EFFICIENT SAFETY MESSAGE DISSEMINATION IN VEHICULAR AD HOC NETWORKS

A Dissertation
Presented to
The Academic Faculty

By

Hamza Ijaz Abbasi

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy in the
School of Electrical and Computer Engineering

Georgia Institute of Technology

May 2018

EFFICIENT SAFETY MESSAGE DISSEMINATION IN VEHICULAR AD HOC NETWORKS

Approved by:

Dr. John A Copeland, Advisor
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Yusun Chang, Co-advisor
S.P. College of Engineering and Engineering Technology
Kennesaw State University

Dr. Raheem A Beyah
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Henry L Owen
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Mostafa H Ammar
School of Computer Science
Georgia Institute of Technology

Dr. Ellen W Zegura
School of Computer Science
Georgia Institute of Technology

Date Approved: December 20, 2017

To my dear parents, siblings, wife, and daughter

ACKNOWLEDGEMENTS

All praise, and thanks be to Allah, the One and Only God, the Most Gracious and the Most Merciful. Peace, blessings and salutations be upon all his prophets from Adam to the last prophet, Muhammad (peace be upon him).

I am honored and very fortunate to have had the opportunity to work under the mentorship and guidance of my advisors, Dr. John A Copeland and Dr. Yusun Chang. I am very grateful for their continued support throughout my PhD. I would like to express my gratitude to Dr. Raheem Beyah and Dr. Henry Owen for reading this dissertation and for providing me their invaluable feedback. I would also like to thank Dr. Mostafa Ammar and Dr. Ellen Zegura for serving in my dissertation defense committee. Additionally, I would like to acknowledge the support of Georgia Department of Transportation for funding part of this research. I would also like to thank my undergraduate research advisor, Dr Tarek Sheltami for inspiring me.

I am deeply indebted to my colleague, Christian Voicu for his help and support. Additionally, I would like to thank my lab mates: Billy, Deuk, Brian, and Huangwei. I am also grateful to Abdul Jabbar, Rizwan, Usman Ali, Ali Murtaza, and others, for their support during my PhD. I would also like to thank the academic professionals in the ECE academic office including Dr. Daniela Staiculescu, Tasha Torrence, and Jacqueline Trappier for their help.

Finally, I am extremely grateful to my parents, siblings, wife, daughter, and our extended family. Their prayers did wonders for me. All of this was made possible due to their selflessness, encouragement, and support.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

SUMMARY

Over the past few years, the occurrence of enormous human, societal, environmental and economic losses due to traffic accidents has led toward a search for highly innovative and practical solutions to improve safety on the roads. One such initiative is the introduction of Intelligent Transportation Systems (ITS), whereby a vital application is to ensure road safety by fast and reliable dissemination of safety messages. This research develops novel and practical schemes to efficiently and reliably disseminate safety information in Vehicular Ad Hoc Networks (VANETs) using Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication to improve the transportation safety.

Firstly, an innovative multi-hop broadcasting protocol is developed, which exploits a smart forwarder selection process, handshake-less broadcasting, ACK Decoupling and efficient collision resolution mechanism. This protocol significantly improves the speed of safety message propagation without compromising on the reliability. Secondly, this research proposes a novel architecture that facilitates the effective sharing of safety information in VANETs by exchanging and storing the data (about potential threats) obtained from the neighboring vehicles as well as from on-board sensor technologies. The architecture leverages entirely on BSMs and improves the visibility and situational awareness of vehicles. The key attraction of this architecture is its novelty, simplicity, practicality, and applicability. Both of the proposed schemes were evaluated under simulation and real-world experimental conditions. The results establish and validate the performance gain of the proposed schemes.

The highlight of the above techniques is that the exchange of safety information among vehicles takes place using the existing V2V standards, without requiring any modifications to the standards. Finally, these techniques can be readily deployed to improve safety on the roads, and thus, reduce human causalities as well as lower the social, environmental and economic expenses.

CHAPTER 1
INTRODUCTION

According to USDOT statistics, the year 2014 alone recorded 6.1 million vehicular crashes, resulting in 32,675 tragic fatalities, 2.3 million injuries, and 4.4 million property damage incidents [1], on top of an already massive $836 billion in societal damage annually [2]. These huge losses have lead toward the initiation of joint efforts by government, industry and academia to ensure road safety by exploiting novel and innovative technologies. One such initiative is the introduction of Intelligent Transportation Systems (ITS) [3], which is a set of advanced applications aimed at providing innovative services related to traffic safety, traffic management, different modes of transportation, smarter flow of traffic information, and so on. In ITS, a critical application is to ensure road safety through an efficient exchange of safety messages between the vehicles on the roads [4]. The Dedicated Short-Range Communications (DSRC) standards, developed for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications specify a dedicated Control Channel (CCH) for these time-sensitive safety messages [5]. Such a network of communicating vehicles (equipped with DSRC radios) is commonly known as Vehicular Ad hoc Networks (VANETs) [6].

The objectives of this research are to develop efficient and robust safety message dissemination techniques for VANETs using V2V and V2I communication in order to improve the transportation safety.

1.1 Vehicular Ad Hoc Networks

Vehicular Ad hoc Network (VANET) - a specific type of Mobile Ad hoc Network (MANET) - is a group of vehicular nodes that spontaneously form a wireless network using the 802.11p protocol for data exchange while moving on the road. Such networks have a

tremendous potential in enabling diverse applications related to traffic safety, traffic efficiency and infotainment [6], [7], [8]. In VANETs, communication can take place between the vehicular nodes as vehicle-to-vehicle (V2V) communication or between vehicles and infrastructure as vehicle-to-infrastructure (V2I) communication.

VANETs possess some distinguishing characteristics from ordinary wireless networks that make them suitable for the highly dynamic traffic conditions. Some of these characteristics include, but are not limited to, ensuring connectivity under high node mobility, not requiring any central coordination, providing support for dynamic and multi-hop communications, and so on. On the other hand, VANETs also carry some unique limitations such as increased obstructions due to different obstacles on the roads, limited transmission range, limited effective bandwidth and unique security challenges.

1.1.1 VANET Standards

To regulate V2V and V2I communications in United States, Dedicated Short Range Communications (DSRC) standards are being actively formulated and finalized [5]. DSRC is aimed at providing high data transmission while ensuring least possible delays for short-to-medium range communications. DSRC primarily supports safety related applications but also offers other applications such as providing traffic information / entertainment services, toll collection, drive-through payment, and so on. According to USDOT, 76% of the vehicular crashes could be avoided through the implementation of DSRC technology.

In VANETs, each vehicle participating in communication must be equipped with DSRC radios. VANETs utilize the licensed DSRC spectrum of 75 MHz at 5.9 GHz (5.85-5.925 GHz), as allocated by Federal Communication Commission (FCC), to exchange data between high-speed vehicles (V2V) and between the vehicles and the roadside infrastructure (V2I). Since transportation safety is the main objective of this freely available bandwidth, several standards specify the rules and regulations. Specifically, DSRC utilizes IEEE 802.11p [9] and IEEE 1609 [10] standards to define the rules of operation for vehicular

communications [5]. IEEE 802.11p standard deals with the low-layer operations such as those dealing with Medium Access Control (MAC) and Physical (PHY) layers, while the IEEE 1609 standard regulates the operation of upper layers such as Network, Security and Application layers. IEEE 802.11p is an enhancement of the generic IEEE 802.11 standard with an emphasis on providing special support for ensuring communication between high-speed moving vehicles and road-side infrastructures. IEEE 1609, which are standards for Wireless Access in Vehicular Environments (WAVE), consist of the following four main components: IEEE 1609.1 addresses the resource management for applications while IEEE 1609.2 deals with security issues such as defining secure message formats as well as processing of those secure messages for use by WAVE devices. On the other hand, IEEE 1609.3 offers network and transport layer services. Lastly, IEEE 1609.4 provides support for multi-channel operation.

The DSRC frequency spectrum consists of seven different channels where each channel has 10 MHz bandwidth. A channel specifically dedicated just for safety purposes is known as Control Channel (CCH), during which specialized safety messages are generally exchanged. Six remaining channels, called Service Channels (SCH) are used for both safety and non-safety applications such as for infotainment, entertainment and so on. [11]

All DSRC-compatible vehicles tune in to the CCH for 50 ms followed by 50 ms to a SCH of choice. During CCH, specialized safety messages called Basic Safety Messages (BSM) as well as WAVE Service Announcements (WSA) are shared. WSAs announce the available services on the various SCH.

1.1.2 Basic Safety Messages

In VANETs, a critical requirement for the V2V-compatible nodes is the periodic exchange of a Basic Safety Message (BSM) containing real-time information about the transmitting vehicle such as its position, speed, direction, brake information, steering wheel angle, etc., as shown in Table 1.1. All other vehicles within the transmission range of the sender, then

Table 1.1: BSM data fields

BSM Data Item	Bytes	Part
Message ID	1	I
Message count	1	I
Temporary ID	4	I
Time	2	I
Latitude	4	I
Longitude	4	I
Elevation	2	I
Positional Accuracy	4	I
Speed	2	I
Heading	2	I
Steering Wheel Angle	1	I
Acceleration	7	I
Brake System Status	2	I
Vehicle Size	3	I
Optional Part	Variable	II

utilize this information to decide whether the driver should be warned of an impending collision, or an autonomous system should be activated instead.

The BSM consists of the following two parts: Part I contains 39 bytes of critical safety information while Part II (optional) can contain up to a few hundred bytes of extra safety information about the transmitting vehicle such as path history and other options. The BSM exchange between vehicles is dictated by the WAVE 1609 and IEEE 802.11p standards. Although, the frequency of BSM exchange between vehicles strictly depends upon the overlying applications, most applications have a requirement of less than 10 Hz (10 BSM broadcasts per vehicle per second). To generate BSMs, a safety application requests the vehicular data from in-vehicle Controller Access Network (CAN) bus and GPS receiver.

On the receiver's side, a safety application receives the BSMs and passes the safety-critical information about the sender to custom applications which can utilize this information for providing safety related functionalities such as collision avoidance, applying automatic brakes, generating traffic warnings and so on. BSMs are single hop broadcast messages that range in size anywhere between approximately 50 bytes up to 800 bytes

depending on the data shared in Part II as well as the level of encryption applied.

Due to the critical and sensitive nature of BSMs, they are shared in the Control Chanel (CCH) so that all vehicles are able to transmit as well as hear the periodic safety-related broadcasts. During CCH, as each vehicle tries to broadcast its BSM randomly, there are chances of the occurrence of packet collisions. As WAVE 1609.4 standard allows for priority queues, BSMs being safety-critical packets are assigned the highest transmission priority. An interesting observation related to the BSM's size is that in a case where vehicles are sharing larger BSM packets (around 800 bytes), it is predicted that there will be higher chances of collisions since it takes longer to place such large packets on the channel (transmission delay) as well as increased transceiver's reception time. Under such scenarios, it is advisable to lower the frequency of BSM transmission to well below 10 Hz so that the probability of having multiple nodes broadcasting BSM at any point of time can be lowered. Hence, finding an optimal balance between the size and frequency of BSMs is a challenging problem.

1.2 Contribution

This dissertation aims to provide highly innovative and feasible solutions to efficiently and reliably disseminate the safety information in VANETs in order to improve the overall transportation safety. The contributions of this research are multi-fold.

First, we present a comprehensive and qualitative review and analysis of the existing safety message dissemination techniques in VANETs by categorizing them based on their message sharing criteria. Additionally, we highlight and discuss the latency, reliability, and collision problems in these existing schemes.

