EFFICIENT MANAGEMENT OF EXCESSIVE MESSAGING FOR EMERGENCY SCENARIOS IN INTERNET OF VEHICLES

By

HASNAT ABID

NATIONAL UNIVERSITY OF MODERN LANGUAGES

ISLAMABAD

August, 2022

Efficient Management of Excessive Messaging for Emergency Scenarios in Internet of Vehicles

By

HASNAT ABID

MSCS, National University of Modern Languages, Islamabad, 2022

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

In **Computer Science**

To

FACULTY OF ENGINEERING & COMPUTER SCIENCE

NATIONAL UNIVERSITY OF MODERN LANGUAGES ISLAMABAD

NATIONAL UNIVERSITY OF MODERN LANGUAGES FACULTY OF ENGINEERIING & COMPUTER SCIENCE

THESIS AND DEFENSE APPROVAL FORM

The undersigned certify that they have read the following thesis, examined the defense, are satisfied with overall exam performance, and recommend the thesis to the Faculty of Engineering and Computer Sciences for acceptance.

Thesis Title: Efficient Management of Excessive Messaging for Emergency Scenarios in Internet of Vehicles

Submitted By: Hasnat Abid **Registration #:** 40 MS/CS/F20

Master of Science in Computer Science (MSCS)
Title of the Degree

Computer Science
Name of Discipline

Dr. Ata Ullah
Name of Research Supervisor

Signature of Research Supervisor

Dr. Basit Shahzad
Name of Dean (FE&CS)

Signature of Dean (FE&CS)

Prof. Dr. Muhammad Safeer Awan
Name of Pro-Rector Academics

Signature of Pro-Rector Academics

August 4th, 2022

AUTHOR'S DECLARATION

I Hasnat Abid

Daughter of Abid Mahmood

Registration # 40 MS/CS/F20

Discipline Computer Science

Candidate of **Master of Science in Computer Science (MSCS)** at the National University of Modern Languages do hereby declare that the thesis **Efficient Management of Excessive Messaging for Emergency Scenarios in Internet of Vehicles** submitted by me in partial fulfillment of MSCS degree, is my original work, and has not been submitted or published earlier. I also solemnly declare that it shall not, in future, be submitted by me for obtaining any other degree from this or any other university or institution. I also understand that if evidence of plagiarism is found in my thesis/dissertation at any stage, even after the award of a degree, the work may be cancelled and the degree revoked.

____
Signature of Candidate

Hasnat Abid
Name of Candidate

4th August, 2022
Date

ABSTRACT

Title: Efficient Management of Excessive Messaging for Emergency Scenarios in Internet of Vehicles

Due to the vast range of applications in numerous fields, the internet of vehicles (IoVs) has recently sparked a lot of attention. For supplying various services, these applications rely on the latest vehicle information. Constant message broadcasts by many vehicles, on the contrary, may not only overwhelm a centralized server but also produce enough traffic that is incompatible with continuous service, particularly in emergencies. Vehicles communicate and send messages for better conveyance. Some messages inform other vehicles about accidents or other unpleasant situations. In prior work, vehicles conveyed messages to one hop. There is a high probability that such a vehicle is not connected with the RSU, so vehicles cannot transfer emergency messages to other vehicles, and vehicles in that area cannot be aware of an emergency. Efficient management of excessive messaging (EEMS) for an emergency scenario in the internet of vehicles is a fog-assisted congestion avoidance strategy for IoV presented in this study. As in the previous research paper, they only implemented just one-hope neighbors to find the closest RSU for relaying an emergency message. However, suppose your one-hop neighbors do not discover the RSU. In that case, the message is likely to be lost and not sent to other vehicles in emergency conditions, making the situation extremely dangerous. When we enhance this one-hop neighbor to more than 2 to 3-hop neighbors, we can more easily locate the RSU and send out emergency signals to the whole network. Unlike most previous systems, EEMS takes advantage of fog computing benefits to reduce communication costs, congestion, and message delay and improve control services. Every vehicle must communicate with a fog server on regular terms, either straight or along intermediary nodes. In an emergency scenario, the fog server alerts approaching traffic to steady down and deploys rescue teams to offer needed assistance and organize patrol operations to clear the route. NS 2.35 simulations are used to validate the proposed scheme's performance. In terms of delay and communication cost, simulation findings show that EEMS reigns supreme over current methods.

TABLE OF CONTENTS

CHAPTER	TITLE		PAGE
	THESIS AND DEFENSE APPROVAL FORM		ii
	AUTHOR'S DECLARATION		iii
	ABSTRACT		iv
	TABLE OF CONTENTS		v
	LIST OF TABLES		viii
	LIST OF FIGURES		ix
	LIST OF ABBREVIATIONS		x
	LIST OF SYMBOLS		xi
	ACKNOWLEDGEMENT		xii
	DEDICATION		xiii
1	**INTRODUCTION**		**2**
	1.1	Introduction	2
	1.2	Motivation	5
		1.2.1 Architecture of Internet of Vehicles	6
		1.2.2 Applications of Internet of Vehicles	7
		1.2.3 Constraints in IoV Networks	7
	1.3	Problem Background	8
	1.4	Problem Statement	9
	1.5	Research Questions	9
	1.6	Aim of Research	10
	1.7	Research Objectives	10
	1.8	Scope of the Research Work	10

	1.9	Thesis Organization	11
2	**LITERATURE REVIEW**		**13**
	2.1	Overview	13
		2.1.1 DSRC-Based Data Dissemination	14
		2.1.2 LTE- Based Data Dissemination	20
		2.1.3 Hybrid Data Dissemination	22
	2.2	Comparison of Studied Emergency Message Dissemination Protocols	34
	2.3	Research Gap and Directions	38
	2.4	Summary	39
3	**METHODOLOGY**		**40**
	3.1	Overview	40
	3.2	Methodology	40
	3.3	Operational Framework	41
	3.4	Research Design and Development	43
	3.5	Simulation Framework	45
		3.5.1 Assumptions and Limitations	45
	3.6	Summary	45
4	**PROPOSED EXCESSIVE MESSAGING MANAGEMENT SCHEME**		**47**
	4.1	Overview	47
	4.2	Proposed Excessive Messaging Management Scheme	47
	4.3	Proposed Excessive Messaging Management Flowchart	50
	4.4	Efficient Messaging Algorithm (EMA)	52
	4.5	Summary	54
5	**PERFORMANCE EVALUATION**		**55**
	5.1	Overview	55
	5.2	Results and Analysis	55
		5.2.1 Performance Metrics	57
		5.2.2 Communication Overhead during Messaging	58

		5.2.3 Packet Delivery Ratio	59
		5.2.4 Packet Loss Ratio	60
		5.2.5 Message Transmission Delay	61
		5.2.6 Throughput	62
	5.3	Summary	63
6	**CONCLUSION AND FUTURE WORK**		**64**
	6.1	Overview	64
	6.2	Conclusion	64
	6.3	Summary of Contribution	65
	6.4	Future Work	65
REFERENCES			**66**

LIST OF TABLES

TABLE NO.	TITLE	PAGE
2.1	Comparative analysis of several emergency message distribution techniques	35
5.1	Simulation Parameters	56

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE
1.1	IoV Network	3
1.2	Fog server-based architecture for transportation systems	5
1.3	IoV Network Architecture	6
2.1	Effective Emergency Message Dissemination Scheme	16
2.2	Emergency Message Dissemination	30
2.3	EV Message Dissemination Scenario	31
3.1	Operational Framework of the Research	42
3.2	Roadside unit at 1-hop neighbors	43
3.3	Research methodology plan for excessive messaging management scheme	44
4.1	RSU at 2-hop neighbors	49
4.2	RSU at 3-hop neighbors	49
4.3	Procedural Flowchart of Excessive Messaging Management Scheme	51
4.4	Algorithm for Efficient Management of Excessive Messaging	53
5.1	Redundant recurrence of messages in IoVs	57
5.2	Communication overhead during messaging	58
5.3	Packet delivery ratio for emergency messages	60
5.4	Packet loss ratio during message dissemination	61
5.5	Average delay for message dissemination	62
5.6	Throughput for the Emergency Message Initiation from Vehicles	63

LIST OF ABBREVIATIONS

IoT	-	Internet of Things
VANET	-	Vehicular Ad-hoc Network
ITS	-	Intelligent Transport System Vehicular
IoV	-	Internet of Vehicle
OBU	-	On-Board Unit
V2V	-	Vehicle-to-Vehicle
V2I	-	Vehicle to Infrastructure
V2P	-	vehicle to Pedestrian
V2C	-	Vehicle to Cloud
GPS	-	Global Positioning Systems
SSVC	-	Sensor Enabled Secure Vehicular Communication
ACO	-	Ant Colony Optimization
DA-TRLD	-	Dynamic Aware Transmission Range on Local Traffic Density
CLPSO	-	Comprehensive Learning Particle Swarm Optimization
JSO	-	Jellyfish Search Optimization
IoCV	-	Internet of Connected Vehicle
WAVE	-	Wireless Access in Vehicular Environment
DBA-PA	-	Driver Behavior Analysis and Personalized Assistance
DSRC	-	Dedicated Short Range Communication
LTE	-	Long Term Evolution
RSU	-	Roadside Unit
QoS	-	Quality of Service
CSN	-	Connected Sensor Network
SCF	-	Store Carry Forward
LAT	-	Link Available Time

LIST OF SYMBOLS

I_v	-	Intelligent vehicle
B_v	-	Basic vehicle
S_v	-	Smart vehicle
V_{TYPE}	-	Vehicle type
EMs	-	Emergency messages
NMs	-	Normal messages
N	-	Nodes
SN	-	Sink nodes
UV	-	Un-clustered Vehicles
UN	-	Unregistered Node
FV	-	Forwarder Vehicle
OC	-	Ordinary Cluster
CH	-	Cluster Head
CM	-	Cluster Member
CF	-	Cluster Forwarder
GC	-	Gateway Cluster
FP	-	Final Vehicle's Position

ACKNOWLEDGMENT

First of all, I wish to express my gratitude and deep appreciation to Almighty Allah, who made this study possible and successful. This study would not be accomplished unless the honest espousal that was extended from several sources for which I would like to express my sincere thankfulness and gratitude. Yet, there were significant contributors for my attained success and I cannot forget their input, especially my research supervisors, Associate Professor. Dr. Ata Ullah, who did not leave any stone unturned to guide me during my research journey.

I shall also acknowledge the extended assistance from the administrations of Department of Computer Sciences who supported me all through my research experience and simplified the challenges I faced. For all whom I did not mention but I shall not neglect their significant contribution, thanks for everything.

DEDICATION

This thesis work is dedicated to my parents and my teachers throughout my education career who have not only loved me unconditionally but whose good examples have taught me to work hard for the things that I aspire to achieve.

CHAPTER 1

INTRODUCTION

1.1 Introduction

In the novel era of IoT, the transformation of old VANETs into IoVs is expedited. The IoVs introduce new technologies into vehicular networks with the goal of overcoming the constraints of VANETs [1]. Paper [2] contrasts VANETs with IoVs from several perspectives, emphasizing the IoVs' design and development benefits. The IoVs are dispersed systems that enable connected vehicles and VANETs to share information. The IoVs primary goal is to permit vehicles to communicate in real-time with their drivers, walkers, other automobiles and roadside infrastructure [3][4][5]. Communication of a vehicle with other vehicles and other elements has the potential to improve safety and driving systems dramatically. Furthermore, it is critical to fully utilize communication and information technology in order to achieve coordinated human, vehicle, and environmental development, which may reduce traffic congestion, improve transportation efficiency, and expand current road capacity [6]. Therefore, constructing an intelligent transportation system for vehicular grid using the Internet of Things in the form of the IoV is essential. The IoVs provide five different network connection modes: On-Board Units (OBUs) are used in intra-vehicle systems to control the vehicle's inner functionality. OBU is a vehicle-mounted device that ensures connection security and reliability by utilizing Wireless Access in Vehicular Environment (WAVE) technology. Vehicle-to-vehicle (V2V) schemes allow for the wireless exchange of data about neighboring vehicles' speeds and locations. Wireless data transfers between both the vehicle and RSUs are enabled via Vehicle to Infrastructure (V2I) networks. Roadside Units (RSUs) have been placed in VANETs to increase network connectivity and help convey messages and provide Quality of Service (QoS) to users [7]. Vehicle to Cloud (V2C) technologies allow vehicles to connect to the internet for extra information via application program interfaces

(APIs). Vulnerable Road Users such as cyclists and pedestrians are supported by Vehicle to Pedestrian (V2P) systems. The IoVs allow for collecting and exchanging data about vehicles, roads, and their surroundings [8]. Figure 1.1 depicts an IoV network. IoV has three levels from a system perspective: vehicles, connectivity, and data.

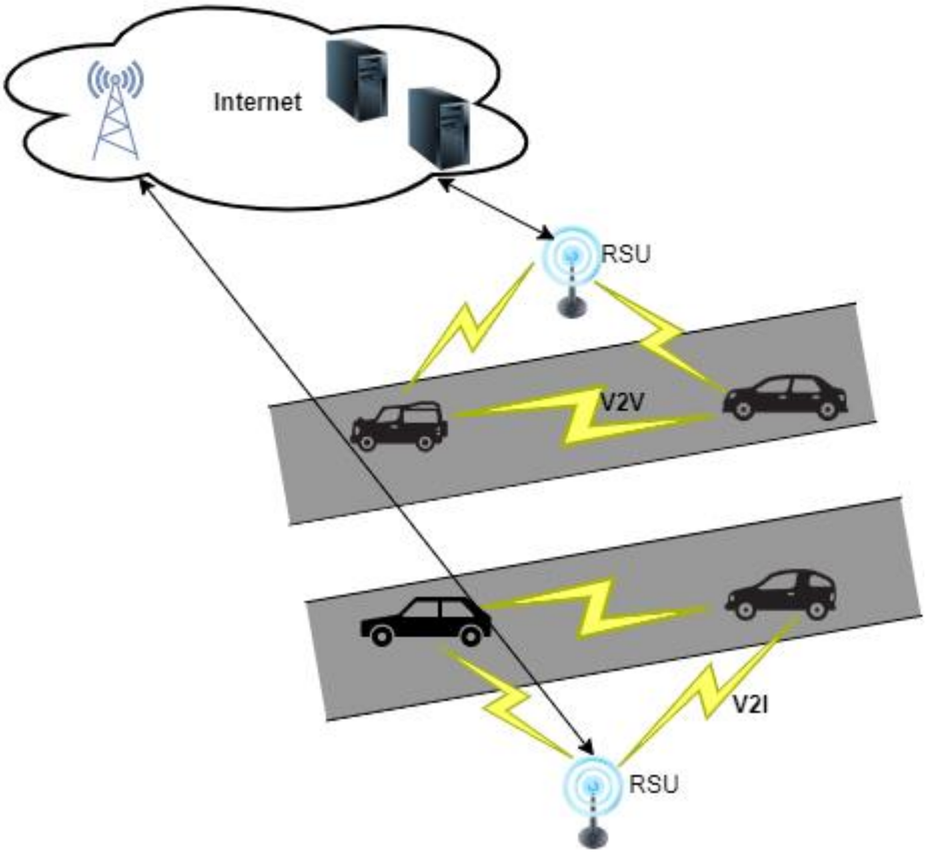

Figure 1.1: IoV Network

The major key goal of VANETs research is to create a low-cost vehicular communication system that allows for effective data dissemination for the safety and comfort of passengers. By restricting the number of retransmissions, an effective broadcast strategy should ensure fast dissemination [9]. Broadcast transmission, which takes use of the wireless channel's broadcasting characteristics, is a cost-effective way to promote information in a wireless network. However, sending emergency alerts to other vehicles is particularly difficult due to the obvious increased mobility and hostile wireless surroundings in vehicular networks. The majority of emergency signals are life-critical and ought to be conveyed as quickly and reliably as possible to other vehicles [10]. The purpose of broadcasting is to send messages from one vehicle to every other vehicles in a system [11]. In order to achieve greater vehicle coverage, location-based advertising promotes dependability, whereas warning transmission, which communicates emerging message to approach vehicles, needs both minimal reliability and propagation latency [12]. The most fundamental and significant use of VANET is the safety application, which aims to minimize the likelihood of traffic accidents and avoid secondary injuries [13].

All of the vehicles including sensors and Global Positioning Systems (GPS) that collect information about the vehicle's location, direction, acceleration, and velocity. These facts are shared with its neighbors in order to ensure safety and avoid any hazards when driving. Finally, it is obvious that selecting proper Dissemination schemes requires much effort and consideration. One of the key problems causes broadcast Storm Problem: message dissemination. It generates unnecessary broadcasting of the same messages, causing communication delays and network performance degradation [14]. Adapt distribution strategies to account for vehicle density and location to reduce broadcast storm problem and increase efficiency. The broadcast storm problem may be measured using packet drop, message latency, and traditional measurements like message accessibility and message cost.

In IoV, a major concerning issue during message dissemination is congestion, which is addressed by present congestion recognition systems. Beaconing messages are used to communicate between vehicles and a central server. Due to the restricted communication range of vehicles, direct connection between the server and the vehicles is not possible. As a part of the result, vehicles might depend on multi-hop communication, which might lead to a message storm and congestion. In IoVs, message congestion might result in poor road protection. It arises after a vehicle repeatedly broadcasts the packet. Recurrent packets cause packet collisions, which is inefficient for scalability. This paper presents an Excessive Messaging Management Scheme for Emergency Scenario in IoVs. This method aids to evade congestion and properly spread all types of communications for dependable communication. Fog computing is used by EEMS to assist process and disseminate data locally. Vehicles provide regular updates to the fog server about their present condition. The anomalous vehicle (Av) in the proposed scenario transmits messages straight to the fog server or maximum three-hop neighbors. If a fog server is not directly available to the abnormal vehicle (Av) at that time, it communicates by adjacent vehicles in maximum three hop neighbors, chooses the vehicle with the shortest route to the fog server, and send emergency signal to it. When server is beyond of the Av range, messages are sent to the server using V2V communication in IoVs.

Figure 1.2 displays the many modes of communication used to exchange information. For information interchange, we employ a fog server, a roadside device, the cloud, a trusted authority, and vehicles. The fog server sits between the cloud server and the vehicles or RSU, sharing information from the vehicles and RSU to the cloud. Vehicles may connect with other vehicles, send information to an RSU nearby, and communicate directly with the fog server in this configuration. In addition, the fog server may interact with both the RSU and the cloud.

