQL that as the WAVE standard needed. Due to this, our proposed system using trust and reputation approaches enhanced the AQL by 82.28%. Our approaches allow awareness of every node as the WAVE standard satisfy. Our proposed trust and reputation model approach can enhance the vehicle awareness level (82.28%) in comparison to the existing approaches (70%).

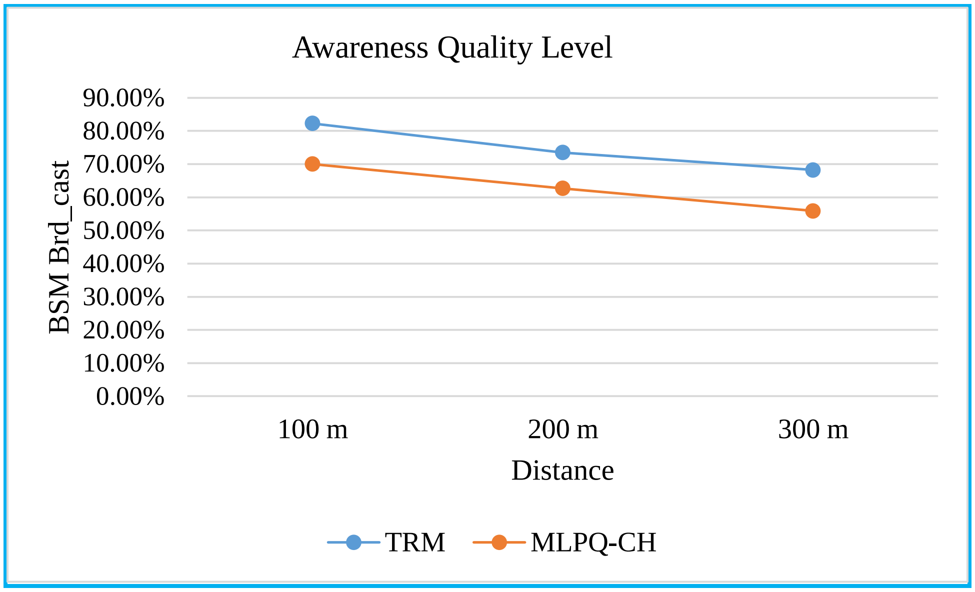


Figure16: Comparison of Awareness quality level

5.5. Summary

Generally, we did test our proposed solution by using SUMO, NS-3, and a Python platform called Jupyter Notebook. After extensive experiments, we analyzed the performance of our propped solution, and finally, we compared our work with the existing BSM prioritization scheme. From the simulation result, we can conclude that our scheme solution has realized better in terms of BSM enhanced verification time verification and awareness quality level. As the objective of our work is to design an enhanced channel-aware-based message verification scheme using the trust and reputation model we are improving the listed above metrics uses, we obtained good results from the simulation.

CHAPTER SIX

CONCLUSION, CONTRIBUTION, AND FUTURE WORKS

6.1. Conclusion

VANET is one type of mobile ad-hoc network designed to solve the problems in ITS applications. The transportation industry has been searching for services to increase safety and provide information to vehicles. VANET system plays a great role in the ITS environment, it can be modified using V2X, V2V, V2I, and hybrid communication. Vehicular Ad hoc Network (VANET) facilitates cooperative awareness applications by periodically sharing basic safety messages (BSMs) with the neighborhood vehicles. VANET has different applications such as safety and non-comfort applications. To broadcasting those applications, VANET needs efficient mechanisms. Safety applications in VANET mainly rely on broadcasting schemes. Those broadcasting schemes can be one-hop or multi-hop schemes. Even though many researchers try to design broadcasting schemes for VANET, still it is a challenging task.