Next, we propose an innovative multi-hop broadcasting scheme for safety message delivery, called Intelligent Forwarding Protocol (IFP), which exploits a smart forwarder selection process, handshake-less broadcasting, *ACK* decoupling technique, and an efficient collision resolution mechanism. The protocol significantly improves the speed of safety

message propagation while ensuring guaranteed message delivery. The protocol is analyzed and optimized using thorough mathematical modeling. Additionally, we carry out extensive simulations that establish the superiority of IFP as compared to the existing multi-hop broadcasting techniques in terms of forwarding latency and reliability. Furthermore, we present the results and analysis of the real-world experimentation and field tests that validate the feasibility and performance gain of IFP under real-world traffic conditions. The research work related to this protocol has been published in [12] and[13], while some portion of the work is under review in [14].

Finally, we introduce a novel architecture that not only facilitates the effective sharing of safety information in VANETs, but also increases the visibility and awareness of the vehicles, by intelligently exchanging and storing the data obtained from the neighboring vehicles as well as from on-board sensor technologies by leveraging the BSM broadcast. Through this approach, vehicles are able to quickly and preemptively identify potential threats, not just in their close proximity, but also those that are further along the roadway by intelligently exchanging safety information between neighboring vehicles. The proposed architecture was evaluated under both simulation and real-world traffic conditions. The results establish and validate the performance gain of the proposed scheme. The research pertaining to this architecture has been published in [15], while some portion of the work is in preparation for submission in [16].

The key advantage of the above techniques is that the exchange of safety information among vehicles takes place using the existing DSRC standards, without requiring any modifications to the standards. Additionally, the experimentation and field trials prove the effectiveness and robustness of the proposed schemes in the real-world VANET conditions. As a result, these techniques can be readily deployed to improve safety on the roads, and thus, reduce human causalities as well as lower the social, environmental and economic expenses.

1.3 Organization

This dissertation is organized as follows. In Chapter 1, we present the basic introduction, contribution, and goals of this work. Chapter 2 presents a comprehensive literature survey of the existing safety message dissemination techniques in VANETs. Additionally, the limitations and shortcomings of these existing techniques have also been highlighted in Chapter 2. Chapter 3 describes an efficient multi-hop broadcasting based Intelligent Forwarding Protocol for fast and reliable safety message dissemination in VANETs. In Chapter 4, we present the performance analysis of Intelligent Forwarding Protocol in comparison to the existing multi-hop broadcasting schemes using extensive simulations and real-world experimentation. Chapter 5 describes a novel cooperative BSM-based architecture to efficiently share safety information among vehicles. Finally, Chapter 6 presents the conclusion and the future research direction.

CHAPTER 2

EXISTING SAFETY MESSAGE DISSEMINATION TECHNIQUES

The efficient and robust sharing of safety information among vehicles on the road is a complex problem which has been profoundly studied in the literature. It is often referred to as safety message dissemination. The safety message dissemination process in VANETs is unique in the sense that it is of a broadcast-oriented nature, since the safety-related information is intended for a group of nodes as opposed to a single node [6]. Additionally, considering the highly dynamic typology of VANETs coupled with a short average link life [17], the common data transmission techniques based on table routing and acknowledgments are inefficient and exhibit low throughput [18]. Therefore, safety applications, which require a more reactive and fast packet delivery mechanism, generally exploit broadcasting schemes for safety message dissemination. Hence, in this research, we exclusively consider broadcasting protocols for safety message dissemination in VANETs. A portion of this chapter also appeared in [14] and [15].

Safety message dissemination encounters numerous challenges in a VANET environment. Firstly, in VANETs, the distribution of vehicles is quite irregular and the connectivity among these vehicles is highly random. Hence, delivering safety messages reliably to each vehicle in the target region is a challenge. Secondly, most safety applications use the common control channel (CCH) for safety message dissemination, leaving them quite vulnerable to collisions and interference. Moreover, having any kind of efficient response mechanism (such as Acknowledgments) from multiple recipient nodes back to the sender is not an easy task in VANETs, thus preventing guaranteed delivery of safety messages. Similarly, multi-hop dissemination of safety messages in VANETs is another non-trivial problem, which is an ongoing topic of research for several years.

A significant amount of research work has been carried out, particularly in the last

decade, to address the above-mentioned problems in VANETs. In this chapter, some of these existing works have been discussed. The safety-related broadcasting algorithms can be classified into one of the following two broad categories: 1) Single-hop Broadcasting, 2) Multi-hop Broadcasting.

2.1 Single-hop Broadcasting

Many existing broadcasting schemes exploit single-hop V2V communication for spreading safety-related information in the network. This kind of communication is easy to be established and provides many critical safety-related applications such as rear-end collision avoidance, head-on collision avoidance, lane change warning, blind spot warning, and so on. Single-hop broadcasting techniques do not flood the network with information packets since the messages are only shared with the immediate one-hop neighbors, and thus, result in minimal redundancy. Generally, the single-hop approach requires vehicles to broadcast the information after a certain interval, which can either be fixed (periodic) or adaptive. Therefore, we categorize the single-hop schemes into one of these two classes: 1) Periodic Broadcasting, 2) Adaptive Broadcasting.

2.1.1 Periodic Broadcasting

In periodic single-hop broadcasting schemes, vehicles periodically broadcast the traffic or safety information to their neighbors after a fixed interval. Upon message reception, the vehicles do not rebroadcast the message immediately. Instead, they store the new information in their databases, provided that the information is valuable and relevant. Periodically, these vehicles then share some of the information with their own neighbors. In this manner, the vehicles cooperate with each other to improve the overall transportation safety. In such protocols, the key design considerations include the duration of the broadcast interval, and the information that needs to be shared with the neighbors. In order to reduce redundancy and share the latest information, an appropriate broadcast interval should be selected, which

is neither too long nor too short. In most existing periodic broadcasting schemes, the main focus is on information selection, aggregation, and distribution.

TrafficInfo [19] and TrafficView [20] are the two main periodic broadcasting schemes designed to facilitate the sharing of traffic information among vehicles. In TrafficInfo [19], the vehicles exchange the travel times on the road segments. The vehicles are assumed to have knowledge of the digital map of the roadways, and their own location on the map. When a vehicle travels through a particular road segment, it records its corresponding travel time in its on-board database. The vehicle then shares the most important records with its neighbors. In this manner, all vehicles collectively learn about the travel times associated with the different road segments. By sharing this travel time information, vehicles are better aware of the traffic conditions on the road network, and thus can plan their route to avoid congestion.

On the other hand, TrafficView [20] facilitates the sharing of speed and position information among neighboring vehicles. Similar to TrafficInfo, in TrafficView, when a vehicle receives a broadcast packet, it stores the useful information in its database. The vehicle then aggregates the speed and positions of many vehicles in a single record, and shares it in the next broadcast cycle. TrafficView proposed two aggregation algorithms, ratio-based algorithm and the cost-based algorithm. The performance of these algorithms has been evaluated and compared by simulation. By using such a system, vehicle drivers will be provided with latest road traffic information, which can help in driving safely in hazardous situations such as foggy weather, or in finding optimal routes to the destination.

However, with the emergence of inexpensive and high data-rate enabled wireless communication technologies such as 4G and LTE, coupled with real-time traffic apps such as Google Maps and Waze, planning routes, estimating travel times, and getting live weather or road updates has become very easy, thus removing the need for protocols like TrafficInfo and TrafficView. A major drawback of such periodic single-hop broadcasting protocols is that due to the fixed broadcast intervals, such protocols can not perform optimally under

all traffic conditions. For instance, if the broadcast interval is long, the information shared might be too old and irrelevant to the receiving vehicles. On the other hand, a short interval can lead to increased packet collisions and a severely congested network. To counter these limitations, numerous adaptive broadcasting protocols have been proposed in the literature.

2.1.2 Adaptive Broadcasting

In adaptive single-hop broadcasting protocols, variable broadcast intervals are exploited to share traffic information among neighboring vehicles. One such protocol known as Collision Ratio Control Protocol (CRCP) [21] proposes a dynamically changing broadcast interval based on the number of packet collisions. The protocol is designed to keep the collision ratio below a certain threshold value. In CRCP, the traffic information shared includes the location, speed, and road ID. As the number of packet collisions increases, vehicles adjust their respective broadcast intervals in order to lower the overall packet collisions. In particular, the broadcast interval is doubled if the collision ratio and the bandwidth efficiency estimated by a vehicle are greater than the predefined threshold value. Otherwise, the broadcast interval is reduced by a second.

Another protocol, Abiding Geocast [22], attempts to disseminate the safety warnings in an effective target region, where these warnings are necessary, relevant, and applicable. In case of an emergency or a hazardous scenario, a vehicle that detects it repeatedly broadcasts a warning packet. The warning packet specifies the target region where the warning is still relevant and should be kept alive. The vehicles that receive this warning message become an active relay node, and keep broadcasting the warning packet as long as they are still in the target region. The vehicles only stop broadcasting when they leave the target region. To keep the number of redundant transmissions to a minimum, each vehicle dynamically adjusts its rebroadcast interval, which is determined by its transmission range, speed, and distance from the hazardous area.

Furthermore, Segment-Oriented Data Abstraction and Dissemination protocol (SO-

DAD) [23] also exploits adaptive broadcast intervals to share traffic information of different road segments and avoid redundant rebroadcast packets. The broadcast interval is adjusted based on the information received from the neighbors. The information received by a vehicle is either classified as a provocation event, or a mollification event. Different weights are assigned to each event, and based on this weight, the broadcast interval is either increased or decreased. The performance evaluation presented in SODAD confirms that by using an adaptive broadcasting scheme, the number of packet collisions can be reduced as compared to periodic broadcasting schemes.

A different approach to enable traffic information sharing in autonomous vehicles has been proposed by CarSpeak [24], a communication system that provides vehicles with an access to sensory information captured by other vehicles in its vicinity. As the cars drive along the road, they are able to access the cloud server to obtain information related to a specific region of interest. In order to ensure a fair sharing scheme between vehicles, each geographical region is divided into smaller 3-D regions, and a higher access priority is given to the vehicles requesting the most popular information. However, a major downfall of CarSpeak is that it is not compatible with the existing IEEE 802.11 standards (requires changes to the MAC layer). Morever, CarSpeak requires WiFi access points along the road to attain the sensory information, which is not highly feasible.

As explained in this section, single-hop broadcasting schemes rely heavily on vehicle mobility, since vehicles carry the information with them while traveling and transmit to their one-hop neighbors during the next broadcast cycle (i.e. store-and-forward technique). Although single-hop broadcasting is efficient if the safety information has to be disseminated within short distances or in delay-tolerant scenarios, they are highly incapacitated if the communication needs to take place at greater distances and with low latency.

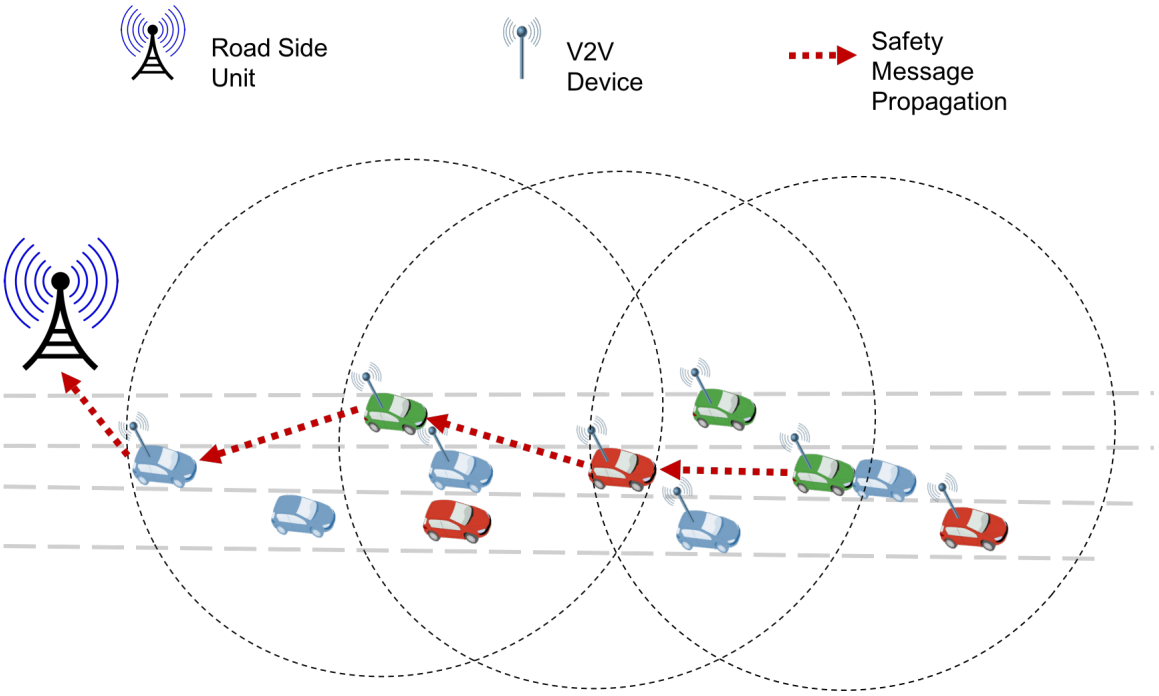


Figure 2.1: Multi-hop communication in VANETs.