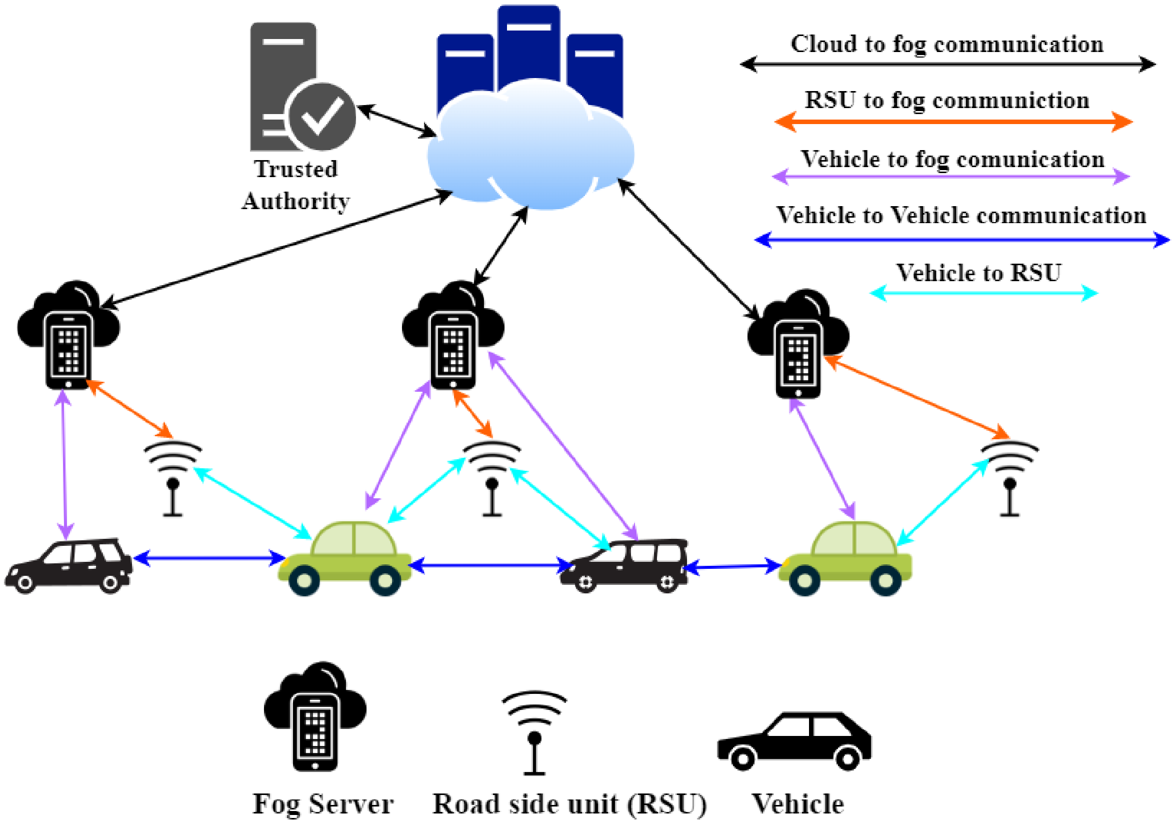

Figure 1.2: Fog server-based architecture for transportation systems

1.2 Motivation

IoV has been implemented in many different fields, including energy, industry, health and smart city transportation management. Applications serve a variety of objectives and provide a variety of services depending on the needs of the user. IoV applications are classified according to their domain. The ITS attempts to increase traffic efficiency while also reducing the risk of road accidents. Vehicles interact with one another by exchanging vehicle-related communications. Vehicles should transmit emergency messages with neighboring vehicles based on the traffic conditions and circumstances so that the urgent situation may be mitigated quickly. Many strategies have been proposed for this aim; however, they are limited in various ways. It is quite difficult to transmit emergency notifications to the appropriate vehicles in a timely manner. IoV is a comparatively novel topic, which has yet to be thoroughly investigated. Consequently, IoV must be thoroughly examined from all angles prior to deployment. Its potential application areas, as well as the security dangers and difficulties that go along with it, must be recognized. A number of academics is already working on the security features of IoV across the world. Therefore, determining the status and issues with existing security solutions is critical. As a result, in this study piece, we have made an honest effort to discover these issues.

1.2.1 Architecture of Internet of Vehicles

IoV is made up of many wireless network components that are sophisticated and diverse. Figure 1.3 below shows the architecture of IoVs. IoV has three levels from a system perspective: Vehicles, connectivity, and servers/clouds.

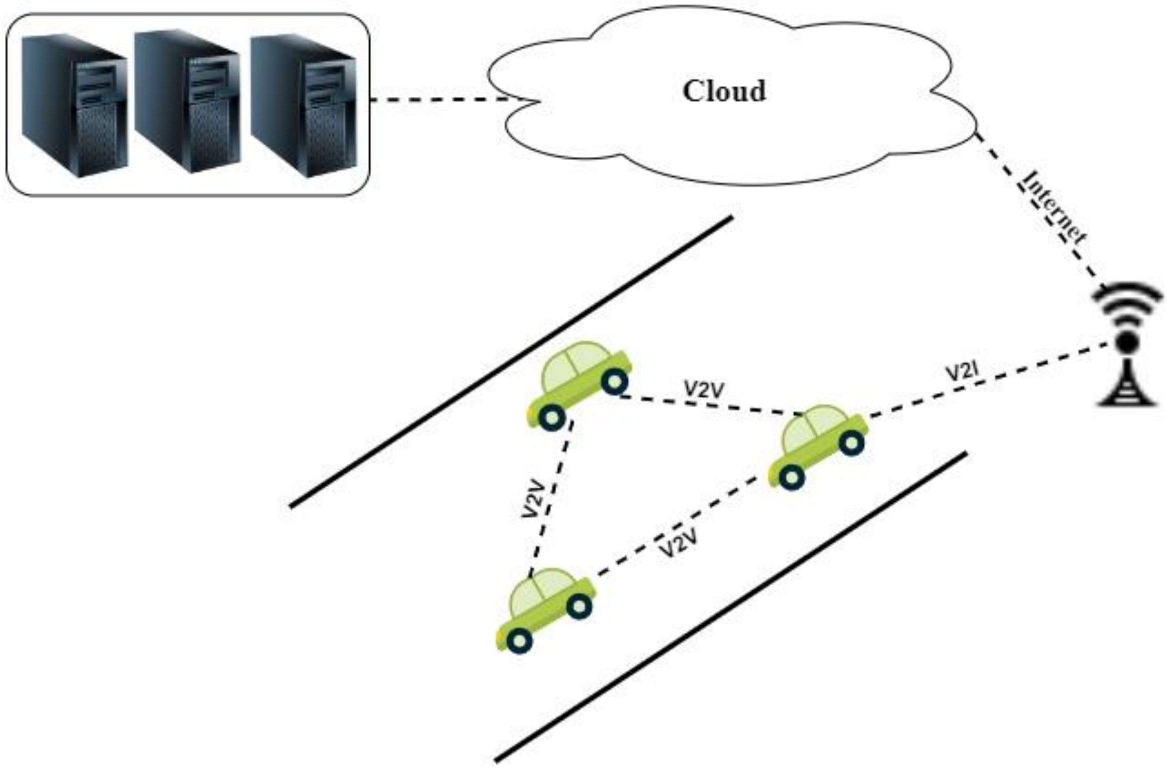

Figure 1.3: IoVs Network Architecture

Vehicles play a dual function in the Internet of Things: they are clients who consume Internet services and they are peers who do distributed computing. IoV is made up of two different sorts of wireless connections in terms of communications. Vehicle to vehicle communication is used to communicate data directly among vehicles. Vehicle to Road (V2R), also known as Vehicle-to-Infrastructure, is the second form of connection (V2I). V2R refers to V2V transmission as well as roadside infrastructure linked with wireless transmission technology, such as traffic signals or roadwork warning signs. V2R, unlike V2V, can communicate over great distances and has a high scalability. To improve the aforementioned applications situations, V2R permits the interaction of vehicles and roadside equipment.Vehicles may get services from servers or cloud data centres. Because servers have higher computational power, storage capacity, and information/data outside of vehicles, sophisticated or complicated IoV systems must use servers on the Internet.

1.2.2 Applications of Internet of Vehicles

Here are few of the primary uses of IoV that alter the driving experience: IoV technology ensures a secure driving environment. Sensors in cooperative collision avoidance systems detect possible collisions and give a warning message to the driver. Periodic alerts on the vehicle's performance or emergency notifications are also sent out. With the aid of new linked highways, traffic congestion, unsafe road conditions, and accidents all prompt an emergency alert. The IoVs enables remote access to a vehicle. This enables services such as remote door lock and retrieving a stolen vehicle, as well as "locate my vehicle," which is particularly useful when you have left your vehicle in a massive parking garage. Traffic guiding systems, safe navigation, intelligent vehicle control, collision avoidance, electronic toll collection, traffic flow monitoring, and even vehicle autonomy are examples of Internet of Vehicle applications.

1.2.3 Constraints in IoV Networks

i. *Delay:* The delay in emergency message sharing among vehicles causes several severe issues. If a critical shipment takes a long time to arrive and several unpleasant situations or issues arise within that time, it is a major issue. Delay refers to a package that is not delivered efficiently and on time. When a packet is delayed and the source does not get acknowledgement then packet is resent, which increases the delay.

ii. *Delivery:* The way a packet is handled by the underlying networks under the management of the network layer is referred to as delivery.

iii. *Forwarding:* The term "forwarding" refers to placing a packet on its way to its destination. A routing table is required for forwarding on a host or router. When a host sends a packet or a router receives a packet to forward, it consults this database to determine the best path to the final destination. However, with today's internetwork, such as the Internet, this simple approach is unworkable since the quantity of entries required in the routing table would make table lookups expensive. The next-hop approach is a way for condensing the contents of a routing table. Instead of storing information about the entire path, the routing table in this method merely stores the address of the next hop.

iv. *Congestion:* Congestion happens when the demand on the system or the number of packets delivered to the system is greater than the network's capability or the number of packets it can process.

1.3 Problem Background

IoVs refer to the number of linked moving vehicles in a network. These mobile vehicles can come into direct contact or via multi-hop transmission. For routine messaging and accident alerts, vehicles interchange various types of communication, including normal messages (NMs) as well as emergency messages (EMs). These messages provide information such as the vehicle's location, velocity, direction, and other pertinent information. When a large number of accidents occur, emergency warnings are transmitted to the server, which locates the nearest server users, causing congestion. Because of the increased packet latency and collisions caused by continuously sent signals, the storm gets more severe in cases of high vehicle density. In [15], there is no error correction in the system with sensors and OBU, which increases processing time greatly. In the IoV, congestion avoidance strategies are critical. Messages appear again on every transmission inside one-hop and multi-hop groups [16], which is the main impact of the issue. Message storms and congestion occur when several IoV vehicles send messages to a central server at the same time. Due to needless messaging, message congestion causes packet loss [17][18], communication costs [19][20], and increased delays. In the case of NMs, these limits are still bearable. Packet loss and message delivery delays during accident reporting are particularly severe in the event of EMs. When simulating a high number of nodes, NS2 consumes a lot of CPU and memory [21]. For security difficulties in privacy and safety-related applications, this approach is inefficient [22]. In current designs, central units and adjacent vehicles generate message transmission delays and information repetitions, resulting in communication overhead. In [19], vehicles transmit emergency messages to one-hop neighbors where there is a high probability that the RSU in that one-hop is unavailable. Therefore, we need to solve this issue by taking one-hop neighbors to two- or three-hop neighbors. If we do not find any RSU for emergency message dissemination at one-hop, we check at two-hop neighbors, and if we still do not find RSU at two-hop neighbors, we extend the search to three-hop neighbors. We need to solve this issue in this paper.

1.4 Problem Statement

For better transportation, vehicles communicate and send messages. Some messages inform other vehicles about accidents or other unpleasant incidents. In previous work, vehicles sent emergency messages to one hop. There is a high probability that such a vehicle is not connected with the RSU, so emergency messages cannot be transmitted to other vehicles, and vehicles in that area cannot be aware of an emergency. Due to this issue, many nearby vehicles involve unnecessary messing without confirmation that the server has already received the message and a rescue effort is already in progress. It increases latency, communication costs, and congestion in the network.

1.5 Research Questions

The key research questions of our work are enumerated as follows:

i. What will be effect of hop count over messaging via RSU?
ii. Which mechanisms reduce congestion and latency?
iii. How to minimize communication costs between vehicle and central server?

1.6 Aim of the Research

Using modern IoT technologies, the IoVs intend to create an integrated intelligent transportation system that improves traffic performance, prevents accidents, maintains road safety, and enhances driving experiences. This work aims to address an issue with emergency message distribution that tends to reduce latency and congestion. This programme seeks to supply emergency vehicles as soon as possible in the event of an accident, as delays cannot be accepted in this situation. This integration intends to improve the environment and public area for citizens while also increasing safety for all road users by permitting the establishment of a shared exchange of information platform among vehicles and diverse vehicular networks. IoV is now attracting a lot of interest from academics and business. This article proposes a new network architecture for the future network with faster data throughput, reduced latency, improved management of excessive messages, and huge interconnectedness in order to aid relevant research.

1.7 Research Objectives

The main objective of research questions are stated as follows:

i. To increase the number of hops for message dissemination during emergency message transmission.
ii. To minimize the congestion and latency for sharing emergency packets.
iii. To assure cost-efficient communication between vehicles and the central server.

1.8 Scope of Research Work

IoV has been implemented in various aspects such as energy, health, industry and even furthermore in transportation management in developed cities. Every application has unique purposes and aims to give different services depending upon on what any user requires. The classification of IoV applications is reliable in its domain. Intelligent transportation systems (ITS) aim to gain better traffic efficiency and provide safety procurements against road disasters. Vehicles interact with each other by sharing about vehicles regarding traffic scenarios and circumstances across road. Vehicles must share emergency messages with the vehicles which are attached with each other's and connect each other via communication messages in order alleviate the condemning situations timely. For this purpose, researchers have demonstrated many techniques, but these are only to a restricted level.

The proposed solution is to manage the immoderate number of messages by adjusting their probabilities based on real-time scenarios. It uses a maximum of three hops for emergency message dissemination. It involves a V2V and V2I mechanism, which helps lower communication costs. EEMS objective is to broaden the efficiency of emergency message dissemination, reducing the risk factor of road accidents and obtaining high information coverage. The proposed approach is dynamic and deliberates real-time scenarios with multi-hop communication. This method provides reliable communication while reducing congestion and latency.

1.9 Thesis Organization

The rest of thesis is systematized as follows:

Chapter 2 provides a literature review and describes detailed background knowledge to emphasize each emergency message dissemination mechanism's benefits and drawbacks.

Chapter 3 presents methodology for our proposed scheme. To begin, we provide an operational framework in which we address the analysis, design, and development of our proposed scheme, as well as performance evaluation phase. We also go through some of the assumptions and constraints.

Chapter 4 offers detail of efficient management of excessive messaging for emergency scenarios in internet of vehicles (EEMS) protocol along with an algorithm for EM dissemination that accomplishes the excessive amount of messaging as per diverse vehicle types. It also contains the systematic procedure in flow chart that designed to show how our proposed solution works in the context of IoV.

Chapter 5 presents the proposed scheme's results and analysis, as well as a performance evaluation of the developed protocol, and employ simulation to evaluate our strategy and explain the consequences.

Chapter 6 provides an overview of contributions as well as recommendations for further research.

CHAPTER 2

LITERATURE REVIEW

2.1 Overview

Many types of research in industry and academia have been carried out to improve information distribution and message congestion avoidance for the IoVs throughout the last decade. Most of these techniques have attempted to overcome well-known issues such as redundant transmission, broadcast storm, message congestion, and repetition rate in such works. It occurs because of repetition and results in information loss. Delay in message transmission is another important element to consider when communicating. The majority of solutions used static or restricted dynamic techniques, which are not always suitable. This section discusses emergency message distribution and congestion avoidance techniques, as well as their limitations. These techniques aimed to disperse emergency alerts to the network and minimize message congestion for dependable communications; however, they have a number of drawbacks. Based on the wireless technology utilized, these schemes may be classified into three groups: (i) DSRC-based Data Dissemination (ii) LTE-based Data Dissemination (iii) Hybrid Data Dissemination. Alert messages for vehicle accidents prevention must meet strict timing and reliability standards to be effective. As a result, any communication issues that may obstruct VANET's ability to disseminate information must be carefully examined. Because broadcast storms have a detrimental effect on information transmission to all willing to participate vehicles, we have listed previous and current initiatives to rectify the issue, as well as potential enhancement prospects, to set the stage for our study assumptions. In this chapter, we study and assess existing IoVs message transmission systems, as well as the need for more advanced broadcasting protocols.

2.1.1 DSRC-Based Data Dissemination

DSRC-based Data Dissemination, which relies entirely on direct short-range communication technology for short-range vehicle communication among vehicles and thereby avoids the use of road infrastructure. The IoVs is used in road protection through emergency message delivery, which assists car drivers in making informed decisions on the road. Although malicious nodes may cause problems, especially on highways, trust organization is vital for removing harmful nodes from the system. It examines diverse groups amongst the nodes in the system founded on group undertakings and welfares, imparts emergency signals skillfully. Fabi et al.[23], proposed an innovative nature-inspired forest fire prototype for selecting the smallest number of transmitter nodes in a system for emergency message distribution and this model compared the extent of emergency information in a system to the development for forest wildfire, and it used forest fire model to determine the important parameters for message transmission. Finally, the proposed system decides whether it should convey the signal based on the reliance value of nodes or not, should be influenced by behavioral characteristics. As a result, any nodes having a lower trust score by detached from the network might be classified as hostile and ultimately. Research showed that the method was particularly robust toward a range of system situations and that chosen least number of distinct nodes was fit able to broadcast the emergency message all through the network. The proposed methodology for choosing particular nodes to reliably relay emergency alerts across vehicle networks is described in this paper. The broadcast of timely catastrophe caution notification is crucial for road welfare in a highway scenario. A forged letter of misfortune, however, could devour negative consequences and undermine IoV's trustworthiness. As it is usually recognized trustworthy signal commencing for an actual node, besides malevolent nodes disseminating phony update through the system, it evaluates the communal integrity of each node. In case of any road crisis or disaster incident, information should be transferred to other automobiles using the most trustworthy nodes capable to expeditiously and competently allocating the information. Community segregation based on social resemblance and social concerns is the first and most important phase in this trust model. The next phase is communal-based propagation of the information assigned for every node. Lastly, this prototype uses behavior to predict node trust scores, that are capable to retained and documenting the trust vector T=T1, T2, ……..Tn. Consistent apprises for all phases and nodes along with trust values, under the pre-defined threshold are removed from the community. This exemplary prototype is made up of numerous nodes, such as automobiles, many IoT nodes, and RSU, as well as three stages: societal public parting, essential nodule and complimentary nodule assortment, and node confidence administration. All of these tasks are rationalized recurrently. The distribution of emergency messages adds another layer to the IoV network, preventing road fatalities. Therefore, a malicious node's phony emergency notification in the network can result in a traffic accident. Phony information broadcast through systems could be inadequate to approximate degree if we can establish a confidence that can effectively tackle internal attacks. It would like to investigate multiple communities with various types of nodes in the future.