However, a challenging task is that lots of BSMs in nearby vehicles simultaneously get verification than faraway vehicles from the receiving vehicle, especially in a high traffic density. Most of the time, nearby vehicles' BSM get verification time redundantly due to consecutive broadcasting and then other vehicles' BSM which are in communication range but distant couldn't get enough verification time. In addition, as the existing system problem, we have raised verification delay still high, and awareness of faraway don't get enough verification. To solve the raised problem, we proposed a novel trust and reputation model to enhance the performance of the Channel Aware-based message verification scheme in VANETs. We design a trust and reputation scheme depending on the direct experience of the transmitter and receiver communication skipping one basic safety message with the help of RSU that stores the information both sender and receiver information.

Finally, we have tested, evaluated, and proved our proposed scheme with the existing ones. The proposed scheme outperforms all mentioned evaluation metrics on the highway with high traffic density. It provides better performance in the case of BSM, waiting time verification decrease, and improved the awareness accuracy between neighboring vehicles. Thus it can be a good candidate for safety messages prioritization in VANET cooperative awareness application.

6.2. Contribution

The core contribution of our work developing a better performance than the existing system such as reducing verification delay, and More Advanced cooperative awareness applications in VANETs. To accomplish this, we propose performance enhancement of channel-aware-based BSM verification using the trust and reputation model in VANETs.

These are:

- We proposed an algorithm to trust and reputation model that jumps one BSM for the trusted vehicle with the help of RSU.
- RSU deployment: our scheme assumes RSU as a constant node create in our sumo environment that can capable of storing information both the sender and receiver.

6.3. Future works

Our proposed scheme can address the extra receiving safety messages at vehicles in VANETs in high dense traffic environments such as achieving high awareness for neighboring vehicles high rate BSMs and decreasing verification rate. Therefore, it can be a good applicant for skipping one BSM scheme for a trusted vehicle suitable to the cooperative driving safety applications.

Besides, our work can be stretched in different ways.

- A clear deferral of the work could be to extend the algorithm trust and reputation design using the Jupiter notebook integrate into the network simulator.
- Another clear postponement of the work sender broadcast basic safety message for both the receiver and RSU this affect the bandwidth how to increase our proposed work without affect bandwidth and also how to deployment RSU device itself integrate with sumo simulation.

Reference

[1] WHO, "WHO, Global status report on road safety," *https://www.who.int/publications-detail-redirect/9789241565684*, 2018.

[2] D. Mazzola, "Integrated System Approach for Usage Sensitive Service.," *GTE Autom. Electr. Worldw. Commun. J.*, vol. 21, no. 2, pp. 45–50, 1983.

[3] IVTS, "'IEEE guide for wireless access in vehicular environments (WAVE)-architecture,'" *inIEEEStd1609.0-2013, IEEE, New York, NY, USA*, 2014.

[4] DoT, "Vehicle Safety Communications-Applications (VSC-A)," *Final Rep. (DOT HS 811 492A), DOT HS 811 492A*, 2011.

[5] D. O. T. Hs, "Vehicle-to-Vehicle Communications : Readiness of V2V Technology for Application," no. August, 2014.

[6] W. Xu and J. B. Adams, "W dimer diffusion on W(110) and (211) surfaces," *Surf. Sci.*, vol. 339, no. 3, pp. 247–257, 1995, doi: 10.1016/0039-6028(95)00654-0.

[7] C. L. Robinson, L. Caminiti, D. Caveney, and K. Laberteaux, "Efficient coordination and transmission of data for cooperative vehicular safety applications," *VANET - Proc. Third ACM Int. Work. Veh. Ad Hoc Networks*, vol. 2006, no. January, pp. 10–19, 2006, doi: 10.1145/1161064.1161067.

[8] S. Biswas and J. Misic, "A cross-layer approach to privacy-preserving authentication in WAVE-enabled VANETs," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2182–2192, 2013, doi: 10.1109/TVT.2013.2238566.

[9] S. Biswas and J. Misic, "Relevance-based verification of VANET safety messages," *IEEE Int. Conf. Commun.*, pp. 5124–5128, 2012, doi: 10.1109/ICC.2012.6364399.