2.2 Multi-hop Broadcasting

Several safety applications require that dedicated safety messages are disseminated quickly to vehicles well beyond the immediate transmission range of the sender. Therefore, in such scenarios, to cover the target region fully, multi-hop broadcasting schemes are often proposed to share the safety information, as shown in Figure 2.1. However, multi-hop communication in VANETs is a challenging task. Since no central administrator exists, fast propagation of messages through a multi-hop network is often difficult, as multi-hop increases the chances of a message collision. This problem becomes severe in dense urban areas where a higher traffic volume results in excessive communication failures. These failures deteriorate the reliability of reception and overall message dissemination speed.

Generally, in multi-hop broadcasting schemes in VANETs, the way in which a safety message is propagated along a roadway is that the original sender broadcasts the message to all vehicles within its transmission range. Following this, one or more nodes within

the transmission range are selected as forwarders to rebroadcast the safety message. This process is repeated until the safety message is disseminated in the entire VANET topology [25]. As mentioned earlier, a plethora of research work has been carried out recently to investigate and tackle the complexities associated with robustly and reliably disseminating safety messages in VANETs in a multi-hop manner. In this section, we review and discuss the existing multi-hop routing techniques by categorizing them into three classes: 1) Delay-based Approach, 2) Stochastic Approach, and 3) Network Coding-based Approach.

2.2.1 Delay-based Approach

Delay-based approach requires different waiting delays to be assigned to each forwarder candidate before rebroadcasting the message. The vehicle with the shortest waiting delay (and thus, the highest priority) gets to rebroadcast the message, while the other vehicles abort their own transmissions once they find out that the message has been rebroadcasted by another vehicle. Most of the existing research works use this delay-based approach. Such techniques use either timer-based delays or contention window-based delays to select a forwarder to rebroadcast the message. In timer-based mechanisms, a node defers the transmission based on a timer (whose timeout period is computed based on different parameters such as distance from the previous forwarder, node density, vehicle speed etc.), while contention window-based mechanisms require a node to defer its forwarding based on the contention window sizes.

One of the first timer-based techniques, Distance Defer Transfer (DDT) [26] assigns each forwarder candidate a waiting delay that is inversely proportional to it's distance from the previous forwarder. Therefore, the furthest forwarder candidate with the shortest waiting delay is able to rebroadcast the message. In this manner, the message is propagated further along the targeted region. Multi-hop Vehicular Broadcast (MHVB) [27] also uses a similar approach to assign the waiting delay to each forwarder candidate. However, both DDT and MHVB don't specify any particular equation and parameters to compute the wait-

ing time. Additionally, they don't address the collision scenario when multiple vehicles are located close to each other, thus having similar waiting delays.

On the other hand, Briesemeister and Hommel [28] and Inter-Vehicles Geocast (IVG) [29] proposed a multicast approach for VANETs that assigns waiting times (WT) to the forwarder candidates based on equation (2.1), where $MaxWT$ is the predefined waiting delay upper bound, $Range$ is the maximum transmission range, and $\hat{d}$ is the distance between the forwarder candidate and the previous forwarder. It can be noted from the equation that the calculated waiting time depends on the $MaxWT$ as well as $\hat{d}$. While a smaller $MaxWT$ will reduce the waiting delay before rebroadcasting , it will result in higher occurrence of packet collisions. Both of these protocols [28] and [29] do not provide a discussion on how to optimize $MaxWT$ and its impact on packet collisions. [28] simply sets the value of $MaxWT$ to $40ms$. These protocols only perform adequately under sparse network conditions.

$$WT(d) = MaxWT \; - \; \frac{MaxWT}{Range} \, . \, \hat{d} \tag{2.1}$$

Moreover, Streetcast [30] and Optimized Dissemination of Alarm Messages (ODAM) [31] also calculate the waiting delays of forwarder candidates as a function of distance in a manner similar to [28] and [29]. However, Streetcast [30] assumes that the vehicular network remains well-connected and thus, offers no solutions for disconnected vehicular networks. UV-CAST [32], on the other hand, attempts to fill this gap by addressing the disconnected network problem as well as broadcast storm problem [33] particularly for urban VANETs. In addition, UV-CAST also attempts to solve the limitations of [28] and [29] under dense network conditions.

Another protocol that also uses equation (2.1) to select forwarders to rebroadcast the safety message is Efficient Directional Broadcast (EDB) [34], which exploits the use of directional antennas. In particular, EDB proposes equipping the vehicles with two direc-

tional antennas, each with a 30-degree beam width. However, the directional antennas employed by EDB limit the propagation of the message to only certain areas as opposed to omni-directional antennas, which disseminate the message in all directions. Hence, EDB is not suitable for intersections. Yang and Chou [35] proposed the Position-based Adaptive Broadcast (PAB) protocol which makes message-relaying decisions at the receiver's end based on the position, direction, and velocity metrics of the sender and receiver pair. However, PAB shows significant improvement only in two-way highway scenario.

One of the major contributions toward delay-based message forwarding was by G. Korkmaz et al. [36], who proposed Urban Multi-Hop Broadcast (UMB) protocol to solve the broadcast storm problem, the hidden node problem, and the reliability problems in multi-hop broadcasting. UMB divided the sender's transmission range into several segments and assigned the highest rebroadcast priority to the forwarder candidates belonging to the furthest most segment. In UMB, to avoid collisions and solve the hidden node problem, the forwarder candidates utilize handshaking mechanisms such as Request-to-Broadcast (RTB) and Clear-to-Broadcast (CTB) prior to rebroadcasting the safety message. After a successful rebroadcast, the chosen forwarder sends an Acknowledgment (*ACK*) back to the original sender to ensure message propagation. However, collisions may still occur if multiple nodes exist in the furthest geographical segment and thus, cause the costly iterative rebroadcasting process to restart. Therefore, UMB encounters a serious latency problem under denser networks. Additionally, UMB assigns the longest waiting time (in the form of a jamming signal called black-burst) to the furthest forwarder candidates, which results in increased rebroadcast latency. Another protocol, Ad hoc Multi-Hop Broadcast (AMB) protocol [37], is an extension of the UMB protocol with a fully ad hoc intersection broadcast mechanism.

Smart Broadcast (SB) [4], a contention window-based forwarding technique, was proposed as an improvement over UMB, since it replaces UMB's complex and costly collision avoidance mechanism and instead, uses contention windows to resolve collisions among

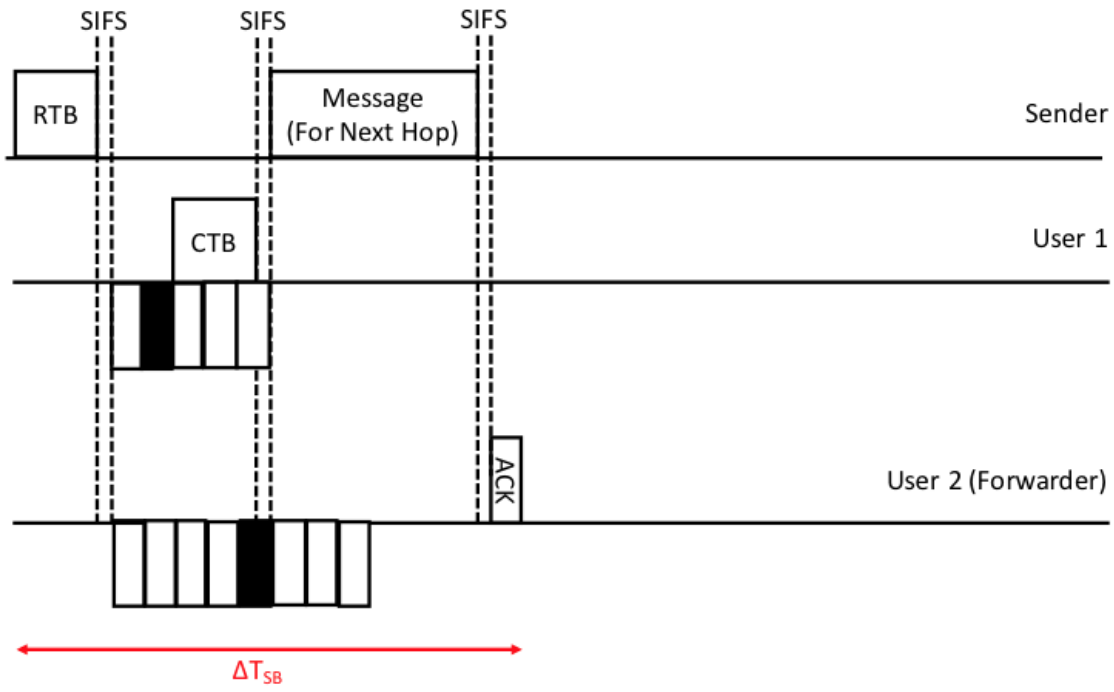


Figure 2.2: Timing diagram – Smart Broadcast protocol.

the forwarders. Moreover, SB assigns the shortest waiting delay to the furthest forwarding candidates before rebroadcasting. Hence, SB exhibits a significant delay and throughput improvement over UMB, as reported in [38]. Figure 2.2 depicts the timing diagram of the rebroadcast mechanism in SB. $\Delta\ T_{SB}$ refers to the time taken to rebroadcast the safety message.

Another contention window-based protocol, Binary-Partition-Assisted Broadcast (BPAB) [39] is also an improved form of UMB. Similar to UMB, BPAB also requires the RTB/CTB handshake, black-burst emission and area segmentation. However, unlike UMB and SB, BPAB proposes an enhanced binary-partition-based segmentation approach to repetitively divide the transmission range to obtain the furthest possible segment. A node belonging to this furthest segment is then randomly chosen to rebroadcast the message. In this manner, BPAB improves the rebroadcast efficiency by reducing the delay incurred during the forwarder selection process. However, large black-bursts result in increased latency in both

UMB and BPAB, especially in sparse network conditions.

Recently, a multi-hop broadcast protocol called RObust and Fast Forwarding (ROFF) [25] was proposed to reduce collisions and long waiting times. ROFF allows each node to decide its waiting times based on its own forwarding priority, which is acquired by sharing empty space distribution (ESD) bitmaps. However, in high-density networks, the overhead of ROFF is very large as ESD information is piggybacked in the broadcast data. Furthermore, a few other protocols that also exploit the delay-based multi-hop broadcasting approach include Reliable Broadcasting of Life Safety Messages (RBLSM) [40], Vehicle Density-based Emergency Broadcast (VDEB) [41], Simple and Robust Dissemination (SRD) [42], and Link-based Distributed Multi-hop Broadcast (LDMB) [43].