In [24], the authors suggest an Effective Emergency Message Dissemination Scheme (EEMDS) for urban vehicular networks. It is vital for road safety to distribute Emergency Messages (EMs) to as many vehicles as possible while maintaining minimal latency and packet loss. The difficult problems include evading the broadcast storm and coping with huge EM propagation in urban vehicular network, particularly near junctions. In a dense network, the challenges become significantly more difficult. To eliminate network latency and creating a steady structure of data, the strategy is based on mobility measurements. Cluster head is in charge of managing cluster members and regulating EM dispersion in each cluster. For picking a good cluster head, each vehicle considers its route angle and route harm factor. Furthermore, it uses predicted link stability to choose suitable relay vehicle, reducing the number of rebroadcasts and network communication congestion. As indicated in Figure 2.1, nodes in the EEMDS are categorized as Unregistered Node (UN), Cluster Head (CH), Cluster Member (CM), or Gateway (GW).

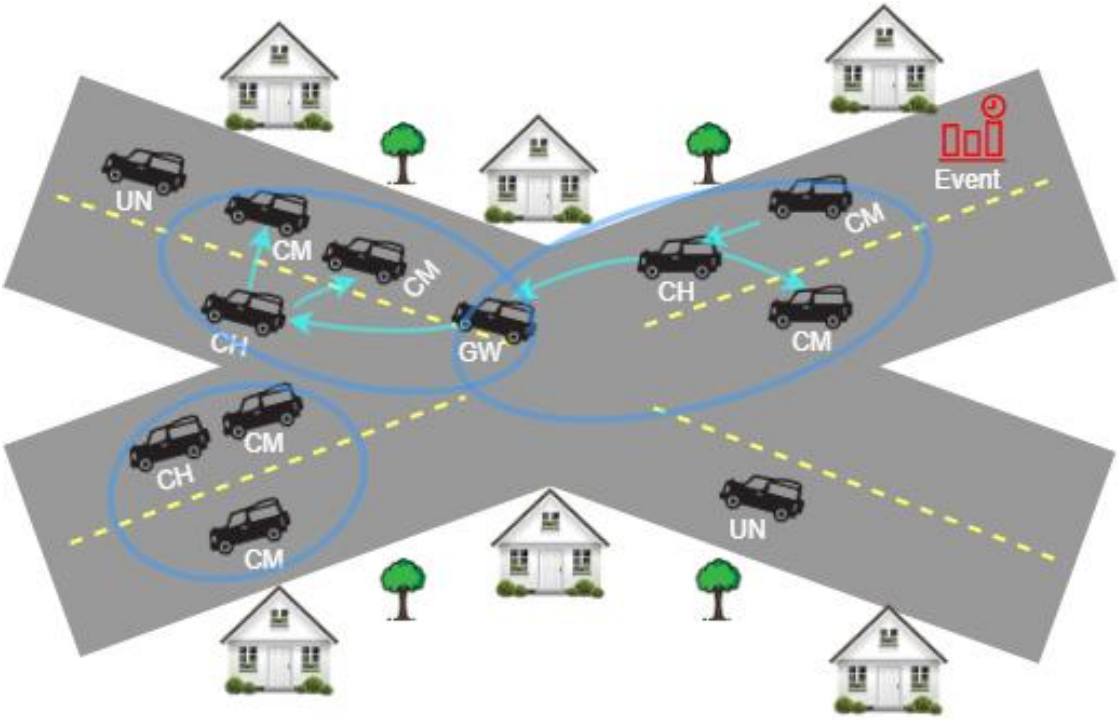

Figure 2.1: Effective Emergency Message Dissemination Scheme

SathyaNarayanan et al.[15], proposes the Sensor Enabled Safe Vehicular Communication (SSVC) protocol, which allows for safe and reliable communications. Traffic congestion, increased travel time, increased CO2 emissions, and parking challenges plague today's transportation systems. As a result, the development of a smart and sustainable transportation network for improved communication has become a need. Advanced technologies have always been created to aid information and regulate traffic flow during transmission. Furthermore, phones, mobile services, edge computing and cloud are all used to build the automobile ecosystem. The primary hurdles include smooth vehicle sensor interoperability, cloud and edge computing coexistence, and edge data storing techniques. The study's objectives are to minimize communication overhead and enhance network communication efficiency. Initially, a network of n vehicles is constructed, and neighbor discovery is carried out using the Wireless Access in Vehicular Environment (WAVE) protocol. Throughout this phase, vehicle location data is used to build the neighbor table. It is used to create the topology of the network. The vehicle's sensors are used to determine its present location, equipment pressure, and vehicle speed. The gateway is picked once the sensor values have been collected. The gateway is where the vehicles are registered and a exclusive ID and password are generated. The cloud connection might also be used to analyze information and spread emergency signals to all vehicles, together with ambulances and retrieval vehicles. Moreover, using a blowfish technique prevents data from being tracked in the cloud by unauthenticated users. The following are the key reasons for allowing cloud-based communication in this project: i) It is sufficient and capable of dealing with a huge quantity of nodes. ii) Whether it is centralized or decentralized reliant on its network connectivity. After registering the vehicles in a gateway, the network's cloud connection is activated to send emergency alerts. As a result, it is vital to ensure the security of congested roads vehicle (V2V) communication. Access to automotive parts is regulated via physical components and keys in this case. Message broadcasting is used to supply motorists with emergency information, weather updates, and traffic updates. The network terminals difficulty and broadcasts storm occur due to the high amount of simultaneous communication. The multi - directional broadcast is hampered by the sender's changing position and region. As a result, it is critical to pick the right vehicle at the right time to send out a message. Before distributing the emergency message to other vehicles, the gateway is selected and the cloud connection is activated in this process. It effectively boosts by the propagation speed and message transmission. Transmission latency is defined as the period it takes for an information to travel from sender to receiver, as given in equation 2.1.

$$Transmission\ Delay = TR - TS \qquad (2.1)$$

The time when the recipient receives the message is *TR*, and the time when the sender transmits, it is *TS*. Experiments have been carried out, and the proposed SSVC approach's simulation results are assessed using a variety of assessment metrics, including as PDR, latency, throughput etc. It is also based on earlier ways in order to demonstrate how effective the new scheme is. According on the comparison, the proposed SSVC surpasses existing systems by quickly and effectively saving vehicle data on cloud. The following are the primary benefits of this work: Improved communication efficiency, minimize latency and improved security. Furthermore, the proposed method for broadcasting messages has restrictions, for example no error correction in the system with sensors and OBU, which decreases process period greatly.

To make optimum use of channel utilization, a clustering and warning message priority technique [25] deliberates inter-cluster and intra-cluster clock synchronization.

Messages are categorized into three categories: message kind, severity degree, and direction. The distance determines the CH election. A medoid node is picked as a CH from a collection of automobiles. Using a clustering method, the proposed methodology increases channel use and decreases communication. The proposed schemes' performance is dependent on the cluster's stability. A cluster head is chosen deprived of considering flexibility. One of these variables is speediness. Because the cluster head varies regularly, there is additional communication overhead.

To circumvent the transmission flood while minimizing transmission delay, a clustering and position-based approach [26] is presented. The probability of effective broadcast packets, interest compatibility and channel fading are all factors in CH selection. The emergency messages are sent by CH to the vehicle coming from the other direction of the present cluster. After receiving the emergency alerts, each CM transmits to the CH. A CM is chosen by the CH to send a message. A cluster member on its own basis cannot send the message. Because the communication is routed to the CH first, the CH chooses a CM to deliver the acknowledged message, causing latency. Furthermore, probability-based systems add unnecessary latency and communication cost for selecting message sending vehicles and CH.

Due to the excessive surge in the petition for transportation mechanisms devices all around the world, the world is seeing a high compactness of automobiles on the main roads, increased road congestion, and catastrophic road traffic accidents. Broadcast techniques are typically used in safety applications to exchange status signals in VANETs. The dependable and on-time transmission of safety signals is important in VANETs that need very efficient transmit models. Sattar et al. [16] developed a broadcast scheme trustworthiness model for information distribution. The likelihood of successfully delivering a message towards its intended end point before the communication's life period expires is described as reliability. Sending the safety warning after its expiration date may be ineffective. The study enables end-to-end dependability in a multi-hop VANET by employing restricted flooding, in which messages are deleted based on two performance measures: packet loss probability and hop count. The proposed protocol's reliability model is based on the chance of receiving a safety packet successfully. The single-path and multi-path dependability models are determined by the protocol. When end-to-end communication and multi-hop VANET are allowed on experimental simulation tools, the network's performance increases. The proposed model compares flooding reliability to packet loss risk and hop count. This technique may be used to increase flooding efficiency. The analytical findings reveal vital information regarding the flooding process. For example, if a given threshold amount of packet loss probability is reached, dependability diminishes rapidly. Second, if not handled properly, the influence of hop duration on dependability can be disastrous. Given the importance of energy-efficient protocols in the forthcoming IoVs, it demonstrates that under the same reliability limitation, restricted flooding is more efficient as compared to plain flooding. Flooding dependability is evaluated in terms of hop count, node degree, and route count. It demonstrates how a network design with a short hop length may help improve dependability. Flooding has become one of the easiest message dissemination strategies since it does not need any routing states on intermediate nodes, but it has low packet distribution dependability in huge scale systems. Future research develops safe zone flood dependability models and compares them to plain flooding, as well as runs simulations to check the effectiveness of safe zone floods to reduce energy consumption and achieve dependability. It also includes the adaptation of well-known dependability techniques for safety message transmission to multi-hop scenarios and the evaluation of their mutual performance. The disadvantage of this strategy is that it consumes more bandwidth by flooding emergency data.

Touil et al.[27], proposed dynamic clustering with a passive approach. The two primary forms of communication that VANET supports are V2V and V2I. Use V2V to get vehicles to work together to improve road traffic safety. The most difficult task is addressing the overhead and stability difficulties produced by the large quantity of messages sent by vehicles in vital regions such as junctions. The authors concentrate on the development of a disseminated system using a passive data distribution strategy. This requires every vehicle distributing other vehicles in almost the same signal range and cluster frequent readings of its position and speed. This suggests that the network was partitioned into virtual subgroups previously in order to comfort message handling and information transmission. Dynamic clustering with a passive approach is essentially a technique for dividing a collection of automobiles into virtual subgroups named clusters. A vehicle identified as the cluster head manages every cluster. Each CH is chosen based on a set of criteria that must be met in order for stable clusters to develop. Clustering enhances network steadiness and data delivery. Thus, this intends to ensure higher stability and strong data transmission in order to enable an improved communication method among vehicles for more well-organized supportive collision threatening utilizing passive method. The goal was to improve a cluster structure more stable so that more traffic data could be delivered to evade collision. The initial simulation outcomes demonstrate that the number of missing packets is greatly decreased when compared to traditional dissemination and other algorithms. Usage of linked automobiles and infrastructure may make Vehicular Ad-hoc Networks a reality one day. The limitations of this work were transmission interval, position, and speed accuracy.

2.1.2 LTE-Based Data Dissemination

LTE-based Data Dissemination, which intends to convey emergency messages to interested organization using vehicle-to-infrastructure communication. Due to the fast movement of vehicles on highways and the influence of velocity on data transmitting in the created system, efficient communication, and network monitoring in IoVs are extremely tough tasks. This research emphasizes the critical need for a systematic and efficient method for adjusting parameters of routing protocols and clustering. In [21], the authors presented a clustering-based modified ant colony optimizer for the IoVs (CACOIOV). This method is intended for IoV networks whose topologies are constantly changing, resulting in network instability. To achieve accessible and steady topology in heterogeneous IoV systems, a unique technique is proposed that employs a heuristic multi-objective clustering approach based on the customized ant colony optimizer in two stages. They presented a novel way for intelligently identifying an initial node in the search region in the first stage, and the dynamic evaporation rate method as a unique strategy for balancing the ACO's convergence speed in the second stage. To keep the IoV network connected, the given method uses a novel proposed DA-TRLD method depending on local traffic density. In terms of latency, packet delivery and loss ratio, cluster number, and throughput, the findings are good. They were able to achieve their research goals in terms of preventing local optimum difficulties and system dispersion challenges due to the improvement of these innovative concepts. Furthermore, this algorithm clearly exhibits ideal performance in terms of establishing efficient and dependable V2I connections that really are qualitative, as well as confirming trustworthy information transfer to each vehicle. As a result, by designing a reliable and effective method for information distribution, this technology delivers sustainable mobility in IoV highway settings for smart cities. This method ensures that each vehicle receives accurate information.

According to simulation findings, this method performs well in terms of packet transmission ratio, data rate, and end-to-end latency.

The IoV is a technology that allows vehicles to communicate with one another. Because vehicular nodes are typically assumed to be moving, the topology changes on a regular basis. These modifications have major consequences, including flexibility, dynamic topology variations, and routing shortest path. Clustering is one solution to such issues. To emphasis on the reliability of the Internet of vehicle topology, Aadil et al. [17] proposed a clustering method for vehicle systems that rely on the dragonfly optimizer (CAVDO) that takes into account communication range and network traffic bulk. Furthermore, the CAVDO algorithm employs a novel mobility-aware model that increases the dynamic range of transmission. In high density, the CAVDO performed well, averaged in medium density, and struggled in low density. CLPSO, on the other hand, only functioned effectively at very low densities. The simulation findings demonstrate that CAVDO delivers the least number of clusters depending on the current channel state in many circumstances. The simulation is run to see how well this method performs in terms of cluster collection and dynamic broadcast range choice with fewer clusters. In the existence of many nodes and cluster establishment time, this approach is compared to current algorithms. The approach provides a longer transmission range while consuming less time. In terms of clustering and re-clustering time, the results are better. The IoV environment, on the other hand, is based on high flexibility, real-time applications, and dynamic topologies, so the forecast aspect for data routing isn't as precise.

In a vehicular network, Feng et al. [18] established the Safety Message Broadcast Strategy (SMBS). The authors conducted a study on reliable data transfer using a hybrid strategy, which has less reliance’s on traffic density and fixed access points. The best forwarder is chosen to send the safety message. The best forwarder is chosen depending on each vehicle's priority, the authors analyzed several parameters such as connection reliability, channel quality, and signal intensity. In order to send safety information to every neighbor vehicle, the vehicle with highest priority sent a safety notice to the vehicle next to it. In the automobile context, their proposed solution eliminated the problem of the competing channel and unneeded data. This method, however, suffers from significant packet loss.

2.1.3 Hybrid Data Dissemination

Hybrid Data Dissemination that incorporates V2V and V2I communication. The edge (infrastructure) intelligently delivers information to the vehicles and uses the vehicle system to distribute the information in a hybrid information distribution model with both V2V and V2I distributions that decrease traffic on the edge. The Internet of Linked Vehicles has made driving vehicles more secure and relaxed. This technology allows for a reduction in road fatalities; nevertheless, growing traffic and environmental uncertainty appear to be barriers to enhancing environmental safety. In [28], the behavior of drivers is examined in order to provide individualized support and to inform nearby vehicles in the occurrence of an urgent situation. The process of this paper is that if the car driver present status is determined to be an emergency, a signal over time is sent to all nearby vehicles in that region as well as adjoining places based on the traffic flow using JSO. If a fog node is not available in a nearby location, a virtual fog node is created by using a constraint-based quantum entropy function to distribute alerts with extremely low latency. A multi-attribute utility prototype is used to provide customized services to the driver depending on behavior analysis, and thus attempting to prevent road accidents. The main purpose of this approach is to reduce road fatalities by connecting vehicles and assessing driver behavior in a real-world setting. The driver's conduct is considered in order to provide intelligent driving assistance. A warning message is given to any nearby vehicles that are in close proximity to a vehicle that poses a threat. The key parts of road safety provisioning are driver behavior analysis and vehicle motion prediction. For IoCV contexts, many research projects have focused on road safety and accident prevention. However, present research on accident detection focuses on either behavior analysis or motion prediction. Driver behavior, in particular, is assessed solely through the detection of vehicle attributes and road data. In the field of driver behavior analysis, the following research issues arise: The prediction of accidents is inaccurate due to a lack of consideration of characteristics from the driver and surroundings, resulting in excessive traffic congestion in both urban and rural locations, as well as re-routing of neighboring vehicles. The author focuses on analyzing driver behavior, sending alert signals to nearby vehicles, and aiding the driver. The proposed project is divided into three tiers, as shown below. Layer 1 (connected vehicles): This layer is made up of intelligent connected vehicles with onboard sensors that acquire data including speed, longitudinal acceleration, yaw angle rate, gyroscope data, and magnetometer data. Layer 2 (fog computing): This layer is made up of dispersed fog nodes that are in charge of monitoring and managing different Layer 1 regions. Layer 3 (cloud server): This is the topmost layer in the design, and it consists of a cloud server that collects and keeps the data provided by Layer-1 and Layer-2 devices on a continual basis. All of these layers work together to assess driver behavior and provide the driver with customized support. The decision to send out alarm signals is based entirely on the driver's present state, which is assessed as driver behavior. The JSO Algorithm is used to spread signals to relay vehicles based on variations in the typical range of longitudinal acceleration. Bad steering is defined as the improper use of steering, as evidenced by abrupt changes in the orientation of the base of mobility, movement direction, and common distance. To safeguard the environment, a fog node delivers an alert signal to all targeted vehicles. Furthermore, the technique is utilized to find the best fog node that is closest to the area that requires this information in order to warn the region. The jellyfish search works in a similar way to how jellyfish choose a hunting place based on the quantity of food available. The direction of the associated unsafe vehicle, which is found as given in equation 2.2, is used to distribute alert messages [28].

$$md = \frac{1}{n_v}\sum md_i = \frac{1}{n_v}\sum(l^* - a_t l_i) = l^* - a_t\sigma \qquad (2.2)$$

The entire population around the vehicle is denoted by nv; the current best location is denoted by l^*; the attraction factor is denoted by at; and the mean position of all vehicles is denoted by σ. The difference between l^* and σ is denoted by the letter dl, which can be written as given in equation 2.3.

$$dl = \delta \times \alpha \times r^f(0,1) \qquad (2.3)$$

The distance of $\pm\alpha\delta$ is defined as the region of probability in which messages are dispersed, where α is the standard deviation and can be represented as given in equation 2.4. Equations 2.4 to 2.8 are taken from [28].

$$\alpha = rand^{\lambda}(0,1) \times \sigma \qquad (2.4)$$

Where

$$a_t = \delta \times r(0,1) \qquad (2.5)$$

So, we use the equation 2.5 instead of a_t in equation 2.6.

$$md = l^* - \delta \times r(0,1) \times \sigma \qquad (2.6)$$

Every jellyfish's new location is estimated as given in equation 2.7.

$$l_i(t+1) = l_i(t) + r(0,1) \times md \qquad (2.7)$$

We use the equations 2.6 instead of md. The following changes can be made to the equation above, as given in equation 2.8.

$$l_i(t+1) = l_i(t) + r(0,1) \times l^* - \delta \times r(0,1) \times \sigma \quad (2.8)$$

The distributive coefficient δ > 0 is related to md in this case. The JSO undertakes two types of distribution: passive and active dissemination. A message is only sent to vehicles in that cluster under passive dissemination. The message is spread to other vehicles based on objective functions in active dissemination. Effective clustering reduces motion prediction error. By analyzing driver behavior, a low number of alerts can be achieved. Effective tailored assistance allows for a large number of high-risk maneuvers. This also raises the score for safety. By executing assistance generation and driving behavior analysis in the fog layer, latency based on the number of vehicles and fog nodes is decreased. The efficiency of alert information sharing is improved by employing the JSO algorithm to distribute messages efficiently. However, the proposed DBA-PA approach has addressed security concerns during efficient V2V and V2X communication. Using the DBA-PA model, road safety is improved in terms of minimizing latency, maximizing resource availability, lowering calculation overhead, and reducing transmission delay. The proposed DBA-PA model may be improved in terms of security in the future by incorporating message encryption between V2V and V2X communication, as well as employing block-chain technology for increased safety.