[10] Z. Li and C. Chigan, "On resource-aware message verification in VANETs," *IEEE Int. Conf. Commun.*, 2010, doi: 10.1109/ICC.2010.5502129.

[11] E. Ben Hamida, M. A. Javed, and W. Znaidi, "Adaptive security provisioning for vehicular safety applications," *Int. J. Space-Based Situated Comput.*, vol. 7, no. 1, p. 16, 2017, doi: 10.1504/ijssc.2017.084120.

[12] E. Ben Hamida and M. A. Javed, “Channel-aware ECDSA signature verification of basic safety messages with K-means clustering in VANETs,” *Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, vol. 2016-May, pp. 603–610, 2016, doi: 10.1109/AINA.2016.51.

[13] S. Banani, S. Gordon, S. Thiemjarus, and S. Kittipiyakul, “Verifying safety messages using relative-time and zone priority in vehicular ad hoc networks,” *Sensors (Switzerland)*, vol. 18, no. 4, pp. 1–21, 2018, doi: 10.3390/s18041195.

[14] S. Banani, S. Kittipiyakul, S. Thiemjarus, and S. Gordon, “Safety Message Verification Using History-Based Relative-Time Zone Priority Scheme,” *J. Comput. Networks Commun.*, vol. 2019, 2019, doi: 10.1155/2019/8568912.

[15] J. Petit, “Analysis of ECDSA authentication processing in VANETs,” *3rd Int. Conf. New Technol. Mobil. Secur. NTMS 2009*, pp. 3–7, 2009, doi: 10.1109/NTMS.2009.5384696.

[16] J. Petit and Z. Mammeri, “Authentication and consensus overhead in vehicular ad hoc networks,” *Telecommun. Syst.*, vol. 52, no. 4, pp. 2699–2712, 2013, doi: 10.1007/s11235-011-9589-y.

[17] S. Vinothini and T. Subha, “An efficient CRL authentication scheme for vehicular communications,” *Proc. Int. Conf. Comput. Commun. Technol. ICCCT 2015*, vol. 57, no. 6, pp. 282–285, 2015, doi: 10.1109/ICCCT2.2015.7292761.

[18] Y. Jiang, M. Shi, X. Shen, and C. Lin, “BAT: A robust signature scheme for vehicular networks using Binary Authentication Tree,” *IEEE Trans. Wirel. Commun.*, vol. 8, no. 4, pp. 1974–1983, 2009, doi: 10.1109/T-WC.2008.080280.

[19] J. H. Cheon and J. H. Yi, “Fast batch verification of multiple signatures,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 4450 LNCS, no. 1, pp. 442–457, 2007, doi: 10.1007/978-3-540-71677-8_29.

[20] Z. S. Khan, A. Alaraj, S. N. Rekha, F. Azam, and M. Zubair, “Weighted Priority Based Signatures’ Batch Verification Scheme in Vehicular Ad-Hoc Networks,” *Lect. Notes Eng. Comput. Sci.*, vol. 2228, pp. 614–618, 2017.

[21] J. Guo, J. P. Baugh, and S. Wang, “A group signature based secure and privacy-preserving vehicular communication framework,” *2007 Mob. Netw. Veh. Environ. MOVE*, pp. 103–

108, 2007, doi: 10.1109/MOVE.2007.4300813.

[22] X. Liang, T. Yan, J. Lee, and G. Wang, “A Distributed Intersection Management Protocol for Safety, Efficiency, and Driver’s Comfort,” *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1924–1935, 2018, doi: 10.1109/JIOT.2018.2817459.

[23] T. Neudecker, N. An, O. K. Tonguz, T. Gaugel, and J. Mittag, “Feasibility of virtual traffic lights in non-line-of-sight environments,” *VANET’12 - Proc. 9th ACM Int. Work. Veh. Inter-NETworking, Syst. Appl.*, pp. 103–105, 2012, doi: 10.1145/2307888.2307907.