2.2.2 Stochastic Approach

Stochastic forwarding approach assigns a different rebroadcast probability (or forwarding probability) to each forwarder candidate. These forwarder candidates then rebroadcast the message according to their assigned probability. Therefore, a forwarder candidate with a higher rebroadcast probability is likely to have higher chances of being selected as a forwarder. In stochastic approach, the rebroadcast probability is assigned based on different factors such as distance from the previous forwarder, node density, vehicle speed etc. The most simplistic stochastic protocols involve assigning predefined fixed rebroadcast probabilities to the forwarder candidates. A key challenge in the stochastic approach is determining the optimal probability assignment function. Several protocols such as Weighted p-persistence [44], Optimized Adaptive Probabilistic Broadcast (OAPB) [45], and AutoCast [46] employ the stochastic based forwarding approach.

Wisitpongphan et al. [44] proposed the following fundamental stochastic forwarding techniques: weighted p-persistence, slotted 1-persistence, and slotted p-persistence. In weighted p-persistence technique, vehicles further away from the previous sender are assigned higher forwarding probability in order to maximize the message progress per hop.

Weighted p-persistence requires a forwarder candidate to rebroadcast a message based on its rebroadcast probability alone without any further contention. On the other hand, slotted 1-persistence scheme assigns each vehicle a forwarding probability of 1 to rebroadcast the message only within its particular time slot T_{Sij}. As shown in equation 2.2, T_{Sij} is a function of the predetermined number of slots (N_s), estimated one-hop delay (τ), distance of node i from the sender (D_i), and the transmission range of the sender (R).

Similar to slotted 1-persistence, slotted p-persistence also assigns a time slot to each forwarder candidate based on its distance from the sender. However, in slotted p-persistence, the forwarder candidates may rebroadcast with a probability p in their respective time slot only (p is inversely proportional to D_i). Similar to delay-based approach, a further vehicle is assigned a shorter waiting period (an earlier time slot) to rebroadcast in both slotted persistence techniques. However, a fundamental problem with these techniques proposed in [44] is that multiple forwarders might be selected to rebroadcast the same message in the target region, resulting in network flooding, collisions and inefficient channel utilization. Another limitation of these techniques is that they only consider the vehicles distance from the sender as a deciding parameter while forwarding the message.

$$T_{Sij} = N_s \,.\, \tau \left(1 - \left\lceil \frac{D_i}{R} \right\rceil \right) \tag{2.2}$$

Some stochastic protocols instead utilize the vehicle density (traffic congestion rate) to compute the forwarding probability including Optimized Adaptive Probabilistic Broadcast (OAPB) [45], AutoCast [46], Location-Based Flooding (LBF) [47], Probabilistic Inter-Vehicle Geocast (p-IVG) [48]. In these protocols the nodes in the congested area either lower their forwarding probabilities or drop the packets altogether. However, in such protocols, the average distance progressed per hop is negatively affected as furthest vehicles are not always selected as forwarders.

On the other hand, Network Topology p-Persistence (NTPP) [49], Irresponsible Forwarding (IF) [50], and Collision-Aware REliable FORwarding (CAREFOR) [51] consider both distance and vehicle density while assigning the forwarding probability to the vehicles. In such protocols, the furthest vehicles have highest forwarding probability. Furthermore, vehicles in sparse regions have a higher forwarding probability as compared to vehicles in dense regions. This helps in reducing collisions and network flooding. However, NTPP, IF and CAREFOR still face performance degradation with respect to one-hop progress during each rebroadcast, since the furthest forwarder candidates (with high forwarding probabilities) might cancel their scheduled rebroadcast.

Although a lot of research has been done to address the shortcomings of stochastic-based techniques, the following two problems still persist. First, the unnecessary broadcasts from multiple forwarder candidates puts an undue burden on network resources. Second, the one-hop message progress achieved might only be a fraction of the total transmission range, if the furthest forwarder candidates cancel their scheduled forwarding.

2.2.3 Network Coding-based Approach

Recently, network coding techniques have been employed in wireless ad-hoc networks to achieve a higher throughput. Network coding reduces the required number of transmissions, which helps in utilizing the bandwidth more efficiently. The concept of network coding was first introduced in [52]. Many studies have investigated the impact of network coding on multi-hop broadcasting in mobile ad-hoc networks such as CODEB [53], EBCD [54], DiFCode [55], and so on. These network coding-based broadcast protocols select a subset of neighboring nodes, which then performing the forwarding task deterministically. Although these protocols could potentially be adapted for VANETs as proposed by [6], there is no existing research that shows their performance in a dynamic vehicular enviroment. On the other hand, a few recent works have tried to exploit network coding for multi-hop information dissemination in VANETs.

Wu et al. [56] proposed a protocol that uses dynamic backbone and network coding to enable multi-hop broadcasting in VANETs. In particular, [56] uses network coding for reducing protocol overhead and improving the packet reception probability. Another protocol FUZZBR-NC [57] selects relay nodes by considering the inter-vehicular distances, node mobility, and signal strength based on fuzzy logic and network coding. However, most of these network coding-based protocols do not present a comprehensive comparison against the more frequently used delay-based or stochastic-based techniques in VANETs.

In conclusion, multi-hop broadcasting in VANETs is an open-ended and complex problem that requires considerable improvements to ensure low forwarding latency, reliable safety message delivery, minimal collisions, and so on. In this chapter, we identified the shortcomings of the existing multi-hop and single-hop broadcasting schemes. In the next chapters, we propose novel and efficient broadcasting protocols that address the limitations of the existing schemes and enable fast and reliable dissemination of safety messages in VANETs.

CHAPTER 3

FAST AND RELIABLE MULTI-HOP BROADCASTING IN VANETS

As mentioned previously, to improve the overall transportation safety, fast and reliable safety message dissemination is the key objective in a highly dynamic VANET environment. Recently, many protocols and schemes have been proposed to efficiently share safety messages using multi-hop broadcasting in VANETs, as discussed in Chapter 2. However, most of these existing techniques do not perform well under real-world traffic conditions, or perform adequately only under very limited scenarios and traffic conditions. In this chapter, we present a highly efficient and reliable multi-hop broadcasting protocol, Intelligent Forwarding Protocol (IFP), that exploits handshake-less communication, ACK Decoupling and an efficient collision resolution mechanism. Additionally, this chapter presents the detailed derivation and validation of the theoretical model of IFP. Toward the end, the optimal parameter choice for the protocol has been discussed. The work presented in this chapter also appeared in [12], [13], and [14].

3.1 Intelligent Forwarding Protocol

3.1.1 Motivation and Contribution

Ensuring rapid propagation of safety messages in a reliable manner is one of the biggest challenges in VANETs [25] due to vehicle movements, limited wireless resources, lossy characteristics of wireless communication, and so on. To address this challenge, we propose an innovative and robust multi-hop broadcasting protocol, known as Intelligent Forwarding Protocol (IFP), that exhibits high performance gain in terms of speed and reliability as compared to existing schemes. Here, we highlight the major improvements and contributions of IFP as compared to the existing techniques.

Firstly, most of the existing multi-hop broadcasting protocols exploit the vehicles' geographical information only (i.e. GPS coordinates) in the forwarder selection process (e.g. DDT [26], MHVB [27], Briesemeister and Hommel [28], IVG [29], UMB [36], SB [4], etc). However, such protocols are not very reliable or accurate as they do not consider terrain interference, signal characteristics, GPS errors, malicious nodes injecting false GPS values, and so on. On the other hand, protocols such as SLBP [58], which simply choose the forwarders based on the SNR level of the received signal, exhibit severe performance degradation due to an absence of contention resolution mechanism, a flawed approach of choosing a low SNR level as an indication of furthest nodes from the sender, and so on. To counter these limitations, IFP proposes a smart mechanism of exploiting both the SNR values and the GPS coordinates in the forwarder selection process, resulting in higher efficiency and reliability.

Secondly, many traditional delay-based broadcasting algorithms in VANETs (such as UMB [36], SB [4], BPAB [39], etc.) use handshaking mechanisms (RTB/CTB) before broadcasting the safety message, and *ACKs* afterwards. This sequential process introduces overheads and thus, reduces the message dissemination speed. Therefore, IFP removes the need for these costly handshaking mechanisms. In addition, IFP also decouples *ACKs* from the message dissemination process, further reducing the delays.

Additionally, as opposed to the stochastic-based protocols, IFP reduces the network load by removing unnecessary rebroadcasts from multiple forwarder candidates, and improves the one-hop message progress (average distance covered during each hop) by ensuring that the furthest forwarder candidates win the contention to rebroadcast. Furthermore, IFP reduces the collision occurrences and average waiting times before rebroadcasting by choosing the optimal forwarders. IFP also introduces an improved collision resolution mechanism, such that packet collisions could be resolved quickly. Finally, contrary to most existing protocols that perform adequately only under certain scenarios, IFP performs optimally under all network and traffic conditions.

3.1.2 Protocol Design

This section describes the key design principles of IFP. Since IFP removes the handshake process (exchange of RTB/CTB packets) prior to the message broadcast, the original sender (safety message initiator) simply accesses the medium using the standard 802.11 CSMA/CA technique and broadcasts the safety message, if the channel is idle. Upon message reception, each node i in the vicinity of the sender (i.e. within its transmission range R) calculates its corresponding SNR value (SNR_i) and its Euclidean distance (D_i) from the sender using the GPS coordinates. Each receiver then uses these calculations to compute its own maximum contention window size (CW_{max}) according to the following equation (3.1):

$$CW_{max} = k\frac{D_{max}}{D_i}\, CW_{base}^{\left(\frac{SNR_i - SNR_{thresh}}{\alpha dB}\right)} \tag{3.1}$$

Here, k is a scaling factor to contain CW_{max} values within a suitable range (the contention window range is typically [0, 1023] but it could be optimized under different traffic conditions, as discussed later in this chapter), D_{max} (or R) is the maximum transmission range of the sender, SNR_{thresh} is the minimum SNR threshold value (in dB) allowed for reliable transmission in VANETs, α is the exponential scaling factor to effectively accommodate the effect of SNR_i while determining CW_{max}, and CW_{base} is the contention window base value that can be optimized based on the density of the network.