Deviet.al in [22] has introduced the Adaptive Scheduled Partitioning and Broadcasting technique (ASPBT) is employed for information dependability with the transmission power automatically changing the segments and beacon to decrease retransmissions. When an emergency message is broadcast on the road, it presents a slew of problems, including dependability, latency, and scalability. In the VANET, beacons are used to deliver messages and collect data from neighbors. A network congestion happens when many automobiles broadcast messages at the same time, resulting in message delivery failure for the vehicles. The emergency message has a short latency, and the message's redundancy is decreasing. ASPBT includes the forwarding of new messages with the choice of the optimal partition. For prioritizing emergency communications, the message prioritization approach is utilized. All communications are prioritized based on their desires. Priorities are then assigned to messages based on information priority and distribution distance in order to maintain message QoS. An adaptive scheduled partitioning and dissemination strategy depends on the space between adjacent nodes along with the system density presented for detecting the divider that spreads the emergency message first. Network density determines partition size, and the Black Widow optimization algorithm evaluates transmission plans for each division. The objective of this technology is to transfer messages without delay, to address hidden difficulties and to terminate the network during storm broadcasting, and thereafter transfer information in both directional and uni-directional traffic load. In density simulation, the proposed ASPBT network with black widow optimization approach performs well. Message retransmission and message latency are reduced as a result. This solution employs an adaptive scheme to minimize beacon congestion in order to mitigate the storm problem during transmission.

Azzaoui et al. [29], introduced Dynamic Clustering strategy, to cope with the broadcast storm issue. The author of this work is targeting disseminating issues of an emergency message to all vehicles. The IoVs is a modern form of vehicle system with the objective of enhancing both road safety and user ease. In this case, forwarding emergency alerts via vehicle-to-vehicle communications (V2V) is crucial for road safety-related applications. Forwarding this information in real time in emergency conditions, such as if an accident happens, can assist to avoid traffic congestion sand other tragedies. Therefore, disseminating an emergency message is a big challenge. A new cluster head selection method is included in this scheme for controlling broadcast storm problem. This approach not only allows for the selection of the most reliable vehicles as cluster - head, and thus their employment in emergency message broadcast, and that eliminates network congestion. This technique decreases packets collisions and broadcast storm difficulties while enhancing packet delivery ratio, and data rates.

In [30], because the purpose of warning signals in VANETs is to prevent accidents, they must adhere to strict delay restrictions. However, in high-traffic metropolitan areas where message transmission is hindered, reliable distribution techniques employing the common dedicated short-range communication (DSRC) protocol, like straightforward broadcasting at every vehicle, endure because the radio channel is at danger of becoming overcrowded. A broadcast storm is a regular event like this. This difficulty can be overcome by grouping cars and employing Cluster Masters to coordinate their communications, resulting in a reduced percentage of vehicles that are informed, especially in metropolitan areas where DSRC channels are frequently blocked. This study presents a novel mixture of Cluster Forwarders, which seem to be vehicles chosen to assist in the transmission of communications around barriers, and a fifth-generation phone system as just the V2I technology to expand the range of the communications that have been transmitted. To combat broadcast storms, new procedures using this combination are being developed with the aim of maintaining the proportion of aware vehicles as achieve the highest. The proposed concept involves a VANET that operates in a densely populated metropolitan area with communication impediments. When an accident occurs, a warning message is sent to all neighboring vehicle clusters. The influence of the CF at street junctions is also examined and compared. As projected, CF increases the scope of information delivery to the surrounding neighborhoods while minimizing signal distortions due to the naturally complicated urban surroundings.

A VANET-Cloud layer is presented in [31], for traffic monitoring and the effectiveness of system enhancements in crowded environments. Due to the extremely dynamic nature of networks in congested environments, network effectiveness enhancements are required to predict and transmit trustworthy traffic information. Although numerous ways to data transmission in vehicular clouds have been developed, they all rely on data dissemination from conventional clouds to automobiles or vice versa. However, these systems have not yet defined expecting and delivering information in a proactive manner in response to a query message. The proposed layer for traffic management combines the advantages of a connected sensor network (CSN) for collecting traffic information with cloud infrastructure for providing on-demand and autonomous cloud services. The cloud services supplied employ a traffic prediction technique to address inherent issues with traffic information accuracy, such as modifying various parameters during the forecast process. Furthermore, traffic services employ an information exchange system in which a variety of messages are presented for disseminating traffic data between automobiles and cloud services. Traffic services in this study employ a data exchange method to convey expected data using a fuzzy aggregation technique. Simulation findings show that the presented VANET-Cloud layer may considerably increase highway safety and system performance when contrasted to previous work in the assessment phase. In congested conditions, a VANET-Cloud layer is presented to achieve vehicle safety, traffic updates, and network management. This paper present two distinct forms of traffic services to assure the transmission of databased on the message request or depending on the happening of an anticipated event in the road. For accurate information collection and networks throughput, provide an information exchange method that integrates downlink and uplink data schemes. The proposed architecture aims to improve road infrastructure use while lowering the number of anomalies connected with data detection, network delay, and data quality distributed. In addition, the architecture incorporates networked traffic detectors to record real-time traffic data. It depicts the progression of traditional VANET architectures to a multi-layer services paradigm. The VANET-Cloud layer's possible cloud services attempt to regulate vehicle movement using three data dissemination models: reactive, proactive, and hybrid. Vehicle-to-cloud (V2C) communication is used to operate the proposed models. Each model enables for the interchange of traffic data between vehicles and cloud services, as well as the other way around. The utilization of each distribution strategy, however, is dependent on traffic data given by cloud services. Three main models are used to communicate traffic data: reactive, proactive, and hybrid. Vehicles may require on-demand services and receive, monitor, and collect traffic information due to the reactive data distribution architecture. This methodology is based mostly on a request/response process in which individual vehicle asserts are assessed. The reactive architecture enables every vehicle to update its local information to improve efficiency and dependability on the road. When traffic information affects all vehicles on the road, the proactive data distribution strategy is applied. In the proactive approach, traffic information is broadcast without regard for vehicle needs, and it is supplied on a regular basis. This concept allows vehicles to be knowledgeable of and communicate traffic data such as traffic jams, nearby destinations (stations, restaurants, and parking), forecasted unexpected changes, and road surfaces. The hybrid distribution model combines the preceding approaches, with vehicles collecting traffic data, detecting road events, and collaborating with cloud services to avoid further vehicles from colliding. When an unanticipated occurrence happens, for example, the vehicles transmit an event descriptive message to the cloud services, indicating the incident or congested circumstances. When the cloud services receive this communication, they use the hybrid distribution approach to educate a set of vehicles about the fresh traffic data. The hybrid data dissemination approach provides more flexibility in the simulation stage by incorporating both reactive and proactive models in circumstances where an anticipated event happens. As a result, our simulation tests and findings show that the hybrid model has an impact on the reactive or proactive information distribution model in some way. The data exchange's major purpose is to give a straightforward mechanism for vehicles to keep away from traffic overcrowding, which may be used in a variety of traffic circumstances for the duration of peak hours or when something unexpected happens on the path. As per the simulation findings, VANET Cloud services encourage optimal performance of the network in respect to data delivery, capacity usage, and latency under crowded conditions.

Ryu et al. [32] proposed a mobility prediction based multi-directional broadcasting (MPMB)) approach for both urban and highway Vehicular Sensor Networks (VSNs). The The MPMB method is a single-directional highway transmission system that emerged from the MPDB method. MPMB's primary goal is really to increase transmission efficiency in both urban and highway environments. For this, MPMB use adaptable indicator sectors and the Store-Carry-Forward (SCF) method to choose the very next transmitting (retransmitting) vehicles relying on mobility forecast. This approach is divided into two levels: a mobility simulation phase that tries to predict all neighboring vehicles' Link Available Time (LAT), and a broadcasting level that flexibly chooses the vehicle with the highest LAT method to estimate in the prior mobility prediction level as a retransmitting vehicle for every feasible positional sector.

In [33], presented Dynamic Fog for Connected Vehicles (DFCV),a fog computing-based approach for dynamically generating, incrementing, and demolishing fog nodes based on communication requirements. DFCV is unique in that it provides decreased delays and reliable message delivery even at large traffic concentrations. Author investigated Connected vehicle issues such as inefficient resource usage, increased delays, and regular vehicle disconnecting, particularly in densely populated areas. This exploited two developing paradigms, fog computing and cloud computing, to solve these difficulties in a connected vehicle context. For message distribution, we present DFCV, a fog-based layered system. Fog and cloud computing are two new concepts that are gaining traction. In contrast to earlier techniques, DFCV considers all conceivable situations for spreading signals in a linked vehicular network, including break and combine. The strategies employed in resource deployment and management, involving disseminating messages, differs between DFCV and the preceding approach. To solve the problems, previous solutions employed either cloud computing or mobility in vehicular fog computing to tackle the challenges, but DFCV uses a three-layered architecture that integrates fog and cloud computing methodologies. One-to-one, one-to-many, and many-to-many vehicle communications are all supported by DFCV. The messages are sent out in single or multi hop manner to the designated recipients. DFCV demolishes the fog once a message has been successfully sent. It ensures optimal resource usage; rapid message broadcast, reduced latency, and improved QoS.

The IoV is a wireless network that uses standard Internet protocols and networks to transmit data between vehicles, infrastructure, and pedestrians. It allows vehicles to communicate with one other and with other networks. Essentially, IoVs is made up of thousands of vehicles that are used for various objectives. Vehicular networks ensure road safety, manage traffic via signals, and notify victims of accidents in real-time by exchanging important information. IoVs must work with a limited lifespan and great mobility. IoV is an appealing notion that has to be studied for the benefit of smooth traffic and road safety by overcoming different restrictions such as congestion. Furthermore, IoV-based systems rely heavily on a centralized server to deliver services. A message storm occurs when messages from multiple IoV vehicles are sent to the central server frequently at the same time, causing congestion. It's a difficult problem in the IoVs world that might result in service deterioration as well as other disastrous repercussions. Message congestion is a key issue and a necessary obstacle during communication in IoV. When the same messages are sent out repeatedly, message congestion occurs, which leads to packet loss. Information and EMs are unable to convey immediately due to packet drop, leading to a rise in accidents. Long delays during message dissemination should be avoided for effective communications. Energy-efficient message dissemination (E^2MD) is a fog-assisted congestion avoidance scheme for IoV is designed by Yaqoob, [19]. E^2MD reduces communication costs and manages services. Each vehicle must communicate with a fog server. Fog computing is used in the proposed work because it simulates the use of local servers for calculation and information delivery, and also works in situations where the server is out of the vehicle's range. This system is applicable not just too smart vehicles, but also to non-smart automobiles that do not have access to the internet. Therefore, it helps prevent more real-world accidents, reduced message delivery costs, and message overhead costs. In places with high vehicle numbers, this technique suffers from excessive routing overhead, high maintenance cost and communication delays. However, as future work, they concentrate on determining the wait size during times of congestion. As depicted in the figure 2.2, this network is built on priority and groupings.

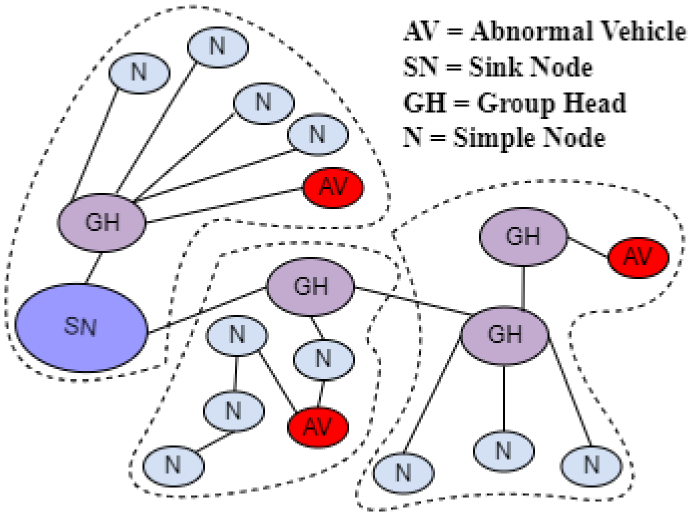

Figure 2.2: Emergency Message Dissemination

Message dissemination with re-route planning (MDRP) technique is observed by Meenaakshi Sundhari et al.[20], that takes into consideration both traffic organization and message distribution. This approach starts a broadcasting boundary to choose neighbors and a heaviness to choose the re-routing pathway. The weight is determined by the road section's traffic situations, as well as the timeout of the emergency vehicle message. The collaborative method of rerouting and information broadcast is aided by reliant queue management, which improves delivery of message and reduces the impact of delayed instances in the travelling path. The visual sensing technique is used to establish the extract distance spanning between the vehicles that is in the emergency and the intersection that happens while setting up an emergency vehicle on traffic. The situation of EV message dissemination is depicted in figure 2.3.

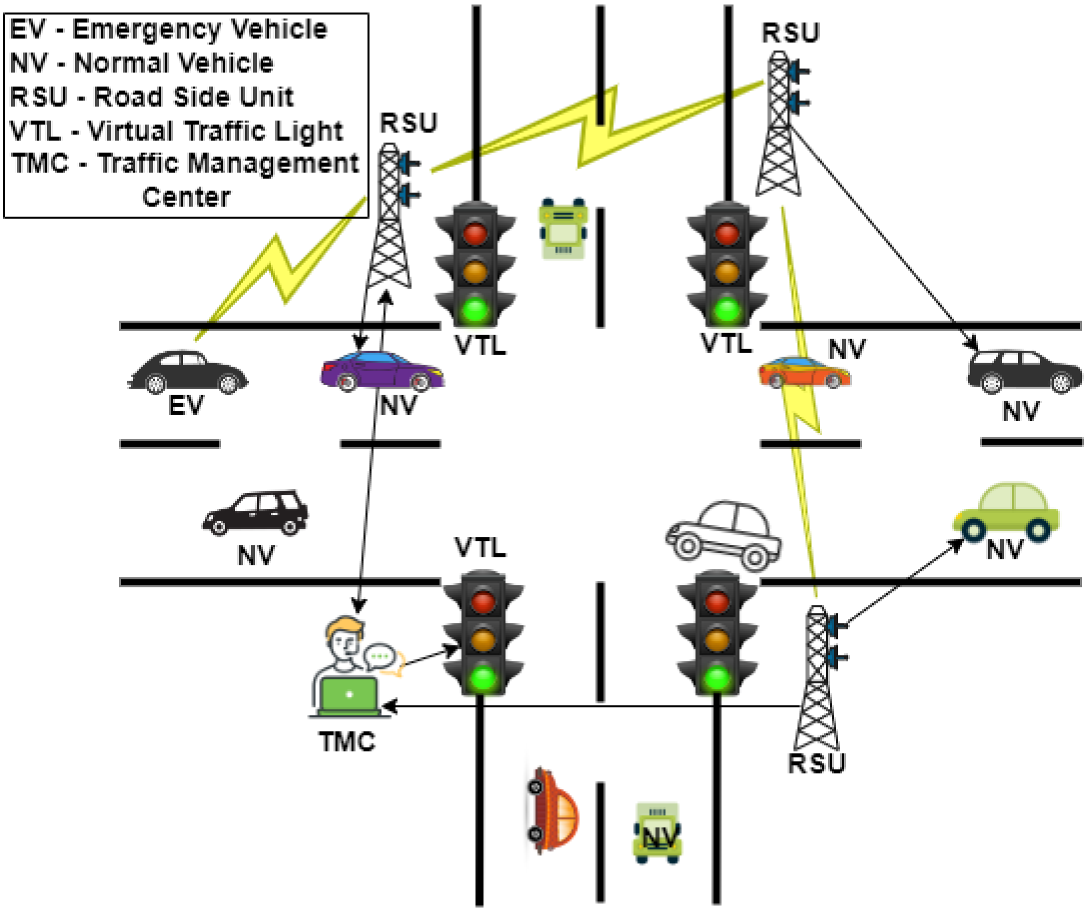

Figure 2.3: EV Message Dissemination Scenario

The roadside unit is used to establish the density of the vehicles. To detect the vehicle's intersection, they used Organizing traffic algorithm in this case. The time is categorized for the complete car on the street that has arrived at a junction. When a signal arrives at the RSU, it is recorded in order to calculate the street weight as given in equation 2.9 [20].

$$W_e = \sum_{x=1}^{n} \text{VW} \ (1) \qquad (2.9)$$

In the equation above, we represent street weight, n represents the number of vehicles on the street, and *VW* represents the time of the vehicle that is in the waiting condition of the previously arriving vehicle. The traffic lights are set on a regular basis based on the weight of the street. The time required to pass through the intersection that follows the lanes on the path, as well as their space, are computed. This study for the congestion-free system also finds the distance between vehicles. The last vehicle and the sender in a specified range communicate using equation 2.10 [20].

$$D = P_s + F_p \tag{2.10}$$

Where *D* is the space between the very last vehicle and the sender, *PS* denotes the sender's location as determined by the Global Positioning Service, and *FP* denotes the final vehicle's position. As seen in equation 2.11, minimum boundaries are also established to promote information transfer.

$$M_B = D - L \tag{2.11}$$

The minimum boundary range limitation for the roadside vehicle is *MB*, the space between the dispatcher and the receiver vehicle is *D*, and the length between the dispatcher and the recipient vehicle is *L*. To reduce waiting instances, the message dissemination method is enhanced with exact neighbor and path selection based on boundary metric, space, and queue. To pick non-congested pathways to the destination, the route of the neighboring vehicle and the compactness of the road segment are pre-estimated based on in and outflows of the road segment. This contributes to a reduction in message broadcast delays and the number of delayed occurrences.

In [34], a safe and privacy-preserving warning message distribution strategy for cloud-assisted IoV is provided. To begin, it uses attribute-based encryption to secure the threatening message that has been sent and provides a verified encrypt and decrypt outsourcing structure to decrease the vehicle's computing expenses. Meanwhile, using anonymous identity-based signature, this approach may protect vehicle identification privacy while still tracing the true identify of harmful vehicles. Additionally, batch verification can greatly minimize the computational overhead of evaluating a bunch of warning signals. This technique has undergone a security analysis and experimental assessment to ensure that it can meet the safety measures and effectiveness criterion of emergency message distribution in cloud assisted IoV.