[24] M. N. Mejri, J. Ben-Othman, and M. Hamdi, “Survey on VANET security challenges and possible cryptographic solutions,” *Veh. Commun.*, vol. 1, no. 2, pp. 53–66, 2014, doi: 10.1016/j.vehcom.2014.05.001.

[25] M. Azees, P. Vijayakumar, and L. J. Deborah, “Comprehensive survey on security services in vehicular ad-hoc networks,” *IET Intell. Transp. Syst.*, vol. 10, no. 6, pp. 379–388, 2016, doi: 10.1049/iet-its.2015.0072.

[26] X. Cheng, C. Chen, W. Zhang, and Y. Yang, “5G-Enabled Cooperative Intelligent Vehicular When Benz Meets Marconi,” *IEEE Comput. Soc.*, no. August, pp. 53–59, 2017.

[27] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, “A comprehensive survey on vehicular Ad Hoc network,” *J. Netw. Comput. Appl.*, vol. 37, no. 1, pp. 380–392, 2014, doi: 10.1016/j.jnca.2013.02.036.

[28] H. ieee. org/servlet. Opac?punumber-6320593, “Draft guide for wireless access in vehicular environment (WAVE) architecture,” 2012.

[29] B. Ducourthial, Y. Khaled, and M. Shawky, “Conditional transmissions: Performance study of a new communication strategy in VANET,” *IEEE Trans. Veh. Technol.*, vol. 56, no. 6 I, pp. 3348–3357, 2007, doi: 10.1109/TVT.2007.907235.

[30] K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang, and Y. Zhou, “Heterogeneous Vehicular Networking: A Survey on Architecture, Challenges, and Solutions,” *IEEE Commun. Surv. Tutorials*, vol. 17, no. 4, pp. 2377–2396, 2015, doi: 10.1109/COMST.2015.2440103.

[31] M. Saini and H. Singh, “VANET, its Characteristics, Attacks and Routing Techniques: A

Survey," *Int. J. Sci. Res.*, vol. 5, no. 5, pp. 1595–1599, 2016, doi: 10.21275/v5i5.nov163726.

32 "https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.mdpi.com%2F4248220%2F19%2F22%2F4954%2Fhtm&psig=AOvVaw2G_NramxU6SSE0t1hR_KlZ&ust=1627674640821000&source=images&cd=vfe&ved=0CAsQjRxqFwoTCPCK6tiGifICFQAAAAAdAAAAABAj." .

[33] S. R. Kolte and M. S. Madankar, "Adaptive congestion control for transmission of safety messages in VANET," *2014 Int. Conf. Converg. Technol. I2CT 2014*, pp. 1–5, 2014, doi: 10.1109/I2CT.2014.7092177.

[34] L. Smith, "Dedicated Short Range Communication (DSRC) Statewide Guidance Summary of Research and Design Considerations Version 1.0," no. November 2018, 2018, [Online]. Available: https://www.tn.gov/content/dam/tn/tdot/traffic-engineering/TDOTDSRC_Final Report_version 1.0_Nov 2018.pdf.

[35] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proc. IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011, doi: 10.1109/JPROC.2011.2132790.

[36] The Institute of Electrical and Electronics Engineers, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11-2016," *IEEE Std 802.11-2016 (Revision IEEE Std 802.11-2012)*, vol. 2016, pp. 1–3534, 2013, [Online]. Available: http://ieeexplore.ieee.org/document/7786995/.

[37] R. J. Nieporent, *Metropolitan Area Networks*, vol. 2, no. March. 2011.

[38] IEEE, *IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages*, vol. 2016. 2016.

[39] IEEE Vehicular Technology Society, *IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture*. 2019.

[40] F. Domingos, A. Boukerche, L. Villas, C. Viana, and A. A. F. Loureiro, "Data Communication in VANETs : A Survey , Challenges and Applications To cite this

version : Data Communication in VANETs : A Survey , Challenges and Applications," 2015.