After calculating the CW_{max}, each node then chooses a random time slot CW_{chosen} in the range [0, CW_{max}] and waits for that amount of slot times. The node with the smallest CW_{chosen} value wins the contention and is chosen as the forwarder, hence, rebroadcasting the safety message. All of the remaining contending nodes, after receiving this rebroadcast message from the forwarder, drop out of the rebroadcasting race. Note that in IFP, nodes further away from the sender are more likely to be chosen as forwarders, thus improving the one-hop message progress. Additionally, this unique approach of selecting forwarders

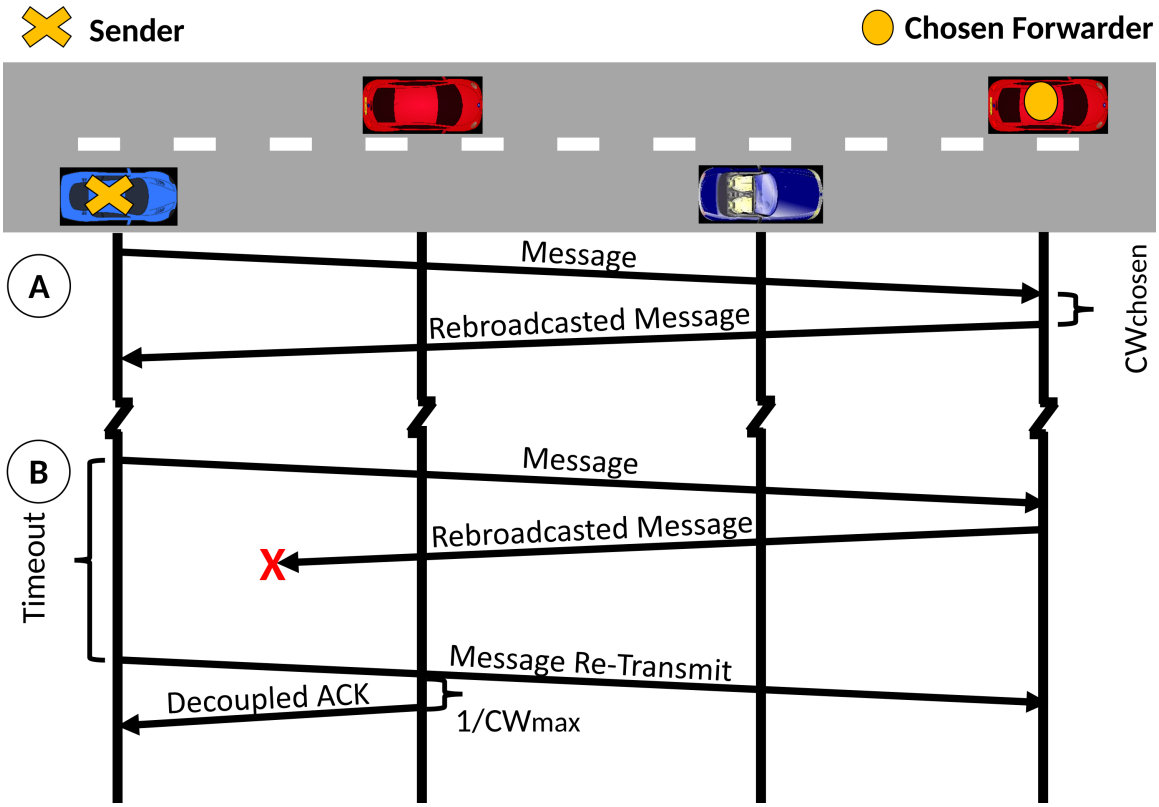


Figure 3.1: Sequence of packets being transmitted under: (A) normal rebroadcast scenario, (B) ACK decoupling and recovery process. *Not drawn to scale*

based on nodes' GPS coordinates and SNR values, helps counter the effects of terrain interference, signal characteristics, GPS errors, malicious nodes injecting false GPS values, and other limitations that exist in the existing traditional schemes. This mechanism of forwarder selection and rebroadcasting the safety message (which also acts as an implicit ACK to the sender) is portrayed in Figure 3.1.A.

Due to IFP's smart forwarder selection mechanism and the omni-directional nature of message broadcasts, the sender is almost always able to overhear the rebroadcast message from the forwarder, thus eliminating the need for a costly *ACK*-ing process. As a result, the safety message can progress without having to wait for the successful reception of an *ACK*, as opposed to the traditional multi-hop protocols such as UMB [36], SB [4], etc. Eliminating the *ACK* dependency yields a significant delay improvement in IFP. However, under

certain rare circumstances where the sender might be unable to overhear the rebroadcast message due to the backward communication channel being lossy or the forwarder node moving out of the vicinity of the sender, as depicted in Figure 3.1.B, IFP proposes the following *ACK* Decoupling and Recovery mechanism: If the previous sender (source) does not receive the rebroadcasted message from the forwarder within a predefined time-out period, it will once again broadcast the safety message. Upon getting the same message twice from the source, a node in the vicinity of both the source and the forwarder will send an explicit *ACK* to the source to cancel any further re-transmissions. However, this *ACK*-ing process is totally independent and decoupled from the message propagation progress, and thus, will not contribute toward the message propagation delay at all.

Although the *ACK*-ing process does slightly increase the collision probability in the vicinity of the sender, these collisions are drastically reduced in IFP by choosing the node closest to the sender for sending *ACK* as well as by limiting the power with which the *ACK* is transmitted. To determine the optimal node for *ACK* transmission, the exact opposite of the contention process proposed by equation (3.1) is used. In this way, a node closest to the sender and with a strong SNR_i is prioritized to send an *ACK* back to the sender. Nevertheless, the best way to completely eliminate the need for *ACKs* is to select SNR_{thresh} with an extra power budget (more than 3 dB), so that the sender is always able to overhear the broadcasted messages from the forwarder, and the entire need for the *ACK* decoupling procedure is removed. Note that the additional power budget to add a few more dB in SNR_{thresh} will only slightly reduce the distance between the sender and the chosen forwarder, since the receiving power in typical mobile environments is inversely proportional to the 4th power of distance.

Figure 3.2 is a graphical demonstration of Receiver 2 ($R2$) recovering the *ACK*, while the message propagation process is continued in parallel by Receiver 1 ($R1$). This ACK recovery process occurs after both of the following events: 1) the forwarder $R1$ rebroadcasts the safety message at t_1, and 2) the sender S re-transmits the message again at t_2 (which is

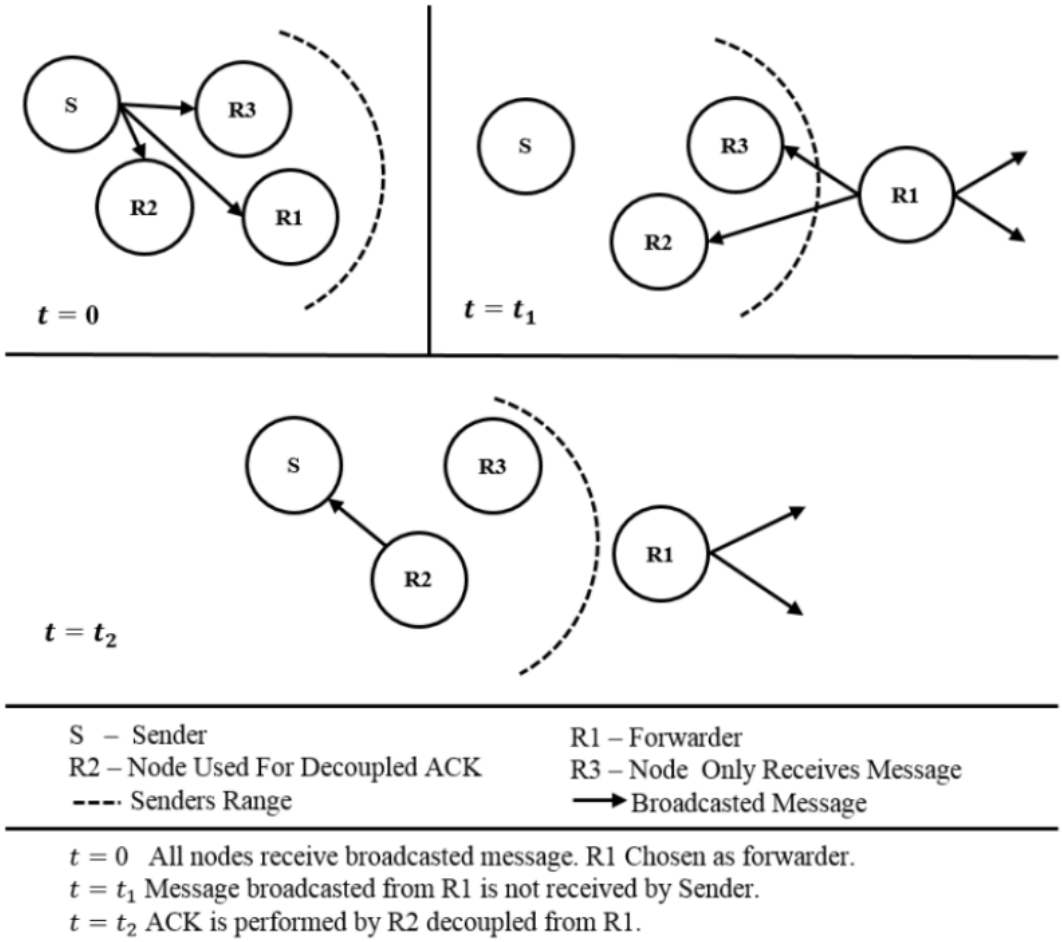


Figure 3.2: ACK decoupling and recovery mechanism. *Not drawn to scale*

the time-out period).

In a typical VANET environment, even with a large number of message broadcasts (usually 10/sec/node), only a few safety messages actually collide, as safety messages are quite small in size and are randomly distributed over time. Once a collision does occur in IFP, it can simply be resolved by the quicker of the following two mechanisms: 1) by selecting the next node (other than the two nodes involved in collision) that wins the contention to be the forwarder, as shown in (Figure 3.3.A), or 2) by repeating the contention resolution procedure between the colliding nodes until the message gets successfully rebroadcast, as depicted in (Figure 3.3.B). Note that in this second mechanism, the nodes use the same

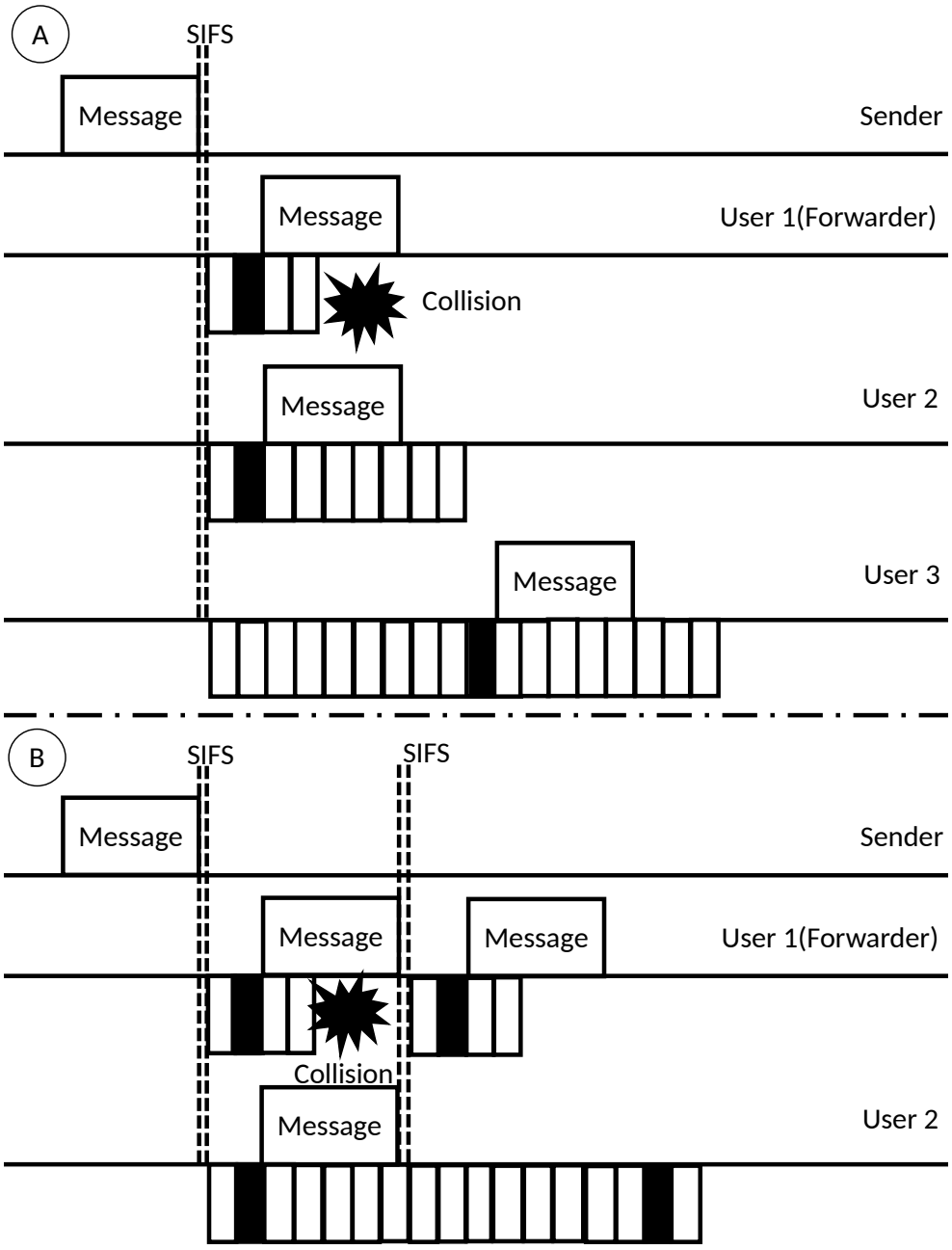


Figure 3.3: Collision resolution mechanism. *Not drawn to scale*

CW_{max} as computed before, but with a new random time slot (CW_{chosen}) to rebroadcast the safety message. Out of the above two techniques, the one through which the forwarder is selected the earliest is used to resolve collisions in IFP. To the best of our knowledge, this novel mechanism introduced in IFP to resolve collisions in a VANET environment by

selecting the quicker of the two aforementioned mechanisms, has been proposed for the first time. The improved collision resolution mechanism results in a significant reduction in the overall message propagation delay.