Dissemination of the emergency message in cooperative vehicular safety applications, Liu et al. [35]presented unique Trust Cascading-based Emergency Message Dissemination (TCEMD) system. This system can easily combine entity-oriented and data-oriented trust evaluations, and it has far higher resilience. One of the most important sections is cooperative safety applications, and a great amount of studies have been undertaken for broadcasting of emergency message in automotive systems [35][36][37][38][39]. When an EM (such as a roadblock) arises, the EM may be propagated in a trust cascade way among surrounding vehicles, entity-oriented trust values have been embraced as vital burdens. Following that, the conceptual examination of the TCEMD prototype's resilience against various types of assaults and malevolent behavior, failed tolerance characteristics, compatibility for many types of unusual scenarios, and inducement systems are discussed. In vehicular networks, trust management is critical because it allows every vehicle to assess the trustworthiness of many other heavy vehicles as well as received messages before taking any action, and a number of trust management strategies for automotive networks have been developed [35][40][38][41][42]. Malicious vehicles make every effort to broadcast false signals in order to deceive following vehicles, whereas fair vehicles make every effort to transmit true messages. As a result, the message of a trustworthy vehicle is more probable to be trustworthy than a malevolent vehicle. A trustworthy vehicle may transmit unreal signals with a possibility of p ($p \in (0,1)$) due to the complicated path situation and restricted awareness and processing capacity. Additionally, because malicious vehicles normally do their hardest to broadcast unreal signals, the likelihood of a malevolent vehicle disseminating fictitious communications is usually greater than p. We use a basic scenario in which the chance of every vehicle disseminating fictitious communications is considered *p*, and every communication recipient takes a judgement using the traditional majority voting approach. The correlation between the right choice probability (written as *P*) of a message receiver and the number of unique message broadcasters examined in its decision process (*n*) may be calculated using the equation 2.12 [35].

$$\mathcal{P} = \sum_{i=\lceil \frac{n}{2} \rceil}^{n} C_n^i (1-P)^i * P^{n-i} \quad (2.12)$$

Also, when *p* takes various values, the *p* versus *n* variation curves change. This approach has large computing, communication, and storage overheads, as well as lack of privacy preservation, severely limiting their usefulness.

The IoVs proposes to create a system of self-driving and linked vehicles that can interact with each other, as well as with roadside units and a central trust authority (TA). To save resources and maintain network security, messages must be delivered securely and efficiently. To improve and manage the network, Trueblood et al.[43] uses an interdisciplinary method by combining information analytics and cyber security. To improve network effectiveness in terms of time utilization, the proposed technique adds Prim's method to a current vehicle safety system, Privacy-Preserving Dual Authentication Scheme (PPDAS). Using prims and dual authentication mechanisms, this proposed approach delivers safe and optimal data transport through the network. The period its takings to distribute messages rises quadratically when a double verification security mechanism is used; when Prim's algorithm is used, the period its takings to distribute messages grows linearly. When Prim's method is used to a vehicular network, it improves system performance and reduces message distribution period. Another benefit of Prim's technique is that it allows vehicle networks to scale up. Because of the enhanced efficiency in v2v communication, researchers were able to reduce the overall time it takes to transmit system messages, allowing more resources to be given to other IoV activities and reducing congestion by lowering the amount necessary for a message dissemination technique. This research topic's possible constraints include energy utilization analysis as it pertains to various rules, studying how to maximize power spent per communication as it travels several distances in the system, and a multi-hop re-authentication method for information distribution.

2.2 Comparison of Studied Emergency Message Dissemination Protocols

We examined the emergency message dissemination schemes here to recognize gaps in the current research. We identified the similarities and differences in the schemes presented in the literature. We discussed several schemes and outlined how those papers differ from one another. Moreover, we explored the common mechanisms, advantages, and limitations. Clustering mechanisms are used by [21] [24] [25] [26] [29] [30] where [21] [25] [29] [30] improves throughput. Many of these methods are only used in urban environments [26] [29] [30]. The schemes [18] and [33] improved QoS. The techniques that we looked at in the literature review are contrasted in Table 2.1. We discussed the principles of the schemes and the methods they use, pointing out the drawbacks of the papers and considering the advantages.

Table 2.1: Comparative analysis of several Emergency Message Distribution Techniques

Scheme	Basic Idea	Mechanism	Advantages	Limitations
DSRC-Based Data Dissemination				
EEMDS [24]	• EM distribution to a large number of nodes.	• To pick an appropriate Cluster Head and construct stable Clusters.	• Reduce communication overhead. • High Packet delivery ratio • Achieve high coverage of information	• Not worthy in sparse networks
SSVC [15]	• Enable secure and reliable communication	• Wave protocol, Blowfish protocol	• Secure communication with low latency	• Susceptible to impersonation and Sybil attacks • Reduce data delivery
PDMAC[25]	• EM dissemination using priority technique.	• Clustering	• Reduce delay • Improve throughput • Improve message loss rate.	• Recurrent CH change • Communication overhead
PED [26]	• Forwarder disseminates EM.	• Clustering	• Improve packet receiving ratio	• High Latency • High communication overhead • Need to extend it into highway scenarios.
RMFF [16]	• Emergency message dissemination using flooding technique.	• Flooding	• Overcome the message storm	• Ineffective in controlling repeated

				message transmission.
LTE-Based Data Dissemination				
CACOIOV [21]	• A dynamic nature enhanced technique is used to provide stability among vehicle nodes	• Clustering and Ant colony algorithm	• Improves throughput • Reduce network latency • Boost network scalability	• When simulating a high number of nodes, ns2 uses a lot of CPU and memory.
CAVDO [17]	• Delivered smallest number of clusters	• Mobility aware dynamic transmission range algorithm (MA-DTR)	• High density • High stability • Low latency	• High computational difficulty • Increases packet loss
SMBS [18]	• Transmit safety alerts among vehicles	• Broadcast	• Improve the efficiency of data distribution and coverage area • Improve QoS • Eliminates unnecessary data	• significant packet loss
Hybrid Data Dissemination				
ASPBT [22]	• Transmitting the messages in both directional and uni-directional.	• Black Widow Optimization Technique	• Reduce message retransmission. • Reduce message latency. • Control beacon	• Need to use VANET for secure privacy and safety-related applications.

			congestion.	
EMD-IoV [29]	• Real-time EM dissemination in an urban environment.	• Clustering	• Increase throughput • Reduces Packet collisions and transmission delay. • Increase Packet delivery ratio	• Need to extend it into highway scenarios.
DSRC [30]	• Dissemination of real time emergency messages in an urban environment.	• Cluster Forwarders	• Increase throughput • Reduce transmission delay.	• Need to extend it to highway scenarios.
MDRP [32]	• Broadcast messages in highway and urban scenarios	• Store-Carry-Forward (SCF) method	• High rate of packet delivery • Minimal packet delay	• Need to investigate how to assign and maintain ID shared by all vehicles along the journey.
DFCV [33]	• A fog computing method	• Fog Server-based	• Reduce delay • Improved QoS	• High maintenance cost
E^2MD [19]	• Timely delivery of emergency messages.	• Fog Server-based	• Reduce congestion • Decrease messages overhead cost • Improved message delivery cost • Low node	• Excessive routing overhead • High maintenance cost • Communication delays

			density	
MDRP [20]	• Organizing traffic and disseminating messages	• Re-route Planning	• Reduce transmission delay • Efficient message delivery • Minimize traffic	• High maintenance cost
TCEMD [35]	• Message dissemination among adjacent vehicles in a trust cascading way	• Entity oriented trust values into data-oriented trust evaluation	• Increase road safety • Increase traffic efficiency	• lack of privacy preservation
PPDAS [43]	• Combining cyber security and data science to control message dissemination in the IoV.	• Broadcast	• Increase efficiency of network	• Less throughput

2.3 Research Gap and Directions

We talk about the issues with the schemes that we looked at throughout the literature review. In addition, we offer a remedy to the issue. Finally, we choose the problem that this article addresses in the conclusion.

1) Many of these approached use their protocol only in urban scenario [29][30]. We need to extend it to highway scenarios.

2) In sparse networks, network efficiency suffers [24]. We need to make every effort to overcome this constraint.

3) In [15], there is no error detection method, which increases processing time. This work may be improved by using sensors and OBUs to identify errors in the networks, which cuts down on processing time.

4) In [21], NS2 consumes a lot of CPU and memory when simulating a large number of nodes. It is possible to improve the IoV route by modifying a number of other ACO features.

5) This strategy is unsuccessful when it comes to security issues in privacy and safety-related applications. VANET might be utilize to address these difficulties [22].

6) In [19], vehicle is unlikely to be connected to the RSU at one-hop neigbors. Because of this problem, a lot of surrounding vehicles get into avoidable mess. It may be improved by increasing the number of hop neighbors.

We choose the case of Yaqoob et al. [19], where they employed just one-hop neighbors to discover the nearest RSU for relaying an emergency message, among the challenges mentioned above in several works. However, suppose one-hop neighbors do not discover the RSU. In that case, the message is likely to be lost and not sent to other vehicles in emergency conditions, making the situation extremely dangerous. We expand this one-hop neighbor to 2 to 3-hop neighbors, allowing us to quickly locate the RSU and distribute emergency messages across the network.

2.4 Summary

In this chapter, we looked at a variety of research studies on emergency message delivery. We discussed their advantages, methods, limitations, etc. Many research efforts have attempted to enhance existing emergency message dissemination techniques for automobiles over the internet. To improve emergency message distribution in the environment, we should consider selecting the next hop neighbors efficiently. From this perspective, we proposed an excessive messaging management scheme for emergency scenarios on the internet of vehicles.

CHAPTER 3

METHODOLOGY

3.1 Overview

In this chapter, we present the methodology for the identified problem. The strategy entails modifying the probability of a large number of messages based on real-time circumstances. We go through the operational framework in depth, starting with the analysis phase, then the design phase, the development phase, and finally the performance evaluation phase. We discussed the many measures we addressed in this study throughout the performance evaluation process. Following that, a description of the simulation scenario is given. Finally, we established some assumptions and limits for our proposed scheme, as well as a summary of how it works.

3.2 Methodology

We chose the IoV field and researched an interesting subject. We started by figuring out the topic's nature and locating relevant areas of expertise. Examine the literature to find out how others handled or resolved the issue. We collect literature through the method of a survey of related schemes. After reading various articles, we found a valid problem in the relevant base scheme. We discover an issue in a paper about emergency message dissemination in the IoV. Then, in order to construct metrics for outcome comparison, we review more papers that identify problems relating to the base scheme. We gathered roughly 60 papers of literature and wrote a literature review on 22 papers. We read the method in the underlying paper and searched for a flaw. Then, in the proposed solution, we provide a solution to the issue and enhance the method. Afterward, data analysis is challenging to gather information in a planned and controlled manner to make informed conclusions. The simulation scenario and its associated set of parameters are explained.

3.3 Operational Framework

This operational framework is divided into three phases, as shown in Figure 3.1. The first phase involves the introductory study on the necessity for efficient management of excessive messaging for emergency scenarios. The first phase shares the knowledge of information distribution, communication overhead, message transformation delay, packet loss, and packet delivery ratio in constraints. In addition, the first phase also elaborates on reducing commutation and overhead delay, reducing the packet loss ratio, and enhancing the better packet delivery ratio. The second phase covers a range of issues uncovered during the extensive literature review, as well as the methods required to develop an efficient approach to controlling excessive messages in the IoV protocol for emergency circumstances. The third phase evaluates the performance of efficient management of excessive messaging. The third phase is categorized into two factors: modeling simulation and evaluation parameters. The modeling and simulation consist of network simulator 2.35, and the second is C and tool command language. The performance evolution phase depends on four parameters: packet delivery ratio, packet loss ratio, communication overhead, and message transmission delay.

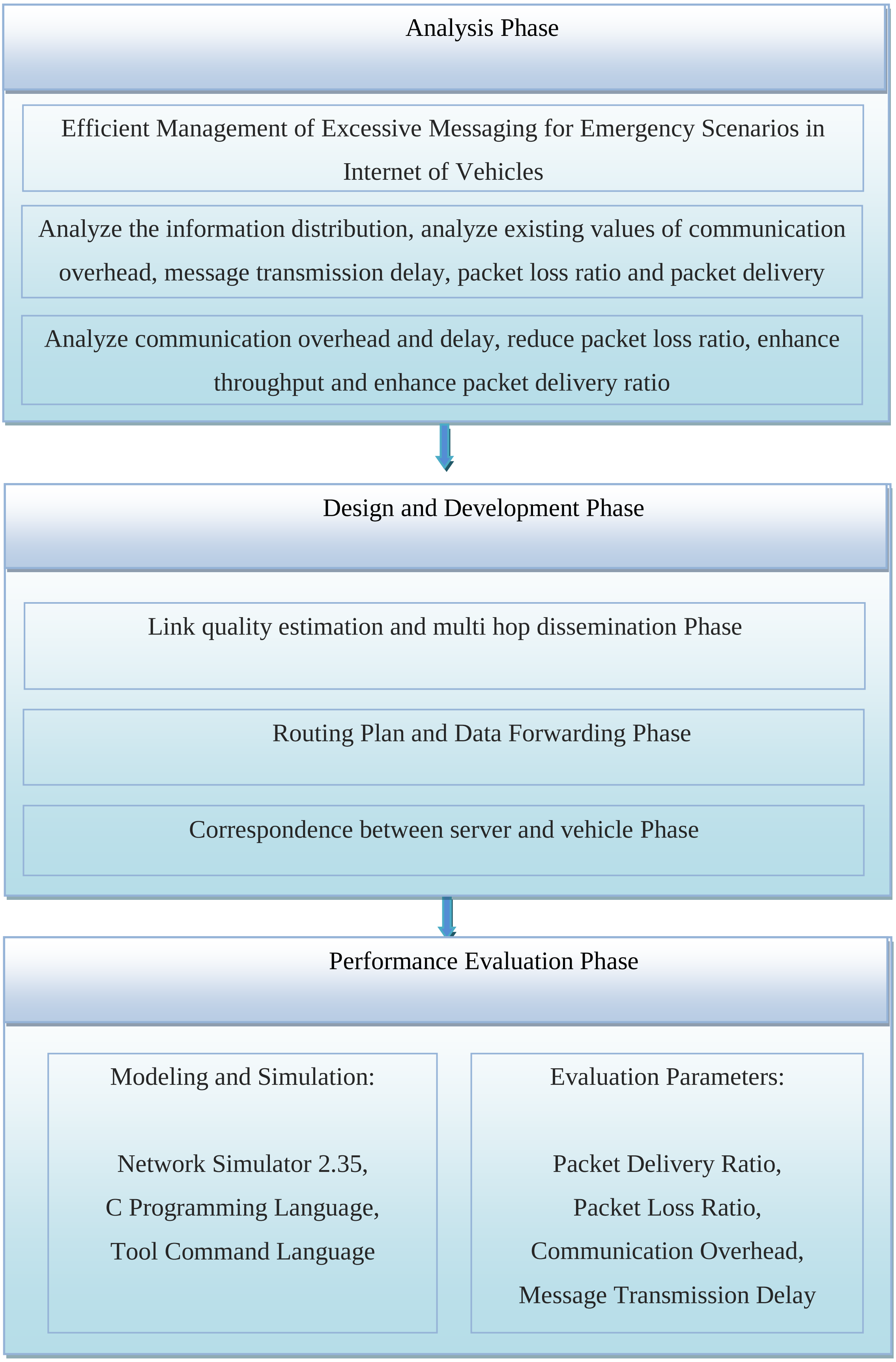

Figure 3.1: Operational Framework of the Research

3.4 Research Design and Development

In this part of the paper, we have enlightened the main objectives of the design and development phase. As it is seen in figure 3.1, we have three phases in the "design and development phase". In order to explain how we achieved the objective in these phases, we collected the literature by initially conducting a survey of related schemes. After that, we identified a valid problem from the base paper with the support of figure. After that, we design the proposed solution in accordance with our objectives after studying the weaknesses of the existing, similar solutions. From this, we derive the methodology that resolved the problem. In the base scheme, we found that the emergency message is sent only to the 1-hop neighbor RSU. There is a high probability that 1-hop neighbors have no RSU, which causes congestion and high communication costs. Figure 3.2 shows the problem statement of our model.

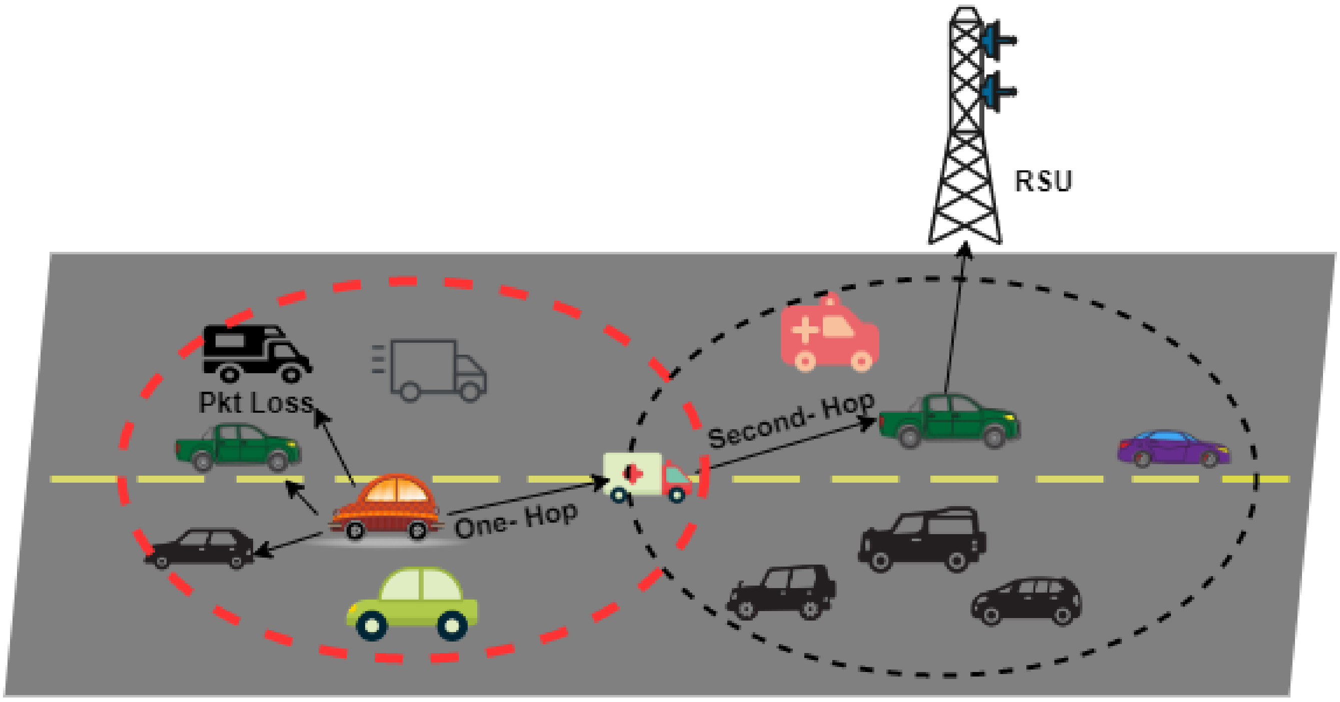

Figure 3.2 Road side unit at 1-hop neighbors

Figure 3.3 provides an illustration of the research methodology plan for the proposed excessive messaging management scheme.