[41] Y. Li, "An Overview of the An Overview of the DSRC/WAVE Technology," vol. 15, no. March, pp. 9–21, 2015.

[42] ETSI, "ETSI TR 102 638 V1.1.1 (2009-06): Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions," *ETSI, Sophia Antip. Cedex, Fr.*, vol. 1, pp. 1–81, 2009, [Online]. Available: http://scholar.google.com/scholar?hl=en%7B&%7DbtnG=Search%7B&%7Dq=intitle:Intelligent+Transport+Systems+(ITS);+Vehicular+Communicatons;+Basic+Set+of+Applications;+Definitions%7B#%7D1.

[43] S. Title, W. Title, T. Title, and T. Miller, "SAFESPOT INTEGRATED PROJECT - IST-4-026963-IP DELIVERABLE SP6 – BLADE – Business models , Legal Aspects , and Deployment The SAFESPOT deployment programme List of Authors," no. February 2006, pp. 1–101, 2010.

[44] C. Manifesto, "CAR 2 CAR Communication Consortium Manifesto," *System*, p. 94, 2007, [Online]. Available: http://www.car-2-car.org/fileadmin/downloads/C2C-CC_manifesto_v1.1.pdf.

[45] SAE, "DSRC Implementation Guide, A guide to users of SAE J2735 message sets over DSRC," *Retrieved from https//www.sae.org/standards/ (accessed January 2018)*, 2010.

[46] CAMP, "Vehicle Safety Communications Project Task 3 Final Report," *Natl. Highw. Traffic Saf. Adm.*, no. March, pp. 8–72, 2005.

[47] M. Van Eenennaam, L. Hendriks, G. Karagiannis, and G. Heijenk, "Oldest packet drop (OPD): A buffering mechanism for beaconing in IEEE 802.11p VANETs (poster)," *IEEE Veh. Netw. Conf. VNC*, pp. 252–259, 2011, doi: 10.1109/VNC.2011.6117108.

[48] N. Gupta, A. Prakash, and R. Tripathi, "Adaptive beaconing in mobility aware clustering based MAC protocol for safety message dissemination in VANET," *Wirel. Commun. Mob. Comput.*, vol. 2017, 2017, doi: 10.1155/2017/1246172.

[49] R. K. Schmidt, T. Leinmüller, E. Schoch, F. Kargl, and G. Schäfer, "Exploration of

adaptive beaconing for efficient intervehicle safety communication," *IEEE Netw.*, vol. 24, no. 1, pp. 14–19, 2010, doi: 10.1109/MNET.2010.5395778.

[50] C. Chigan and J. Li, "A delay-bounded dynamic interactive power conftol algorithm for VANETs," *IEEE Int. Conf. Commun.*, pp. 5849–5855, 2007, doi: 10.1109/ICC.2007.969.

[51] H. Lu, "MobiCo m 2010 Poster : Balancing Broadcast Reliability and Trans m ission Range in VANETs," pp. 25–27, 2010.

[52] K. A. Hafeez, L. Zhao, Z. Liao, and B. N. W. Ma, "A new broadcast protocol for vehicular ad hoc networks safety applications," *GLOBECOM - IEEE Glob. Telecommun. Conf.*, pp. 1–5, 2010, doi: 10.1109/GLOCOM.2010.5683409.

[53] E. M. Van Eenennaam, G. Karagiannis, and G. J. Heijenk, "Towards scalable beaconing in VANETs," *Fourth ERCIM Work. eMobility*, pp. 103–108, 2010.

[54] R. Stanica, E. Chaput, and A. L. Beylot, "Broadcast communication in Vehicular Ad-Hoc Network safety applications," *2011 IEEE Consum. Commun. Netw. Conf. CCNC'2011*, pp. 462–466, 2011, doi: 10.1109/CCNC.2011.5766513.