Lastly, if the sender does not receive a message back from any forwarder within the time-out period due to unavailability of nodes in the transmission range, the entire forwarder selection mechanism is repeated over again.

Figure 3.4 shows a flow chart describing the design procedures executed at each i-th node. As can be noted, the proposed protocol is a distributed algorithm where all nodes cooperate to help in safety message dissemination in VANETs. Due to the advancements and novelties discussed earlier, IFP significantly improves the rate at which the message is propagated along the VANET as compared to the traditional protocols.

Next, we present a design comparison of IFP and a traditional handshaking-based Smart Broadcast (SB) protocol [4] with the aid of timing diagrams. In Figure 3.5, a detailed timing diagram is presented to illustrate message transmission and delay during a normal rebroadcast scenario in both SB and IFP. It can be noted that IFP removes the handshake process (exchange of RTB/CTB packets) prior to the message broadcast and *ACKs* afterwards.

On the other hand, Figure 3.6 depicts a scenario when a collision occurs while rebroadcasting the safety message. As shown in Figure 3.6.A, once a collision occurs in SB, the two nodes involved in collision remain in the contention phase, and the node with the next minimum back-off sends the CTB and is selected as a forwarder. As for the collision resolution process in IFP, Figure 3.6.B-1 illustrates the first mechanism, where the nodes involved in collision back-off for a random time slot (CW_{chosen}) in the range [0, CW_{max}] to rebroadcast the message and repeat this cycle until the collision has been resolved. Figure 3.6.B-2 portrays the second mechanism, whereby a third node wins the contention and is selected as a forwarder before the two colliding nodes could recover from the collision.

Figure 3.5 and Figure 3.6 show that IFP significantly improves the rate at which the message is propagated along the VANET as compared to the traditional SB protocol. These

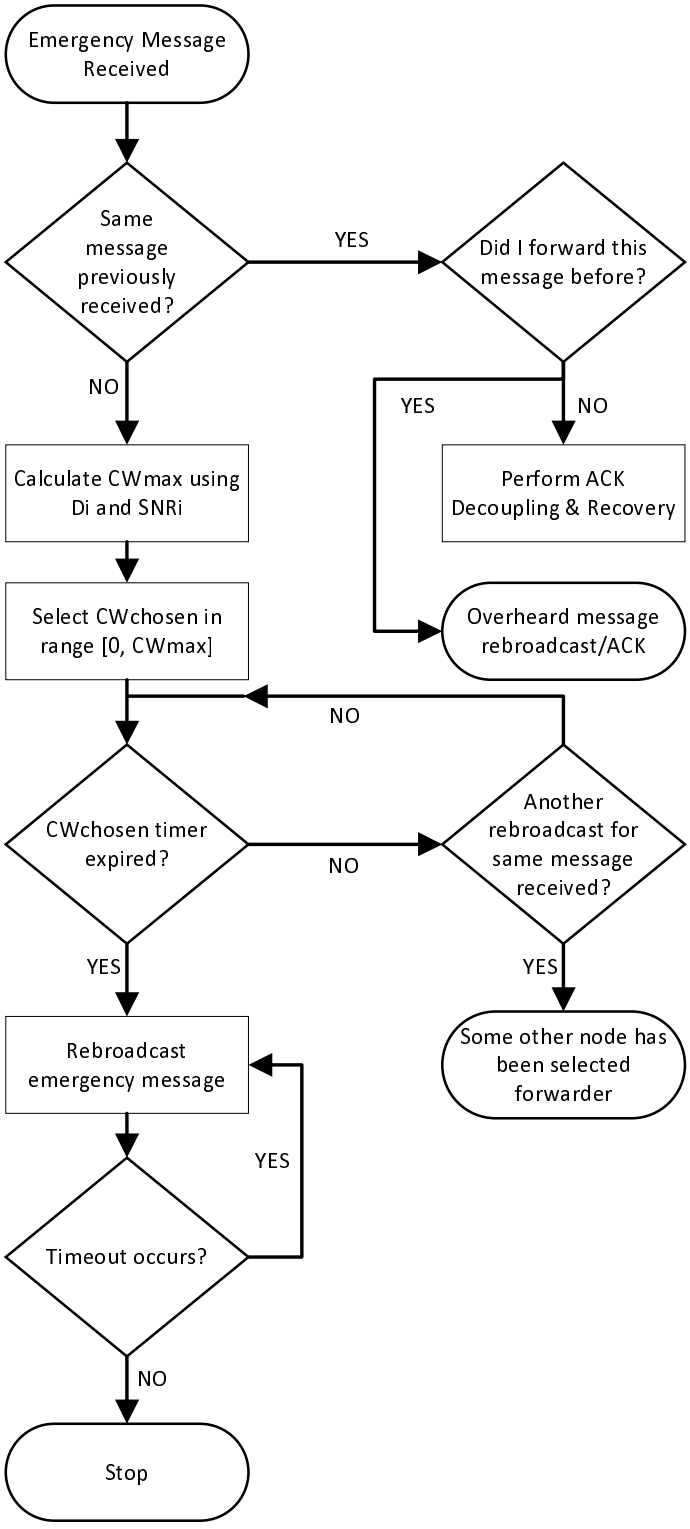


Figure 3.4: Flow chart describing key design steps at each $i-th$ node.

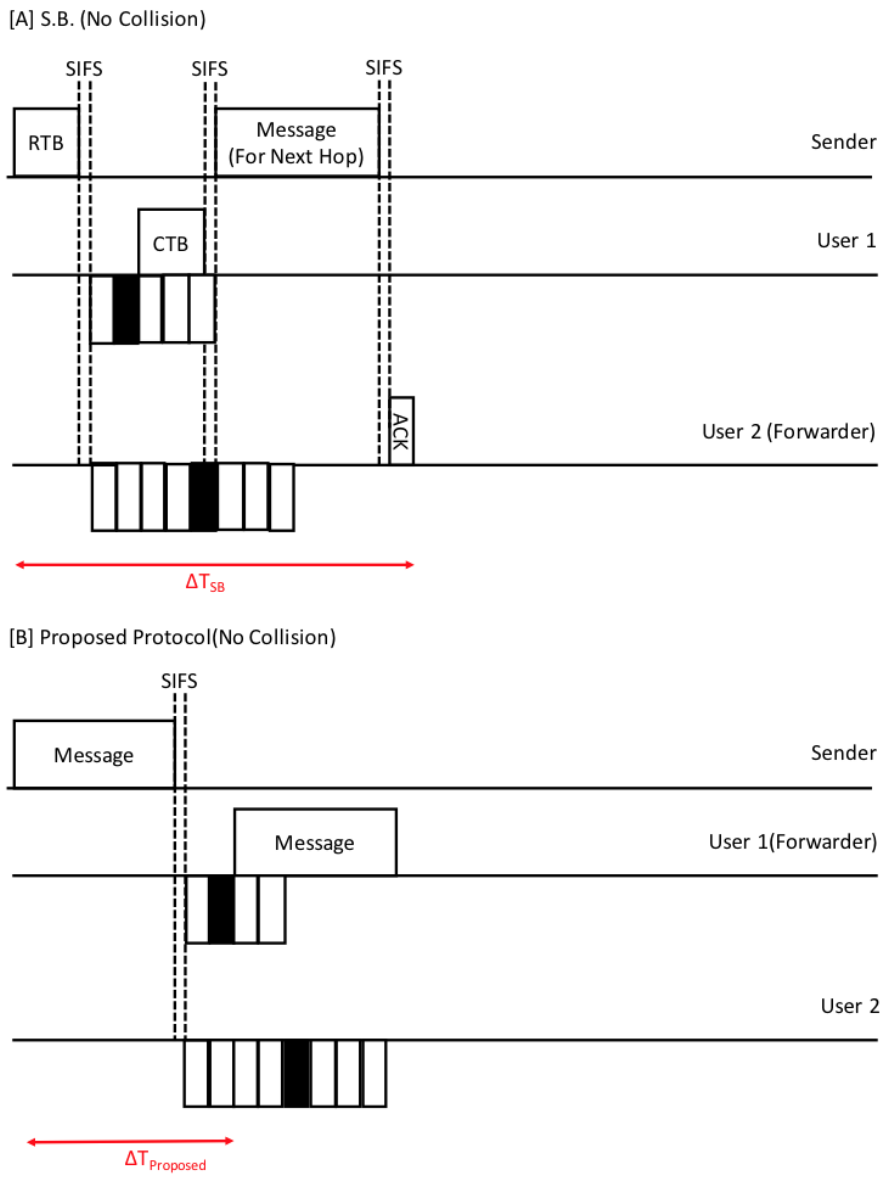


Figure 3.5: Timing diagram – Normal rebroadcast scenario (SB vs. IFP).

results are verified later in the thesis.

3.2 Theoretical Analysis

In this section, we present the theoretical analysis of IFP to establish and validate its effectiveness, robustness and reliability. The expressions constructed and analyzed include per-hop rebroadcast latency (T_{HOP}), average one-hop message progress (D_{AVG}), and av-