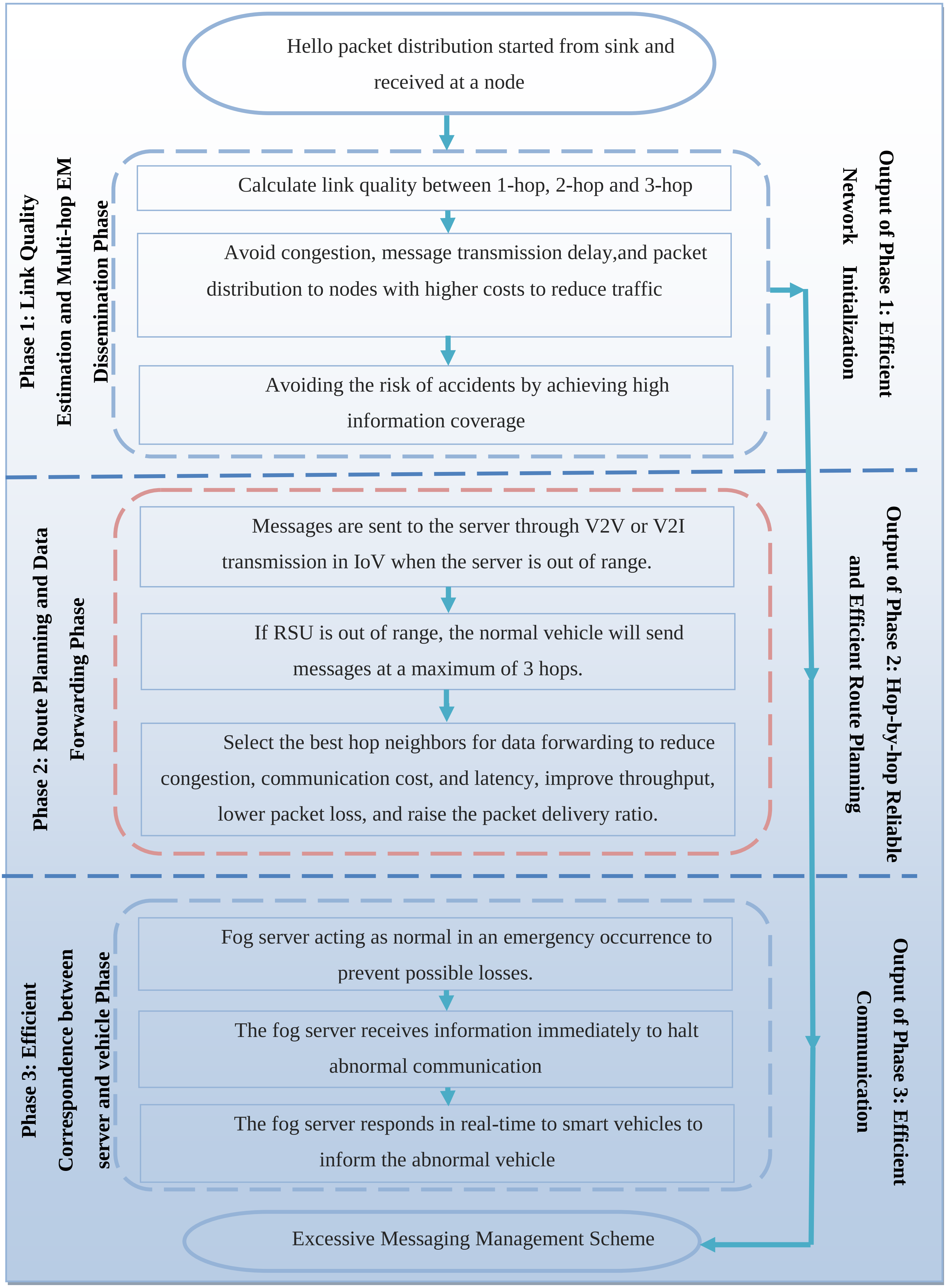

Figure 3.3: Research methodology plan for excessive messaging management scheme

Figure 3.3 shows the phases that are identical to those in Figure 3.1's design and development phase. However, we have opened them up in Figure 3.2 to clarify our process.

3.5 Simulation Framework

For verification of the proposed strategy, we used NS2.35 to run a large number of simulations. For vehicle road segmentation, deployment, and clustering, as well as information initiation, we employed tool command language (TCL). In a similar manner, result extraction from trace files is done using the practical extraction and report language (PERL). Furthermore, the transmit and receive functions are implemented in the C programming language, as are the recommended algorithms.

3.5.1 Assumptions and Limitations

We assume that vehicles would keep a list of one-hop, two-hop, and three-hop neighbors based on their communication range. The limitation is that a realistic environment is created in which all sorts of vehicles, such as Iv, Sv, and Bv, travel according to speed regulations. The communication duration for EMs between vehicles is set at 3 minutes, during which vehicles are expected to send and receive large amounts of data.

3.6 Summary

We provide the methodology for solving the identified problem in this chapter. The technique requires adjusting a large number of messages' probabilities based on current situations. The analytical step is followed by the design phase, the development phase, and the performance assessment phase as we thoroughly examine the operational framework. Throughout the performance review process, we review the several measures we examined in this study. The simulation scenario is then described after that. Ultimately, we establish certain assumptions and constraints for our proposed scheme and provide an overview of our model's operation.

CHAPTER 4

PROPOSED EXCESSIVE MESSAGING MANAGEMENT SCHEME

4.1 Overview

In this chapter, we present the proposed solution to the identified problem. The Fog server manages the excessive messages. It involves a V2V and V2I mechanism, which helps to reduce communication costs. This work provides traffic efficiency; it manages excessive messages, reducing the risk of road accidents and controlling traffic congestion. A flow chart is designed to show how our proposed solution works in the context of IoV. Finally, we explore an algorithm for our proposed model that defines each stage of our model in order. A detailed description is provided for the proposed algorithm.

4.2 PROPOSED EXCESSIVE MESSAGING MANAGEMENT SCHEME

In this section, we present the proposed solution to the identified problem. The proposed solution is to manage the excessive number of messages by adjusting their probabilities based on real-time scenarios. It uses a maximum of three hops for EM dissemination. It involves a V2V and V2I mechanism, which helps to reduce communication costs. EEMS aims to extend the efficiency of emergency message dissemination, reduce the risk of road accidents, and achieve high information coverage. We use the fog server, which reacts to normal and emergency occurrences in order to prevent possible losses. In urgent situation, the anomalous vehicle's urgent notice must be relayed to surrounding vehicles and the reporting server in order to coordinate a timely reaction. Fog servers serve as local servers in a variety of ways. The proposed approach is dynamic and deliberates real-time scenarios with multi-hop communication. Vehicles exchange all types of communications, either normal messages (NMs) or emergency messages (EMs), for ordinary messaging and accident notifications, respectively. These messages provide information such as the vehicle's location, velocity, direction, and other emergency or safety-related information. Based on their communication range, we anticipated that automobiles keep a list of one-hop, two-hop, and three-hop neighbors. Periodic safety (beacon) messages and event-driven messaging are the two forms of important public safety communications. Messages are sent to the server through V2V or V2I transmission in IoVs when the server is out of range of the abnormal vehicle. In the event of an emergency, such as an accident, event-driven messages are sent. In order to transport multi-hop neighbors, this form of communication is regarded as trustworthy. Normal vehicles reach the fog server by roadside units; they send a message to the RSU, which then transmits it to the fog server. If no roadside units are nearby, the messages can be conveyed utilizing the V2V concept through other vehicles. This architecture's primary goal is to offer reliable communication, and our method provides reliable communication while reducing congestion and latency.

If no RSU is available within the normal vehicle’s range, then the abnormal vehicle sends messages to a maximum of three-hop neighbors. These messages reach the fog server and receive a response from it. When the fog server receives information, it immediately contacts that abnormal vehicle to halt communication. The Fog server responds in real-time to smart vehicles to inform the abnormal vehicle. Fog server is regarded as a local server since it quickly calculates the problem and contacts the user. The two-hop and three-hop neighbors’ situations are depicted in figures 4.1 and 4.2, respectively.

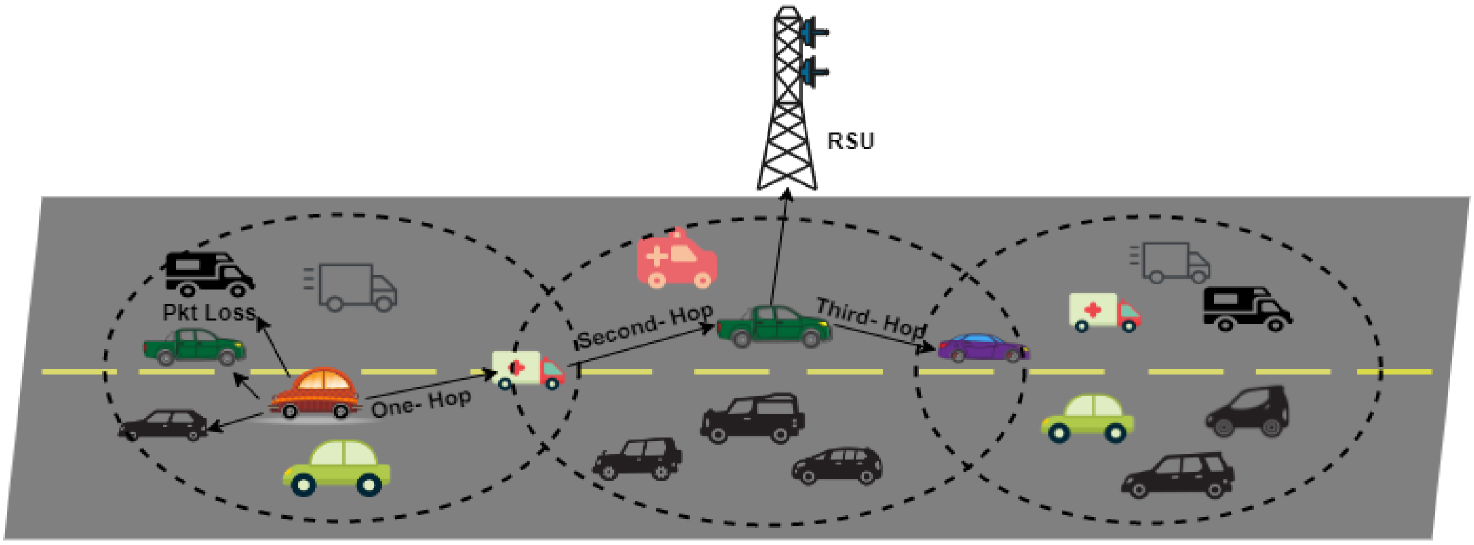

Figure 4.1: RSU at 2-hop neighbors

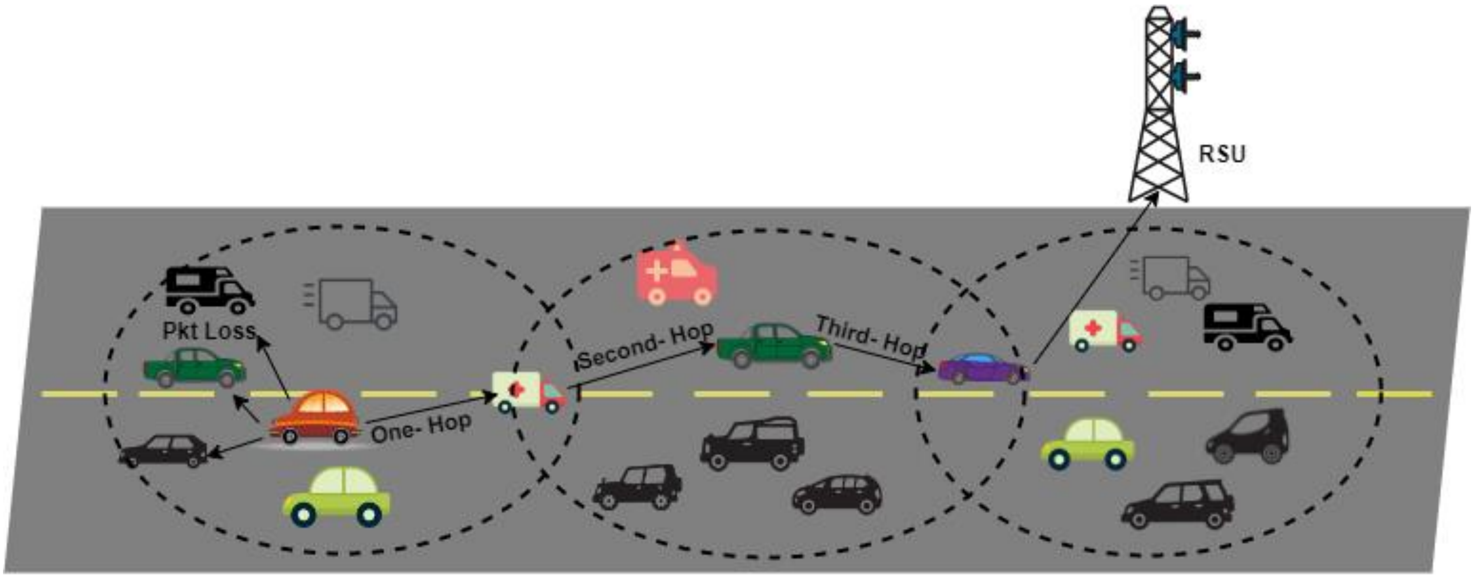

Figure 4.2: RSU at 3-hop neighbors

EEMS takes into consideration three different types of vehicles based on their resource availability and capabilities. The first is an Intelligent Vehicle (Iv) uses sensors connected to the vehicle to identify obstacles and vehicle speed. Using the internet and V2I sensors, it may recognize an accident and report it straight to the fog server. The second is a smart vehicle (Sv) has wireless sensors that transmit data to an application that is either built into the vehicle or connected to the driver's smartphone. It communicates directly with the fog server via the internet. The third one is a Basic Vehicle (Bv) uses V2I communication to send the data. In an emergency, a Sv with weak internet connectivity is also required to serve as a Bv. Due to the lack of an internet connection, RSUs are used in this situation to approach the base station and then interact with the fog server. Both types of vehicles can execute V2V communication in the absence of a nearby RSU until a vehicle approaches that can do V2I communication.

4.3 PROPOSED EXCESSIVE MESSAGING MANAGEMENT FLOWCHART

The following is a description of a flowchart. When an accident occurs, then autoVehFlag and inetFlag are set to 1, meaning internet and V2I sensors are accessible for message transmission, and if both are available, then it selects the vehicle type as intelligent vehicle (Iv). If only the internet is accessible, then select the vehicle type as smart vehicle (Sv), and if there is no internet, then RSUFlag is activated, select the vehicle as basic vehicle (Bv). After choosing a vehicle type, it checks if the vehicle is Iv or Sv and the internet is available. Then the message is directly sent to the fog server. If the vehicle is not Iv or Sv and the condition is false then it means the vehicle is basic (Bv). If the vehicle is $B_{V,}$ then the severe condition flag is activated and checks for the neighbor count of which vehicles have Iv or Sv. Then a message is sent to the fog server through Iv or Sv vehicle and the severe condition flag is deactivated If the severe condition flag is still on, the send message flag is activated, and the search for the vehicle closest to the RSU begins, with a maximum of three-hop neighbors. If any of these 3-hop neighbors finds RSU in a nearby location, it sends a message to RSU using a V2V connection and turns off the send message flag. If RSU is not available in 2 to 3-hop neighbors then SentMsgFlag is turned on and the message is sent to nearest vehicles, which take less time for packet to reach at RSU. This flowchart depicts the correct flow of our model from beginning to end, as well as how the model should be handled. The reader does not have to work hard to understand the model's flow; all they have to do is look at the flowchart.