[55] D. B. Rawat, G. Yan, D. C. Popescu, M. C. Weigle, and S. Olariu, "Dynamic adaptation of joint transmission power and contention window in VANET," *IEEE Veh. Technol. Conf.*, 2009, doi: 10.1109/VETECF.2009.5378793.

[56] M. Raya, J.-P. Hubaux, and Claims, "Securing vehicular ad hoc networks," *Vol. 15, Issue 1January 2007Special Issue Secur. Ad-hoc Sens. Networks*.

[57] P. D. Kilmer, "Review Article: Review Article," *Journalism*, vol. 11, no. 3, pp. 369–373, 2010, doi: 10.1177/1461444810365020.

[58] X. Liu, Z. Fang, and L. Shi, "Securing Vehicular Ad Hoc Networks," 2007.

[59] N. M. Mittal and S. Choudhary, "Comparative Study of Simulators for Vehicular Ad-hoc Networks (VANETs)," vol. 4, no. 4, 2014.

[60] "SUMO User Documentation," *https://sumo.dlr.de/docs/index.html*, 2021. .

[61] M. Boban and T. T. V Vinhoza, "Modeling and Simulation of Vehicular Networks : Towards Realistic and Efficient Models."

[62] Y. R. B. Al-mayouf, M. Ismail, N. F. Abdullah, and S. Al-qaraawi, “Survey on VANET technologies and simulation models,” no. January, 2016.

[63] Installation, “NS3 Network Simulator,” *https://www.nsnam.org/*. .

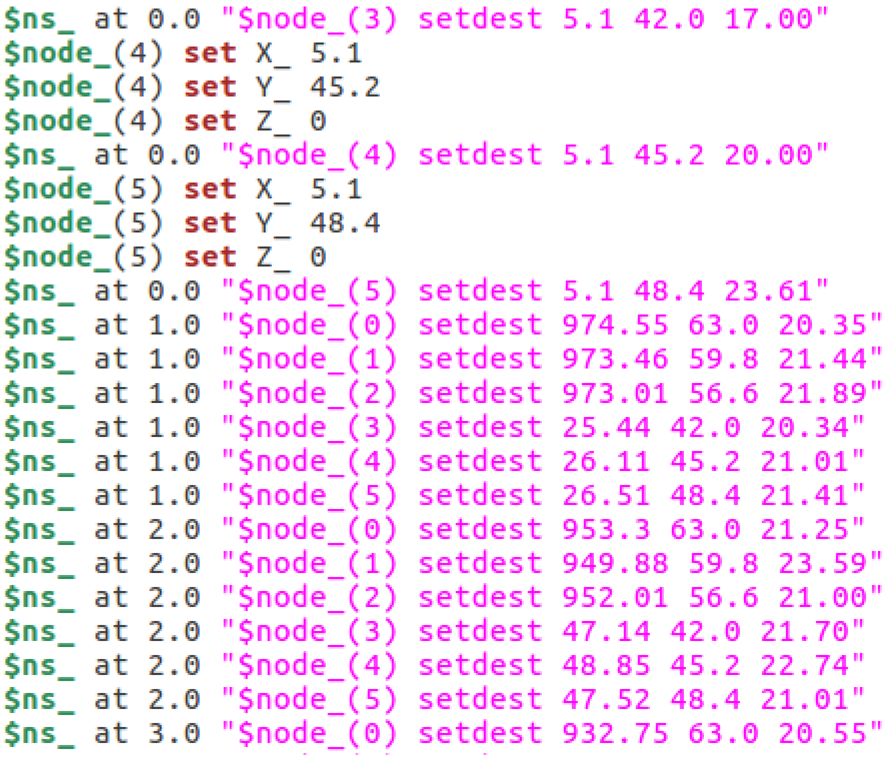
[64] C. Ozgur, T. Colliau, and G. Rogers, “MatLab vs . Python vs . R,” no. July, 2017.