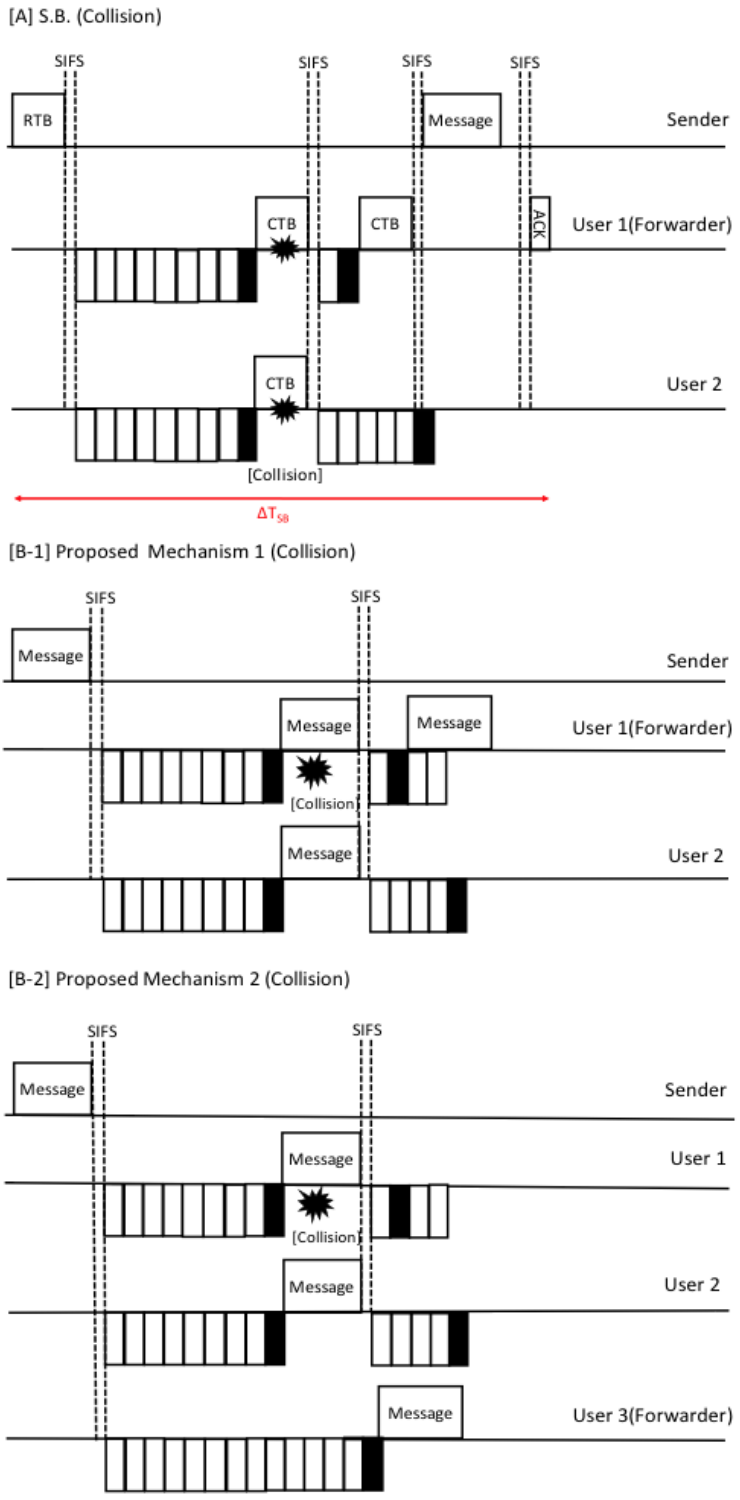


Figure 3.6: Timing diagram – Collision scenario (SB vs. IFP).

erage message dissemination speed (v). First, the theoretical model of IFP is described, along with the assumptions and hypothesis. Then, we present the results and analysis, as well as suggest the optimal parameters to improve IFP's performance.

3.2.1 Theoretical Model

Prior to presenting the expressions constructed for theoretical analysis, we first lay down some basic assumptions and hypothesis. The highway scenario has been analyzed, whereby a safety message is propagated along a rectangular strip of length R, which is equivalent to the typical transmission range of a vehicle. Therefore, nodes within this range from the sender will be able to hear the broadcast message, considering good channel conditions. The nodes are distributed along the road strip following a bi-dimensional Poisson process with the parameter λ nodes per strip. In comparison to the sender, the nodes moving in the same direction of message propagation have a small relative velocity, which is negligible compared to message propagation speed. Hence, we assume that nodes do not leave the transmission range R of the sender during the contention period.

Once the sender broadcasts the safety message, each i-th node within the range R chooses a random time slot $CW_{chosen,i}$, in the range [0, $CW_{max,i}$], as described in section 3.1. Note that according to IFP, each node chooses its time slot independently of any other node. We denote N_x to be the total number of nodes that choose the x-th time slot. Therefore, under these assumptions, N_x are independent and identically distributed (*i.i.d.*) Poisson random variables with the parameter $\hat{\lambda} = \lambda/(E[CW_{chosen}])$. Here, $E[CW_{chosen}]$ corresponds to the expected number of time slots that a node has to wait for, before it can rebroadcast the message. Since the nodes are within a relatively short distance of each other ($< R$), the message propagation time is almost negligible. Hence, the time slots for all nodes are assumed to be synchronized. At any x-th time slot, one of the following three events occurs:

1. If $N_x = 0$: The channel remains Idle (I).

2. If $N_x = 1$: Exactly one node broadcasts the message, resulting in Success (S).

3. If $N_x > 1$: Multiple nodes attempt to rebroadcast in the same time slot, resulting in Collision (C).

Based on the *i.i.d.* Poisson random variable property of N_x (as described earlier), each of these events occur with the following respective probabilities:

$$P_I : P_r(N_x = 0) = \frac{(\hat{\lambda})^0 e^{-\hat{\lambda}}}{0!} = e^{-\hat{\lambda}} \; ; \tag{3.2}$$

$$P_S : P_r(N_x = 1) = \frac{(\hat{\lambda})^1 e^{-\hat{\lambda}}}{1!} = \hat{\lambda} e^{-\hat{\lambda}} \; ; \tag{3.3}$$

$$P_C : P_r(N_x > 1) = 1 - P_I - P_S = 1 - e^{-\hat{\lambda}}(\hat{\lambda} + 1) \; ; \tag{3.4}$$

where P_I is the probability of having an idle time slot, P_S is the probability of having a successful message rebroadcast in the time slot, and P_C is the probability of having a collision in the time slot.

3.2.1.1 Per-Hop Rebroadcast Latency

The first expression constructed is for mean per-hop rebroadcast latency (T_{HOP}), the average time between a node receiving a safety message from the previous sender and rebroadcasting it. We denote T_I to be the time taken for event I, T_S for event S, and T_C for event C respectively. While T_I requires a single time slot, T_S and T_C take message transmission/reception time (including message propagation delay), followed by SIFS. Let us denote T_F to be the average time spent during a failure event i.e. either the time slot is

wasted (I) or a collision occurs (C). Therefore, T_F can be calculated as follows:

$$T_F = T_I \frac{P_I}{P_I + P_C} + T_C \frac{P_C}{P_I + P_C} \tag{3.5}$$

The average number of failure events (N_F) before a subsequent success event (successful rebroadcast) is given by the following expression:

$$N_F = \frac{1 - P_S}{P_S} \tag{3.6}$$

Next, we construct an expression for T_Z, which is the time wasted if no forwarder candidates (exactly zero forwarders) exists within the range R of the sender:

$$T_Z = P_Z \cdot T_o \tag{3.7}$$

where T_o is the time-out value, P_Z is the probability of having zero forwarder candidates in range R and can be approximated as $e^{-\lambda}$ (Note: $\lambda = \hat{\lambda}\ .\ E[CW_{chosen}]$). Finally, the expression for mean per-hop rebroadcast latency of IFP is:

$$T_{HOP} = N_F T_F + T_S + T_Z \tag{3.8}$$

3.2.1.2 Average One-Hop Message Progress

Next, we derive the expression for average one-hop message progress (D_{AVG}), the average distance covered by the message in a single hop. If the exact geographical location of each node in the strip is known, the approximate distance between the sender and forwarder (D_F) can be computed as follows:

$$D_F = \sum_{i=1}^{total\ nodes} (W_i D_i) \tag{3.9}$$

where D_i is the distance between each i-th node and the original sender, and W_i is the weight assigned to each i-th node based on its $CW_{max,i}$ value (which is a function of its distance and SNR value). As the node intensity in the road strip increases, the probability of having a node closer to the boundary of the range R also increases. These furthest nodes have the highest probability of being chosen as forwarders. Therefore, a greater weight is assigned to the furthest forwarder candidates during the forwarder selection process. W_i can be calculated as follows:

$$W_i = \frac{1}{CW_{max,i} \cdot \sum_{m=1}^{\lambda} \frac{1}{CW_{max,m}}} \tag{3.10}$$

Let us assume that the λ nodes are spatially placed along the road strip at a regular interval such that each node (except sender and the last node) is equidistant from two other nodes, and that the furthest node within the transmission range R is chosen as the forwarder. Hence, the average one-hop message progress (D_{AVG}) of IFP can be given by:

$$D_{AVG} = \frac{\lambda - 1}{\lambda} \cdot R \tag{3.11}$$

3.2.1.3 Average Message Dissemination Speed

Lastly, we create an expression for the average message dissemination speed (v), which can be defined as the ratio between the average one-hop message progress and per-hop rebroadcast latency:

$$v = \frac{D_{AVG}}{T_{HOP}} \tag{3.12}$$

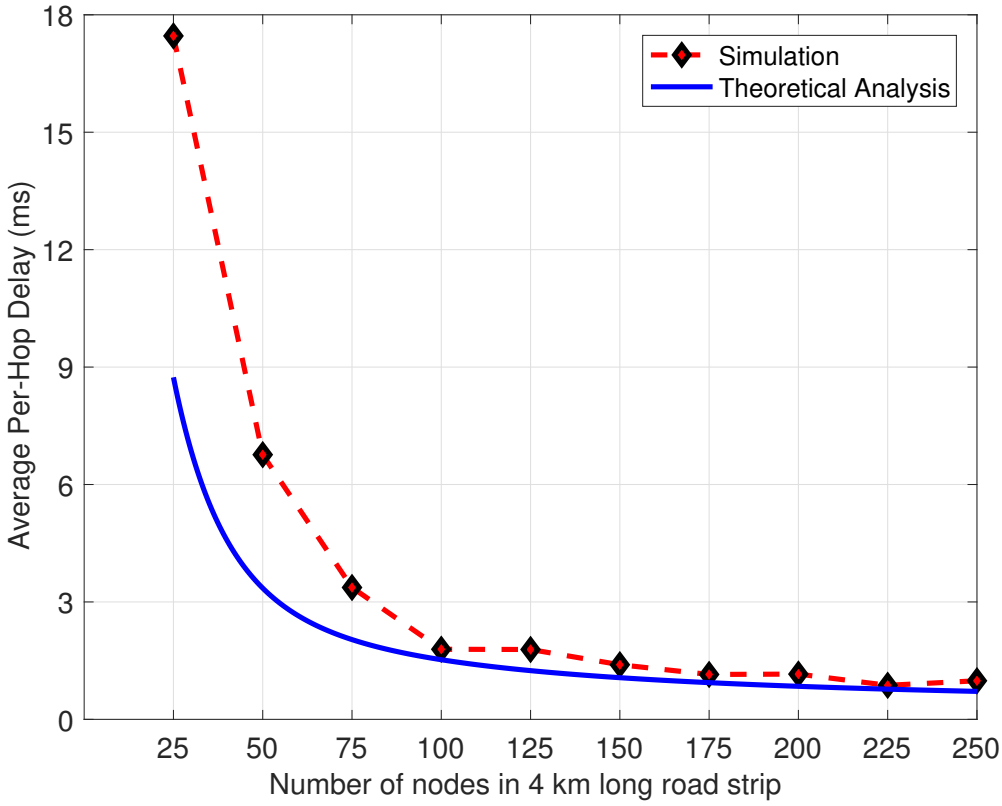


Figure 3.7: Avg. per-hop rebroadcast latency (T_{HOP}) - Theoretical vs. simulation results.

3.2.2 Validation of Theoretical Model

Next, we present a comparison of the theoretical and simulation results of IFP to validate the mathematical model constructed above. The simulations were conducted using the latest version of ns-3, a discrete-event network simulator. The simulation environment and parameters are discussed in detail later in Chapter 4 and in Table 4.1 respectively. In order to closely align the simulation environment with the theoretical model, we ensure that no background messages (other than the safety message) exist in the simulation scenario. Similar parameters were chosen for both simulation as well as theoretical analysis to achieve a fair comparison. Since the theoretical model analyzes a highway scenario, we vary the node intensity between 25 to 250 vehicles (in a $4\ km$ long road strip), which corresponds to the typical highway traffic conditions.