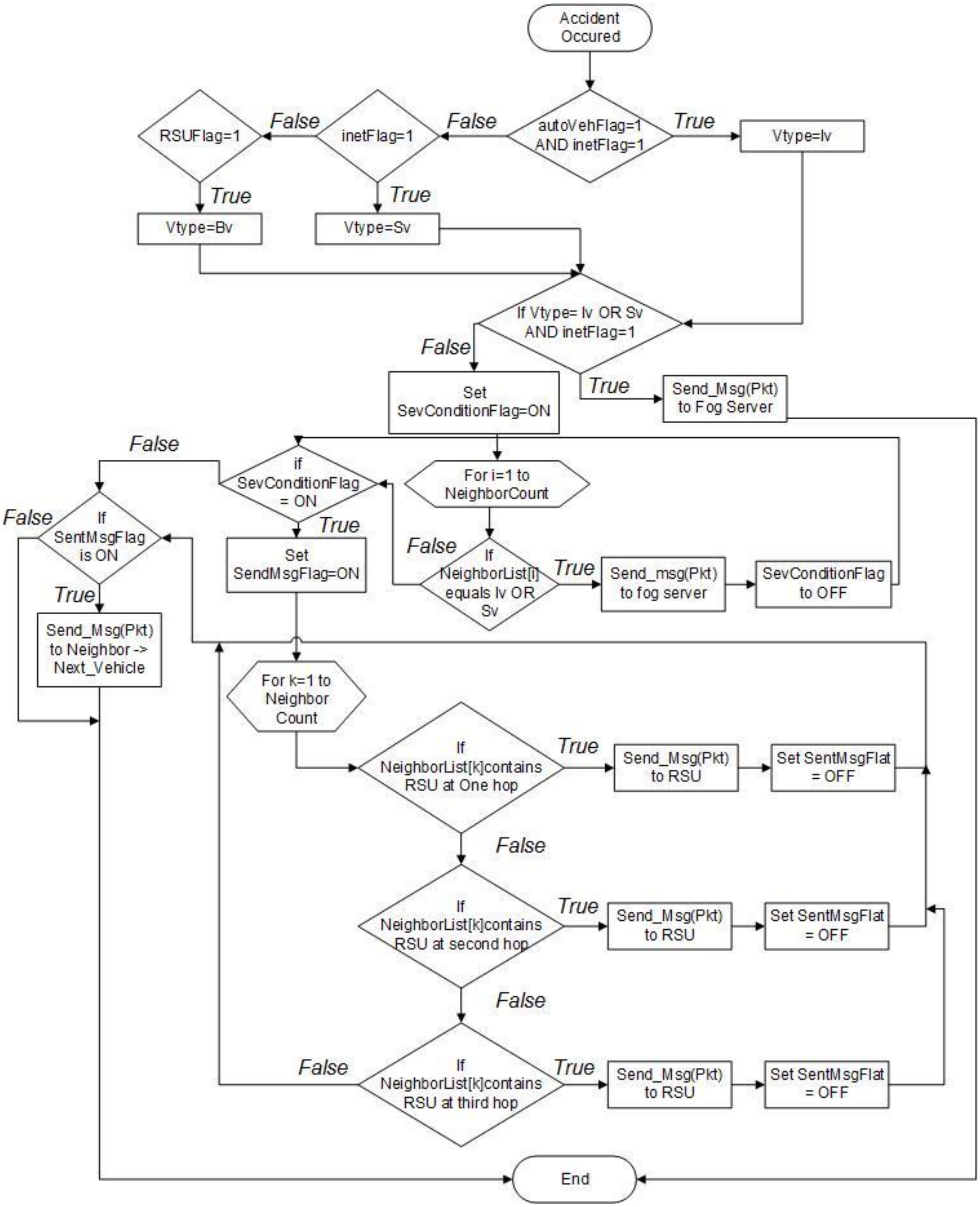

Figure 4.3: Procedural Flowchart of Excessive Messaging Management Scheme

4.4 EFFICIENT MESSAGING ALGORITHM (EMA)

We provided algorithm 1 for dynamically exploiting a vehicle's available capabilities to manage the message. The following is a step-by-step description of the algorithm: AutoVehFlag and inetFlag are engaged when an accident occurs. If V2I sensors and the internet are available for transmitting messages, pick Iv as the vehicle type. If just the internet is accessible and no v2I sensors are present, set the vehicle to Sv. At last, if RSUFlag is enabled, pick Bv to display the lack of internet. The vehicles are chosen based on their main concern, as shown in steps 1–7. If the vehicle is an Iv or Sv and the internet is accessible, send a message to the fog server to contact the rescue team for remedy and to remove any inadvertent automobiles off the road, therefore reducing the number of accidents. If the vehicle is Bv, the severe condition flag is set, and NeighborCount begins counting neighboring vehicles that have Iv and Sv. Then, using Iv or Sv, send a message to the fog server and disable SevConditionFlag, as shown in steps 8–18. In steps 19–36, the severe condition flag is checked, and if it is engaged, Sent-MsgFlag is switched on, and the process of selecting the vehicle to which RSU is closest in one-hop begins. If no RSU is available in one-hop neighbors, the condition checks whether the RSU is close to second-hop neighbors and the same condition applies to third-hop neighbors. A vehicle is found which is closest to the RSU, and then messages are sent to the RSU using V2V connection in this manner. We Deactivate the SentMsgFlag after the message has arrived at its destination. In steps 37–40, if the SentMsgFlag is still on, then the message is sent to surrounding vehicles until it approaches the server.

```
// Accident occurred
If autoVehFlag is 1 AND inetFlag is 1 then
    Set VTYPE = IV
Else if inetFlag is 1 then
    Set VTYPE = SV
Else if RSUFlag is 1 then
    Set VTYPE = BV
End if
If VTYPE equals IV OR SV AND inetFlag is 1 then
    Send_Message (Pkt) to fog server
Else
    Set SevConditionFlag to ON
    For i =1 to NeighborCount
        If NeighborList[i]equals IV OR SV
            Send_Message (Pkt) to fog server
            Set SevConditionFlag to OFF
            Break loop
        End If
    End For
    If SevConditionFlag is ON then
        Set SentMsgFlag to ON
        For k =1 to NeighborCount
            If NeighborList[k]contains RSU at one hop then
                Send_Message (Pkt) to RSU
                Set SentMsgFlag to OFF
                Break loop
            Else If NeighborList[k]contains RSU at second hop then
                Send_Message (Pkt) to RSU
                Set SentMsgFlag to OFF
                Break loop
            Else If NeighborList[k]contains RSU at third hop then
                Send_Message (Pkt) to RSU
                Set SentMsgFlag to OFF
                Break loop
            End If
        End For
    End if
    If SentMsgFlag is ON then
        Send_Message (Pkt) to Neighbor ->Next_Vehicle
    End if
End if
```

Figure 4.4: Algorithm for Efficient Management of Excessive Messaging

4.5 Summary

In this chapter, we describe the flow of our proposed approach by drawing the flowchart of our model. A flowchart can help the reader understand how an author works. The reader does not have to work hard to understand the model's flow; all they have to do is look at the flowchart. Then, for our recommended technique, we design an algorithm explaining each model step. Through this process, we can easily indicate how we have processed our model to a paper reader.

CHAPTER 5

PERFORMANCE EVALUATION

5.1 Overview

In this chapter, we present the findings and discussion of the proposed scheme compared to its counterparts. We begin by discussing the simulation scenario and the associated list of simulation parameters. The results are presented to evaluate our proposed routing protocol, excessive messaging management scheme, and algorithm introduced in Chapter 4. We have evaluated the performance of the proposed methodology by evaluating and illustrating it with different parameters and metrics. The main metrics include communication overhead and packet loss ratio during information dissemination; packet delivery ratio for emergency messages; average delay for message dissemination; and throughput for emergency message initiation from vehicles.

5.2 Results and Analysis

We explain the simulation framework technically in this chapter, as described earlier in chapter 3 regarding simulation framework. We used NS2.35 to run a large number of simulations. Every simulation scenario is run ten times to generate trace files, and after that the results are calculated using PERL scripts. LTV and HTV vehicles are used, with the former consuming lower energy and transmission range than the later. According to NXP's (Editors 2016) radar sensor specifications, the broadcast range of LTV and HTV is set at 30 meters. The zone of deployment of nodes is adjusted at 100 X 2000 m, 100 m indicates the width of the road and the surrounding area, and 2000 m indicates the space between nodes. In Table 5.1 simulation parameters are listed. A realistic environment is created in which all sorts of vehicles, such as Iv, Sv, and Bv, are travelling according to speed regulations. The communication duration for emergency messages between vehicles 3 minutes, because in that time frame vehicles are expected to share large amounts of data either by sending or receiving. Vehicles nodes are setup in three different ways during simulation. We simulated the proposed EEMS and compare these results to that of E^2MD (Yaqoob et al. 2019) and RMFF (Sattar et al. 2018). This section examines the Excessive Messaging Management Scheme for emergency scenario protocol using various node mobility speeds and packet rates.

Table 5.1: Simulation Parameters

Parameter Descriptions	Values
Deployment region	2000 × 100 m
Tx power at node	0.819 μJ
Receiving POWER	0.049 μJ
Transmission range	30 m
Queue type	Queue/DropTail/PriQue
Antenna type	Omni antenna
Agent trace	On
Router trace	On
Vehicles initiated messages	20–50

5.2.1 Performance metrics

The amount of vehicle connections is computed as $\frac{|N|\times|N-1|}{2} = \frac{12(12-1)}{2} = \frac{132}{2} =$ 66 when there are twelve vehicles in the vicinity of Av, as seen in Figure 5.1. For Graph (N, L), the total number of vehicles in total during a single hop is denoted by N also, the existing linkages are denoted by L. Packet loss and congestion are caused by all existing link connections. Replication of messages also aids in the formation of congestion as $L \times \frac{\sum_{i=1}^{n}(DM+RM)}{100}$ here L denotes connection links that are established, DM denotes dropped messages, and RM denotes replayed messages. The measures listed below are used to evaluate the efficiency of the proposed EEMS. These figures are supposed to show how strong the planned strategy is. Any network that has a low communication overhead, latency, and packet loss ratio is dependable, whereas IoVs with a smooth communication throughout and high packet delivery ratio. Smooth communication is feasible when packet delivery is faster and there is less danger of packet loss. Figure 5.1 depicts the impact of node mobility on end-to-end latency. The graph indicates that the number of nodes rises; the end-to-end latency increases.

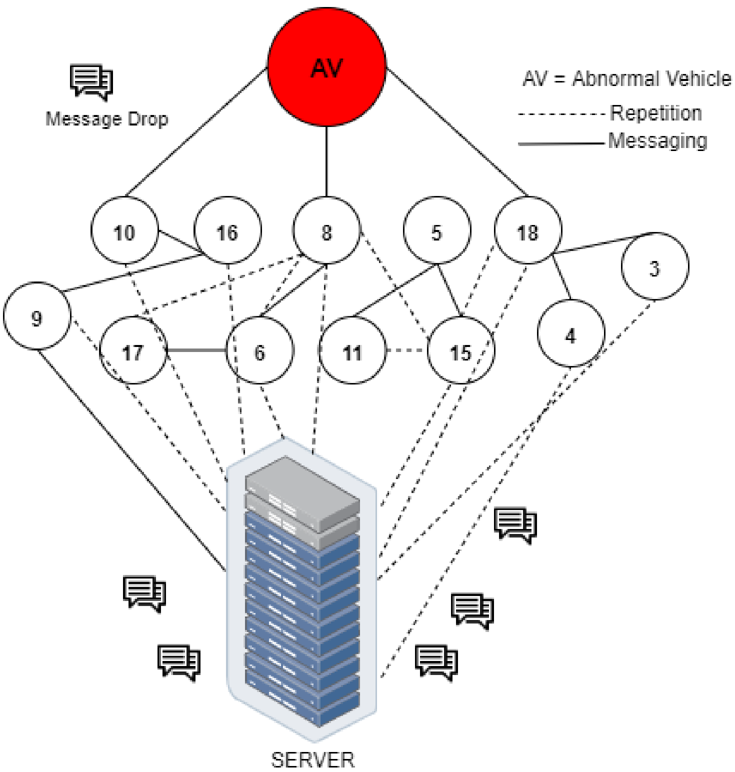

Figure 5.1: Redundant recurrence of messages in IoVs

5.2.2 Communication overhead during messaging

Communication overhead refers to transmission overhead during messaging. The total number of messages in the system is referred to as transmission overhead. Total energy consumption is known as the total number of packets in a network. This metric (communication overhead) is also used to compare the proposed EEMS to other techniques in order to emphasize the paper's accomplishments. The communication overhead in terms of total messages is seen in Figure 5.2. The data clearly shows that EEMS has considerably reduced communication overhead compared to E^2MD and RMFF. The messaging overhead rises with more neighbors and more communication through the internet from different sources. It is also worth mentioning that EEMS minimizes communication overhead dramatically in crowded networks. Due to limited flooding, however, RMFF has the highest messaging cost for message dispersion. E^2MD has the highest messaging cost when it comes to message distribution if RSU is not discovered in the single hop neighbor. Messages are not transmitted and so do not reach the other lane. Our proposed approach transmits messages to dependable vehicles and neighbors in two to three-hop neighbors that implies messages are sent to vehicles in close proximity. Meanwhile, the server keeps track of other incoming traffic and has an advantage over its competitors.

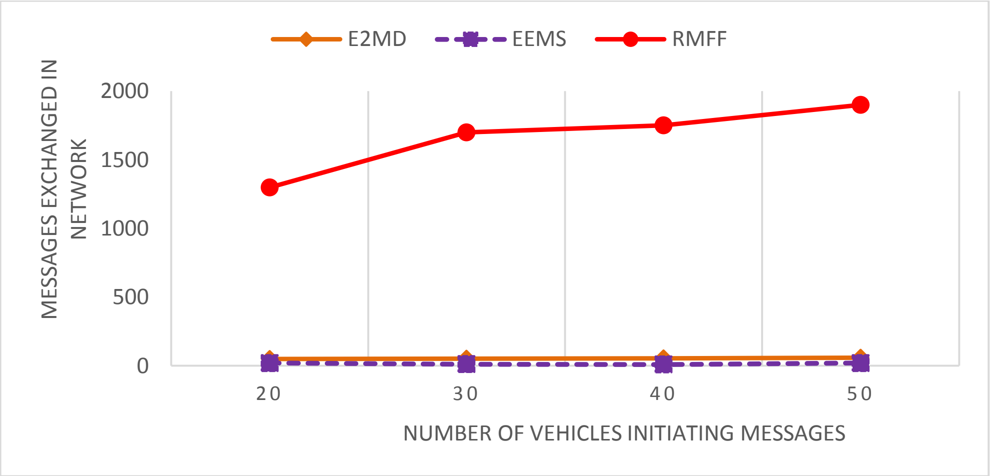

Figure 5.2: Communication overhead during messaging

5.2.3 Packet delivery ratio

The packet delivery ratio (PDR) compares the number of packets received at the destination to the number of packets transmitted from the source. Because of the fog server, the proposed method, EEMS, has a higher packet delivery ratio than the existing methods. The fog server aids in alleviating crowding caused by message repetition. EEMS choose a dependable vehicle to send signals to the fog server. The fog server is in charge of informing the rescue crew and approaching traffic. E^2MD and RMFF notify the server and oncoming traffic via neighboring vehicles, causing congestion due to message recurrence. Figure 5.3 depicts the PDR in terms of successful message broadcast among a large number of adjacent vehicles. The study looked at a real-world scenario in which vehicles broadcast varying numbers of messages, such as 20, 30, 40, and 50. The quantity of messages sent depends on the number of vehicles present; for example, a congested region with numerous vehicles sends a significant number of messages. In a scarce atmosphere with fewer messages, congestion is reduced naturally. Packet delivery is improved when there is less congestion. In general, minimal congestion reduces the likelihood of packet loss. The congestion in a compact environment is higher than in a sparse one with few messages. Messages in E^2MD are sent to the fog server by selecting a reliable vehicle, which implies that if there is no RSU available in a single hop neighbor, congestion ensues, resulting in packet loss. RMFF systems result in a flood of repetitive messages, causing severe congestion. As we have shown, greater levels of congestion result in lower PDR. On the other hand, the proposed approach handles excessive messages by adding three different vehicle types and employing a fog server.

The data shows that EEMS has a much higher PDR than E^2MD and RMFF. The PDR for E^2MD and RMFF for a situation with 30 vehicles initiating messages is 96 percent and 53 percent respectively however; our proposed EEMS prevails by successfully delivering 97 percent.

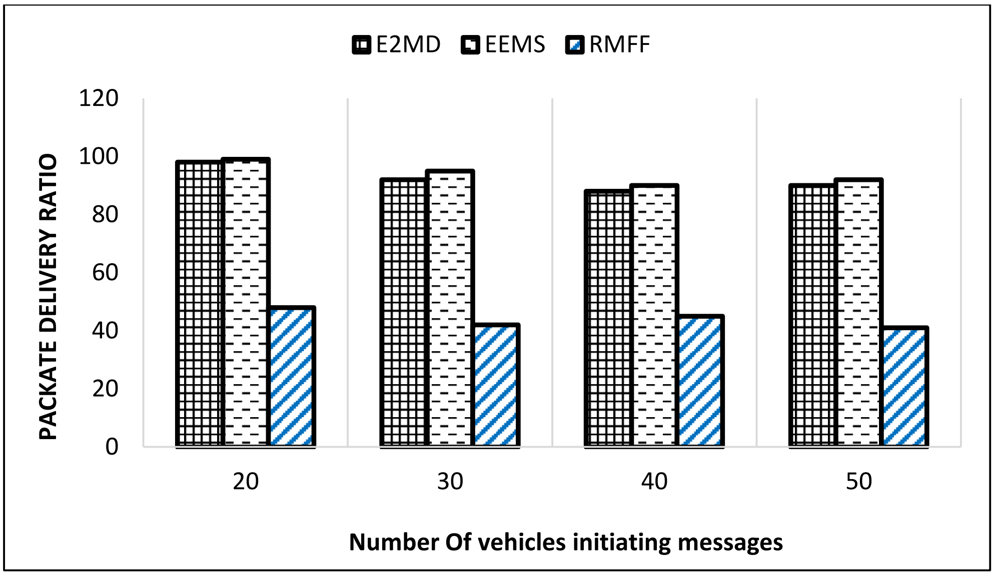

Figure 5.3: Packet delivery ratio for emergency messages

5.2.4 Packet loss ratio

The packet loss ratio (PLR) is a metric that measures how many messages are lost during packet transmission from source to destination. In comparison to existing schemes E^2MD and RMFF, the proposed scheme EEMS has a lower packet loss ratio. Message congestion leads to packet loss in existing methods because of repetitive messages. In the event of emergency messages, packet loss is extremely dangerous; if EMs are unable to arrive in time, it may consequence in undetermined deaths. Due to a smart fog-based situation with three forms of cars, EEMS gives less PLR. Because there are fewer repetitive messages in this instance, it helps to alleviate congestion. The PLR is depicted in Figure 5.4 in terms of message loss while sending packets. The PLR is calculated by subtracting received information from the packets being sent. Dropped messages, in fact, aid in calculating the average packet loss. This study looked at a real-world scenario with varying numbers of messages transmitted from source to destination, such as 20, 30, 40, and 50. The results vary depending on the quantity of messages delivered since a small number of packets results in a lower PLR than a considerable number of packets. Compared to E^2MD and RMFF, the data clearly show that EEMS causes considerably less PLR. In comparison to RMFF and E^2MD, our EEMS method achieves 99 percent and 96 percent less PLR, respectively.

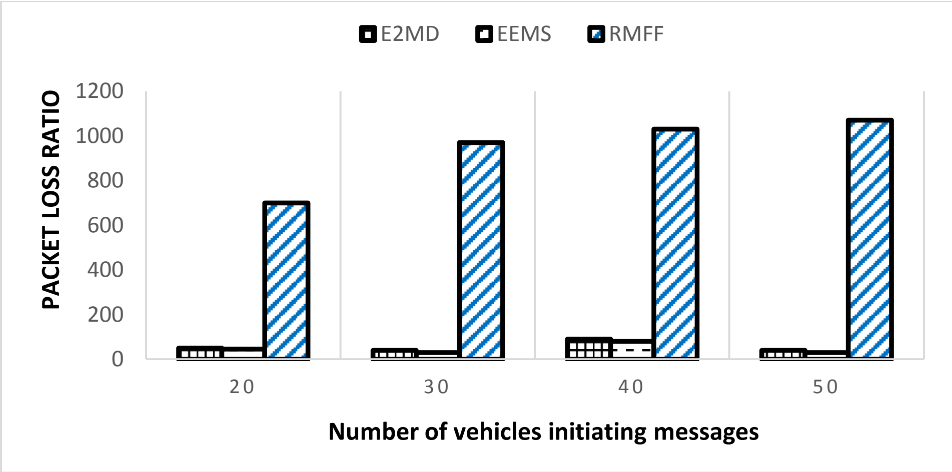

Figure 5.4: Packet loss ratio during message dissemination

5.2.5 Message transmission delay

The average delay is the time taken for n messages to travel from sender to receiver. Current vehicle speeds must be kept to a minimum and not exceed maximum speeds Small automobiles travelling at high speeds can travel in the right lane of LTV traffic. Vehicles can drive at regular speeds in the medium lane, while HTV traffic with big trucks and loaders can go in the left lane. LTV vehicles must have a shorter range than HTV vehicles. Current vehicles' acceleration should not exceed the restrictions. The average latency during information transfer from an abnormal vehicle to the server is explored in Figure 5.5. Eq. 5.4 calculates the average delay for the proposed method and E^2MD:

$$\text{Delay}_{\text{avg}} = \frac{\sum(\text{ End−to−End delay})}{\sum(\text{R}_{\text{packets}})} \qquad (5.4)$$

When unique neighbors are present throughout the Av, the average latency varies in seconds and milliseconds. In comparison to RMFF and E^2MD, our EEMS method delivers 72 percent, and 28 percent reduced latency, respectively. In comparison to E[2]MD and RMFF, our approach dominates by consuming less delay.