[65] C. Ozgur, T. Colliau, G. Rogers, Z. Hughes, and E. B. Myer-tyson, “MatLab vs . Python vs . R,” vol. 5, pp. 355–372, 2017.

[66] J. Bu, G. Tan, N. Ding, M. Liu, and C. Son, “Implementation and evaluation of WAVE 1609.4/802.11p in ns-3,” *ACM Int. Conf. Proceeding Ser.*, 2014, doi: 10.1145/2630777.2630778.

Appendix

Sample of .tcl file



```
$ns_ at 0.0 "$node_(3) setdest 5.1 42.0 17.00"
$node_(4) set X_ 5.1
$node_(4) set Y_ 45.2
$node_(4) set Z_ 0
$ns_ at 0.0 "$node_(4) setdest 5.1 45.2 20.00"
$node_(5) set X_ 5.1
$node_(5) set Y_ 48.4
$node_(5) set Z_ 0
$ns_ at 0.0 "$node_(5) setdest 5.1 48.4 23.61"
$ns_ at 1.0 "$node_(0) setdest 974.55 63.0 20.35"
$ns_ at 1.0 "$node_(1) setdest 973.46 59.8 21.44"
$ns_ at 1.0 "$node_(2) setdest 973.01 56.6 21.89"
$ns_ at 1.0 "$node_(3) setdest 25.44 42.0 20.34"
$ns_ at 1.0 "$node_(4) setdest 26.11 45.2 21.01"
$ns_ at 1.0 "$node_(5) setdest 26.51 48.4 21.41"
$ns_ at 2.0 "$node_(0) setdest 953.3 63.0 21.25"
$ns_ at 2.0 "$node_(1) setdest 949.88 59.8 23.59"
$ns_ at 2.0 "$node_(2) setdest 952.01 56.6 21.00"
$ns_ at 2.0 "$node_(3) setdest 47.14 42.0 21.70"
$ns_ at 2.0 "$node_(4) setdest 48.85 45.2 22.74"
$ns_ at 2.0 "$node_(5) setdest 47.52 48.4 21.01"
$ns_ at 3.0 "$node_(0) setdest 932.75 63.0 20.55"
```

Sample of python program

```
brd_counter = 0
sndr_id = 0
for i in sorted_nodesInfo:
    if i[0]!=0:
        if i[0]!=sndr_id:
            sndr_id = i[0]
            brd_counter=0
        else:
            if brd_counter >= 6 :
                if sndr_id in RSU['Sdr_Id'].values:
                    brd_counter=0
                    continue
            else:
                brd_counter+=1
                jumped_brd_info.append([i[0], i[1]])
    else:
        jumped_brd_info.append([i[0], i[1]])
```