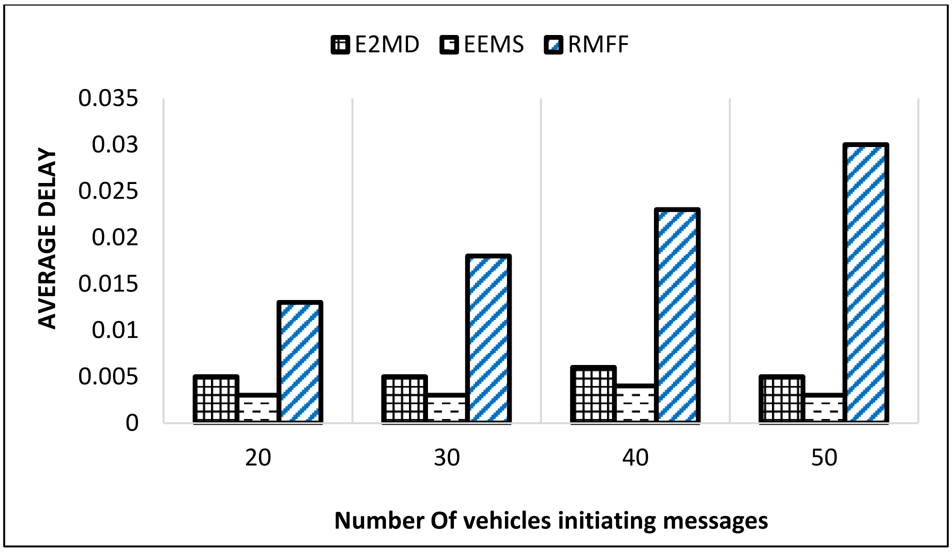

Figure 5.5: Average delay for message dissemination

5.2.6 Throughput

The throughput is the number of packets received at the destination per unit time. It aids in network performance analysis. Figure 5.6 shows the throughput of messages sent in a particular amount of time. This study looked at a real-world scenario with varying numbers of messages transmitted from source to destination, such as 20, 30, 40, and 50. Average throughput is computed by multiplying the obtained results after dividing received packets by average delay and packet size by 1000, as stated in Eq. 5.6. In comparison to E2MD, the data shows that EEMS has a higher throughput:

$$Throughput_{Avg} = \frac{R_{packets}}{Delay_{avg}} \times \frac{P_{size}}{1000} \tag{5.6}$$

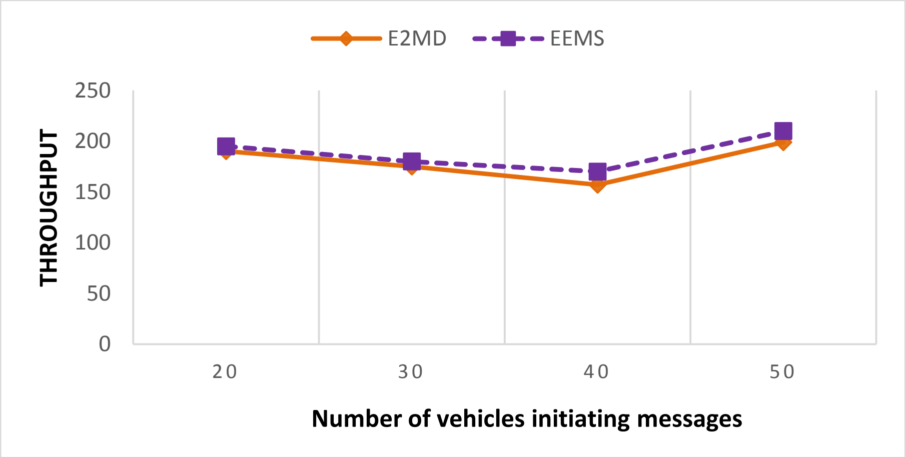

Figure 5.6: Throughput for the Emergency Message Initiation from Vehicles

5.3 Summary

This chapter presents the findings and discussion of the proposed scheme compared to its counterparts. Initially, we discussed the simulation scenario and related list of simulation parameters. The results are presented to evaluate our proposed routing protocol, excessive messaging management scheme, and algorithm introduced in Chapter 4. In performance evaluation, we illustrate the performance of our proposed method with different parameters and metrics. The main metrics include the packet delivery ratio for emergency messages, communication overhead during messaging, packet loss ratio during information dissemination, the average delay for message dissemination, and throughput for the EM initiation from vehicles.

CHAPTER

CONCLUSION AND FUTURE WORK

6.1 Overview

In this chapter, we conclude our work. We begin by describing the component of our field known as IoV. Then, we talked about a few issues we had with benchmarking techniques. We next go over the advantages of our proposed scheme. We contrast our work with the base scheme and discuss the differences. Ultimately, we suggest more ideas for future research that should aid researchers in their continued study of this topic.

6.2 Conclusion

IoVs are a network of vehicles used in transportation systems for dependable communication. Fundamentally, IoVs are made up of thousands of vehicles that are used for certain functions. Message congestion is a key difficulty and a necessary barrier in IoV communication. Message congestion happens when the same messages are sent out repeatedly. Packet loss occurs because of repeated messages. Information and EMs are unable to deliver immediately due to packet drop, resulting in increased accidents. This research proposed an EEMS strategy for excessive message transmission and congestion reduction. Fog computing is used in the proposed study because it simulates the use of local servers for computation and data delivery. This strategy is beneficial not just for smart automobiles but as well for regular vehicles that do not have access to the internet. As a result, it aids in the prevention of further accidents in the real universe. Our proposed technique also works when the server is out of the vehicle's range. We have described numerous messaging strategies in this paper, with an emphasis on congestion avoidance and control-based approaches.

Taxonomy of similar approaches is maintained, with static and dynamic systems separated. The proposed Fog aided IoV architecture is ideally suited to message efficiency. In addition to RSUs, this research examines the role of smart automobiles, which include vehicle-synchronized telephones and internet access. It also investigates the importance of several parameters like latency, transmission range, and throughput in achieving optimal performance. We evaluated the performance of the proposed EEMS system to that of E^2MD and RMFF. Compared to E^2MD and RMFF, EEMS improved message delivery costs while reducing message overhead costs by 97 percent and 98 percent, respectively.

6.3 Summary of your contribution

The summary of our contributions is as follows:

i. We increased the number of hops for message dissemination during emergency message transmission.
ii. We minimized the congestion and latency of sharing emergency packets.
iii. We assured cost-efficient communication between vehicles and the central server.

6.4 Future Work

Future research will focus on the use of queue size to manage the congestion due to emergency messages. Moreover, we would concentrate on investigating various communities with various node types.

REFERENCES

[1] C. Wang, X. Cheng, J. Li, Y. He, and K. Xiao, "A survey: applications of blockchain in the Internet of Vehicles," *Eurasip J. Wirel. Commun. Netw.*, vol. 2021, no. 1, 2021, doi: 10.1186/s13638-021-01958-8.

[2] O. Kaiwartya *et al.*, "Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects," *IEEE Access*, vol. 4, no. c, pp. 5356–5373, 2016, doi: 10.1109/ACCESS.2016.2603219.

[3] T. A. Butt, R. Iqbal, S. C. Shah, and T. Umar, "Social Internet of Vehicles: Architecture and enabling technologies," *Comput. Electr. Eng.*, vol. 69, no. December 2017, pp. 68–84, 2018, doi: 10.1016/j.compeleceng.2018.05.023.

[4] R. Iqbal, T. A. Butt, M. O. Shafique, M. W. A. Talib, and T. Umer, "Context-aware data-driven intelligent framework for fog infrastructures in internet of vehicles," *IEEE Access*, vol. 6, pp. 58182–58194, 2018, doi: 10.1109/ACCESS.2018.2874592.

[5] K. N. Qureshi, S. Din, G. Jeon, and F. Piccialli, "Internet of Vehicles: Key Technologies, Network Model, Solutions and Challenges with Future Aspects," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 3, pp. 1777–1786, 2021, doi: 10.1109/TITS.2020.2994972.

[6] F. Yang, J. Li, T. Lei, and S. Wang, "Architecture and key technologies for Internet of Vehicles: a survey," *J. Commun. Inf. Networks*, vol. 2, no. 2, pp. 1–17, 2017, doi: 10.1007/s41650-017-0018-6.

[7] J. Wang, C. Jiang, Z. Han, Y. Ren, and L. Hanzo, "Internet of Vehicles: Sensing-Aided Transportation Information Collection and Diffusion," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 3813–3825, 2018, doi: 10.1109/TVT.2018.2796443.

[8] W. Wu, Z. Yang, and K. Li, "16 16.1," pp. 299–317, doi: 10.1016/B978-0-12-805395-9/00016-2.

[9] N. Ababneh and H. Labiod, "Safety message dissemination in VANETs: Flooding or trajectory-based?," *9th IFIP Annu. Mediterr. Ad Hoc Netw. Work. MED-HOC-NET 2010*, 2010, doi: 10.1109/MEDHOCNET.2010.5546862.

[10] Y. Bi, L. X. Cai, X. Shen, and H. Zhao, "A cross layer broadcast protocol for multihop emergency message dissemination in inter-vehicle communication," *IEEE Int. Conf.*

Commun., 2010, doi: 10.1109/ICC.2010.5501865.

[11] S. Arianmehr and M. A. Jabraeil Jamali, "HybTGR: a hybrid routing protocol based on topological and geographical information in vehicular ad hoc networks," *J. Ambient Intell. Humaniz. Comput.*, vol. 11, no. 4, pp. 1683–1695, 2020, doi: 10.1007/s12652-019-01332-z.

[12] J. Liu, Z. Yang, and I. Stojmenovic, "Receiver consensus: On-time warning delivery for vehicular ad-hoc networks," *IEEE Trans. Emerg. Top. Comput.*, vol. 1, no. 1, pp. 57–68, 2013, doi: 10.1109/TETC.2013.2273445.

[13] Z. Dou, J. Tian, Q. Yang, and L. Yang, "Design and Analysis of Cooperative Broadcast Scheme Based on Reliability in Mesh Network," *Mob. Inf. Syst.*, vol. 2021, 2021, doi: 10.1155/2021/5554563.

[14] M. U. Ghazi, M. A. Khan Khattak, B. Shabir, A. W. Malik, and M. Sher Ramzan, "Emergency Message Dissemination in Vehicular Networks: A Review," *IEEE Access*, vol. 8, pp. 38606–38621, 2020, doi: 10.1109/ACCESS.2020.2975110.

[15] P. S. V. SathyaNarayanan, "VANET: A novel service for predicting and disseminating vehicle traffic information," *Digit. Signal Process. A Rev. J.*, vol. 85, pp. 10–16, 2019, doi: 10.1016/j.dsp.2018.06.003.

[16] S. Sattar, H. K. Qureshi, M. Saleem, S. Mumtaz, and J. Rodriguez, "Reliability and energy-efficiency analysis of safety message broadcast in VANETs," *Comput. Commun.*, vol. 119, no. June 2017, pp. 118–126, 2018, doi: 10.1016/j.comcom.2018.01.006.

[17] F. Aadil, W. Ahsan, Z. U. Rehman, P. A. Shah, S. Rho, and I. Mehmood, "Clustering algorithm for internet of vehicles (IoV) based on dragonfly optimizer (CAVDO)," *J. Supercomput.*, vol. 74, no. 9, pp. 4542–4567, 2018, doi: 10.1007/s11227-018-2305-x.

[18] D. Feng, M. Yajie, Z. Fengxing, W. Xiaomao, and H. Kai, "A Safety Message Broadcast Strategy in Hybrid Vehicular Network Environment," *Comput. J.*, vol. 61, no. 6, pp. 789–797, 2018, doi: 10.1093/comjnl/bxx075.

[19] S. Yaqoob, A. Ullah, M. Akbar, M. Imran, and M. Shoaib, "Congestion avoidance through fog computing in internet of vehicles," *J. Ambient Intell. Humaniz. Comput.*, vol. 10, no. 10, pp. 3863–3877, 2019, doi: 10.1007/s12652-019-01253-x.

[20] R. P. Meenaakshi Sundhari, L. Murali, S. Baskar, and P. M. Shakeel, "MDRP: Message dissemination with re-route planning method for emergency vehicle information exchange," *Peer-to-Peer Netw. Appl.*, 2020, doi: 10.1007/s12083-020-00936-z.

[21] S. Ebadinezhad, Z. Dereboylu, and E. Ever, "Clustering-based modified ant colony optimizer for internet of vehicles (CACOIOV)," *Sustain.*, vol. 11, no. 9, pp. 1–22, 2019, doi: 10.3390/su11092624.

[22] M. R. Devi, "Black Widow Optimization Algorithm and Similarity Index Based Adaptive Scheduled Partitioning Technique for Reliable Emergency Message Broadcasting in VANET," 2021.

[23] A. K. Fabi and S. M. Thampi, "A trust management framework using forest fire model to propagate emergency messages in the Internet of Vehicles (IoV)," *Veh. Commun.*, vol. 33, Jan. 2022, doi: 10.1016/j.vehcom.2021.100404.

[24] S. Ullah, G. Abbas, M. Waqas, Z. H. Abbas, S. Tu, and I. A. Hameed, "Eemds: An effective emergency message dissemination scheme for urban vanets," *Sensors*, vol. 21, no. 5, pp. 1–19, 2021, doi: 10.3390/s21051588.

[25] G. Abbas, Z. H. Abbas, S. Haider, T. Baker, S. Boudjit, and F. Muhammad, "PDMAC: A priority-based enhanced TDMA protocol for warning message dissemination in vanets," *Sensors (Switzerland)*, vol. 20, no. 1, pp. 1–20, 2020, doi: 10.3390/s20010045.

[26] M. Ali, A. W. Malik, A. U. Rahman, S. Iqbal, and M. M. Hamayun, "Position-based emergency message dissemination for Internet of vehicles," *Int. J. Distrib. Sens. Networks*, vol. 15, no. 7, 2019, doi: 10.1177/1550147719861585.

[27] A. Touil and F. Ghadi, "Efficient dissemination based on passive approach and dynamic clustering for VANET," *Procedia Comput. Sci.*, vol. 127, pp. 369–378, 2018, doi: 10.1016/j.procs.2018.01.134.

[28] M. Alowish, Y. Shiraishi, M. Mohri, and M. Morii, "Three layered architecture for driver behavior analysis and personalized assistance with alert message dissemination in 5G envisioned fog-Iocv," *Futur. Internet*, vol. 14, no. 1, Jan. 2022, doi: 10.3390/fi14010012.

[29] N. Azzaoui, A. Korichi, B. Brik, and M. E. A. Fekair, "Towards optimal dissemination of emergency messages in internet of vehicles: A dynamic clustering-based approach," *Electron.*, vol. 10, no. 8, 2021, doi: 10.3390/electronics10080979.

[30] O. AlQahtani and F. T. Sheldon, "Validation of VANET message dissemination algorithms otherwise vulnerable to broadcast storms in urban contexts," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 10, pp. 1–16, 2021, doi: 10.1002/ett.4312.

[31] S. Abdelatif, M. Derdour, N. Ghoualmi-Zine, and B. Marzak, "VANET: A novel service for predicting and disseminating vehicle traffic information," *Int. J. Commun. Syst.*, vol. 33, no. 6, pp. 1–16, 2020, doi: 10.1002/dac.4288.

[32] M. Ryu and S. H. Cha, "Mobility Prediction Based Multi-Directional Broadcasting for Both Highway and Urban Vehicular Sensor Networks," *IEEE Access*, vol. 8, pp. 148595–148605, 2020, doi: 10.1109/ACCESS.2020.3016308.

[33] A. Paranjothi, M. S. Khan, and M. Atiquzzaman, *DFCV: A novel approach for message dissemination in connected vehicles using dynamic fog*, vol. 10866 LNCS. Springer International Publishing, 2018.

[34] Q. Huang, N. Li, Z. Zhang, and Y. Yang, "Secure and Privacy-Preserving Warning Message Dissemination in Cloud-Assisted Internet of Vehicles," *2019 IEEE Conf. Commun. Netw. Secur. CNS 2019*, pp. 1–8, 2019, doi: 10.1109/CNS.2019.8802649.

[35] Z. Liu *et al.*, "TCEMD: A Trust Cascading-Based Emergency Message Dissemination Model in VANETs," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4028–4048, 2020, doi: 10.1109/JIOT.2019.2957520.

[36] M. Saini, A. Alelaiwi, and A. El Saddik, "How close are we to realizing a pragmatic VANET solution? A meta-survey," *ACM Comput. Surv.*, vol. 48, no. 2, Nov. 2015, doi: 10.1145/2817552.

[37] T. Yang *et al.*, "Two-Stage Offloading Optimization for Energy-Latency Tradeoff with Mobile Edge Computing in Maritime Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 5954–5963, Jul. 2020, doi: 10.1109/JIOT.2019.2958662.

[38] Q. Li, A. Malip, K. M. Martin, S. L. Ng, and J. Zhang, "A reputation-based announcement scheme for VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 9, pp. 4095–4108, 2012, doi: 10.1109/TVT.2012.2209903.

[39] D. Tian *et al.*, "A Distributed Position-Based Protocol for Emergency Messages Broadcasting in Vehicular Ad Hoc Networks," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1218–1227, Apr. 2018, doi: 10.1109/JIOT.2018.2791627.

[40] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "A multifaceted approach to modeling agent trust for effective communication in the application of mobile Ad Hoc vehicular networks," *IEEE Trans. Syst. Man Cybern. Part C Appl. Rev.*, vol. 41, no. 3, pp. 407–420, May 2011, doi: 10.1109/TSMCC.2010.2084571.

[41] H. Hu, R. Lu, Z. Zhang, and J. Shao, "REPLACE: A Reliable Trust-Based Platoon Service Recommendation Scheme in VANET," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1786–1797, Feb. 2017, doi: 10.1109/TVT.2016.2565001.

[42] Z. Liu, J. Ma, Z. Jiang, H. Zhu, and Y. Miao, "LSOT: A lightweight self-organized trust model in VANETs," *Mob. Inf. Syst.*, vol. 2016, 2016, doi: 10.1155/2016/7628231.

[43] F. Trueblood, S. Gill, R. Wong, S. Tayeb, and M. Pirouz, "A Data-Centric Approach to

Taming the Message Dissemination in the Internet of Vehicles," *2020 10th Annu. Comput. Commun. Work. Conf. CCWC 2020*, pp. 207–214, 2020, doi: 10.1109/CCWC47524.2020.9031272.