Sample NS3 program

```
using namespace ns3;
int main (int argc, char *argv[]) //int argc, char *argv[] kun isaa duratti
{
  CommandLine cmd;
  cmd.Parse (argc, argv);



  // uint32_t SenderPackets=0;
   //uint32_t SenderPackets=0;
   //uint32_t SenderPackets=0;

  //A tool I created so that we only start the applications within nodes when they actually enter the simulation.
  Ns2NodeUtility ns2_utility ("scratch/DagiThesis/Mymobility1.tcl");
  uint32_t nnodes = ns2_utility.GetNNodes();
  double sim_time = ns2_utility.GetSimulationTime();

//Create a node container for vehicles
  NodeContainer nodes;
//create a node coantainer for RSUs
  NodeContainer rsu_container;
  nodes.Create (nnodes);
  rsu_container.Create(1);

 // FlowMonitorHelper flowmon;
  //flowmon = flowmon.InstallAll ();

  //For vehicles,you can use SUMO-generated trace.Using the bulit-in ns-2 mobility helper
 Ns2MobilityHelper sumo_trace ("scratch/DagiThesis/Mymobility1.tcl");
```

```
sumo_trace.Install(nodes.Begin(),nodes.End()); //install ns-2 mobility in all nodes
//For RSU, use contantPositionMobiltyModel
MobilityHelper mob;
mob.SetMobilityModel("ns3::ConstantPositionMobilityModel");
mob.Install(rsu_container);

//Now that you installed contantPositionMobiltyModel,we can set RSU node positions as you please
//For node RSU 0, We can set the position to 100,200,3

rsu_container.Get(0)->GetObject<MobilityModel>()->SetPosition(Vector(100,200,3));

//we can also using the loop For example if the RSU are in straight Highway and spaced by 300 meters
//WaveSetup wave;
//wave.ConfigureDevices(rsu_container);
double distance=300.0;
for (uint32_t i=0;i<rsu_container.GetN();i++){

rsu_container.Get(0)->GetObject <MobilityModel>()->SetPosition( Vector(100 + distance,200,3));



}

  //To write shorter code, I put the code to setup WaveNetDevice in a separate file.
  WaveSetup wave;
  wave.ConfigureDevices(nodes);

  //Let's install my CustomApplication to all nodes and start them at the appropriate time using my utilitiy.
  for (uint32_t i=0 ; i<nnodes; i++)
    {
      Ptr<Node> n = nodes.Get(i);
      Ptr<CustomApplication> app = CreateObject <CustomApplication>();


      app->SetStartTime(Seconds (ns2_utility.GetEntryTimeForNode(i))); //this is the first time the node appears in the ns-2 trace

      app->SetStopTime (Seconds (ns2_utility.GetExitTimeForNode(i)));

      n->AddApplication(app);

    }



  Simulator::Stop(Seconds (sim_time)); //because this is the last timestamp in your ns-2 trace


//AnimationInterface anim("/home/dagy/ns-allinone-3.29/netanim-3.107/vehiclesmotion.xml");

          //EPC server



  std::cout << "End of Program" << std::endl;


}


namespace ns3

{

  Ns2NodeUtility::Ns2NodeUtility (std::string name)

  {

    m_file_name = name;

    m_input_file.open(m_file_name);


    std::string line;


    std::vector <uint32_t> node_ids;
  while (std::getline (m_input_file, line))
    {
        std::smatch sm;
        std::regex r("\\$ns_ at (\\d*.\\d) \"\\$node_\\((\\d*)\\)");
        if (std::regex_search(line, sm, r))
          {
            //std::cout << "MATCH!" << std::endl;

            uint32_t id = std::stoi(sm[2]);
            double new_latest = std::stof(sm[1]);

            if ( std::find (node_ids.begin(), node_ids.end(), id) != node_ids.end())
              {
                  double entry_time = std::get<0> (m_node_times [id]);
                  m_node_times [id] = std::make_pair(entry_time, new_latest);
              }
            else
              {
                  m_node_times [id] = std::make_pair(new_latest, new_latest);
              }
            node_ids.push_back(id);
          }
        else
          {
            //std::cout << "No Match!" << std::endl;
          }
    }
}
uint32_t
Ns2NodeUtility::GetNNodes ()
```

```
{
  return m_node_times.size();
}
double
Ns2NodeUtility::GetEntryTimeForNode (uint32_t nodeId)
{
  return std::get<0>(m_node_times [nodeId]);
}
double
Ns2NodeUtility::GetExitTimeForNode (uint32_t nodeId)
{
  return std::get<1>(m_node_times [nodeId]);
}
double
Ns2NodeUtility::GetSimulationTime()
{
  double time = 0;

  for (uint32_t i=0 ; i<m_node_times.size(); i++)
    time = std::max ( time,  std::get<1>(m_node_times[i]) );

  return time;
}



void
Ns2NodeUtility::PrintInformation()
{
  uint32_t s = m_node_times.size();
  for (uint32_t i=0 ; i<s; i++)
```

```
      {
            std::cout << "Node " << i << " started " << std::get<0>(m_node_times[i]) << " and ended " <<
std::get<1>(m_node_times[i]) << std::endl;
      }
  }
}
```