A key performance metric analyzed was the average per-hop rebroadcast latency (T_{HOP}). Figure 3.7 shows the average per-hop rebroadcast delay vs. the node intensity in a $4\ km$ long road strip. As shown in the figure, under sparse traffic conditions (e.g. around 25 nodes), the average per-hop delay for both theoretical results as well as simulation results is much larger as compared to slightly denser traffic conditions ($<$100 nodes). The reason is that under sparse traffic conditions, it is highly probable that there is no node present within the transmission range (R) of the sender to rebroadcast the message, resulting in time-outs, which impact the delay values quite adversely. It can also be noted from Figure 3.7 that simulation results generally depict higher delays as compared to theoretical results. This behavior can be attributed to the fact that simulation environments consider many realistic limitations, which the mathematical analysis tend to ignore, such as the signal fading model (Nakagami fading model), channel conditions, medium characteristics and so on. These limiting factors lead to an increase in the delay values of simulation results. Moreover, in fairly dense traffic conditions ($>$ 200 nodes), the delay reduces to a significantly low value of almost 1 ms. This happens because, under such conditions, the chances of having a node closer to the boundary of the transmission range (with a small CW_{max} value) are quite high, thus reducing the average waiting time before a message rebroadcast. Overall, the results of theoretical analysis and simulation are conforming.

Similarly, Figure 3.8 depicts average one-hop message progress (D_{AVG}) i.e. the average distance covered by the safety message during a single successful broadcast. It can be noticed from Figure 3.8 that as the number of nodes increase, the average distance covered by the message across a hop also increases. At higher node intensities, the probability of having a node closer to the edge of the sender's transmission range R increases. Therefore, the forwarder selected to rebroadcast the safety message will likely be further away from the sender. Thus, the message will travel a greater distance on average; however, as the node intensity increases further, the distance growth steadies toward the maximum transmission range (300 $meters$). Once again, the simulation and theoretical results match.

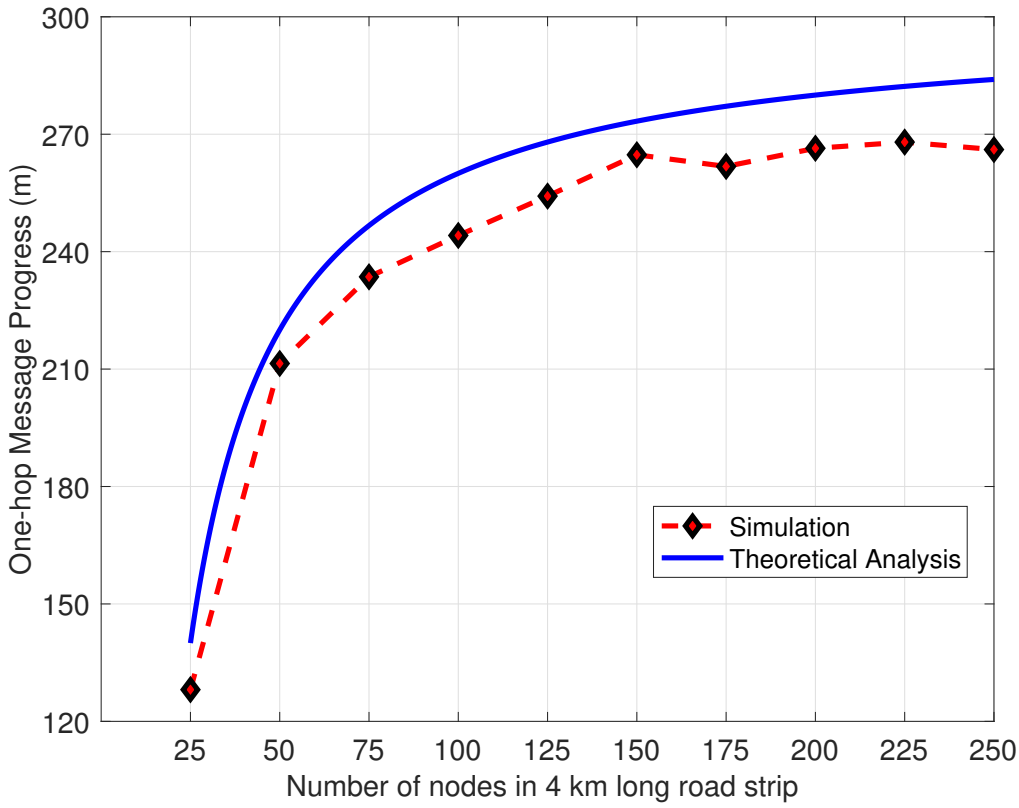


Figure 3.8: Avg. one-hop message progress (D_{AVG}) - Theoretical vs. simulation results.

Finally, Figure 3.9 shows the message propagation speeds (v) obtained by the theoretical and simulation results. As can be noted, the speed is generally increasing for both environments with the increase in node intensity. This upward trend occurs because as the number of nodes increase toward 225 nodes, the average per-hop delay decreases, whereas the distance progressed per-hop increases (as explained previously). Again the slight difference between the theoretical results and the simulation results is due to the lack of consideration of channel characteristics and other physical attributes in the theoretical model. However, both the curves are relatively matching with a similar trend.

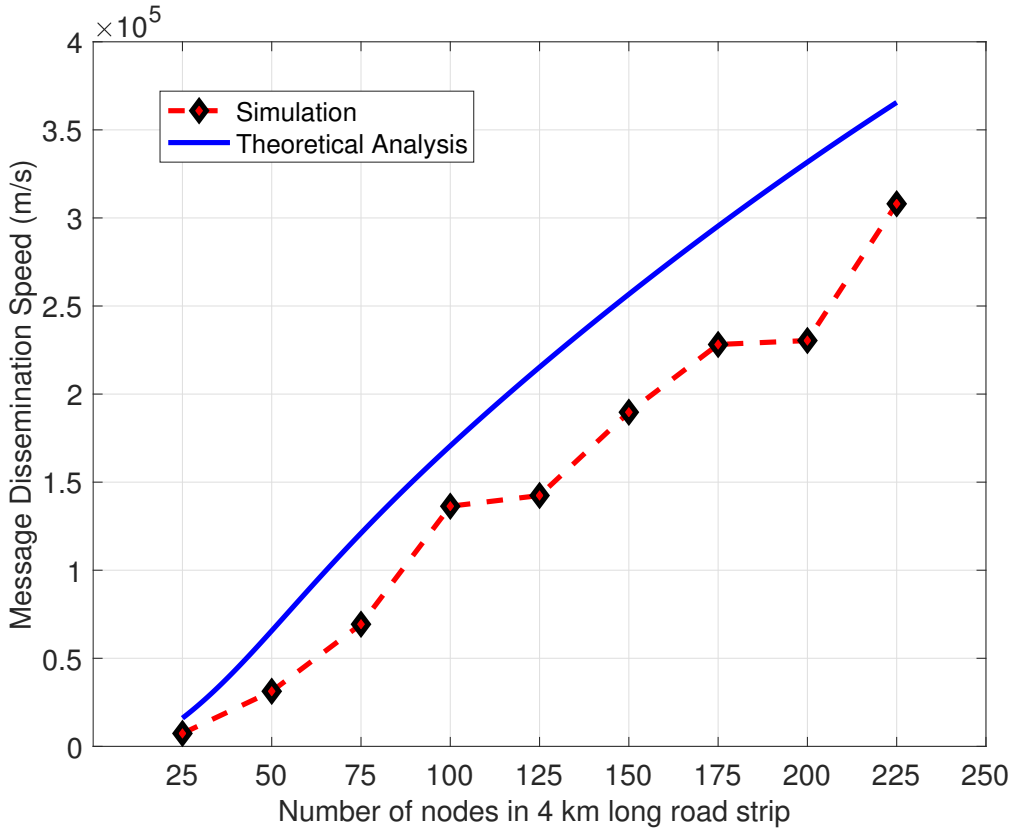


Figure 3.9: Avg. message dissemination speed (v) - Theoretical vs. simulation results.

3.2.3 Delay Comparison with Simple Delay-Based Protocol

To evaluate the performance of IFP, we compare the theoretical per-hop rebroadcast delay (T_{HOP}) results of IFP with a representative delay-based multi-hop broadcasting protocol, which we refer to as Simple Delay-Based (SDB) protocol. SDB closely follows a widely-popular technique proposed by a number of different protocols such as Briesemeister and Hommel [28], IVG [29] , Streetcast [30], ODAM [31], and EDB [34] etc., and uses equation (2.1) for the forwarder selection process. Note that in this comparison, we do not include any stochastic-based protocols since deriving an accurate mathematical delay expression for such protocols is highly complex and non-trivial, and not the objective of this research. Moreover, to the best of our knowledge, the existing literature does not provide any generic mathematical model for stochastic-based multi-hop broadcasting protocols. To

evaluate the IFP delay results, equation (3.8) is used. On the other hand, for SDB, the following per-hop rebroadcast latency expression is used:

$$T_{HOP}(SDB) = (1 - P_C) \cdot (MaxWT - WT_f) + P_C(MaxWT) + T_Z \quad (3.13)$$

where P_C is the collision probability (extrapolated from results published in ROFF [25]), $MaxWT$ is the predefined waiting delay upper bound, WT_f is average waiting time of a forwarder candidate before a rebroadcast, and T_Z refers to the time wasted in case of time-outs (because of no nodes present within the transmission range R); T_Z can be calculated using equation (3.7). Note that the time-out period (T_o) directly corresponds to $MaxWT$.

Figure 3.10 depicts the comparison between the theoretical T_{HOP} results of IFP and

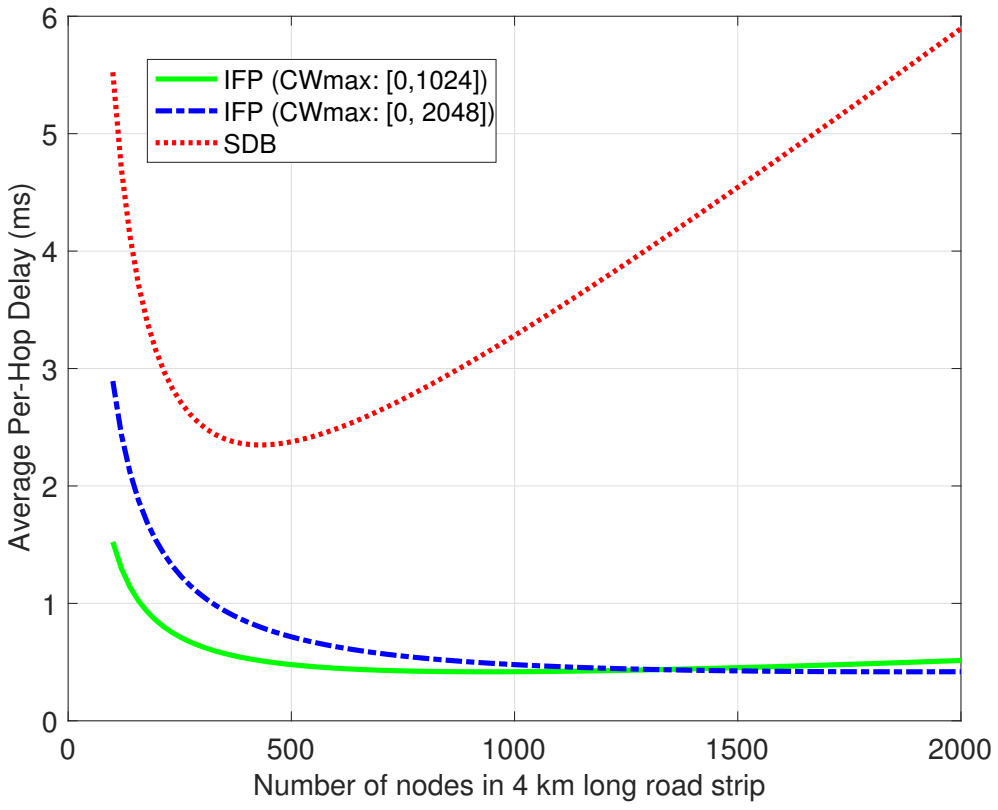


Figure 3.10: Theoretical delay comparison between IFP and SDB.

SDB. Similar to the simulation results, IFP again exhibits a significant delay improvement over SDB as shown in Figure 3.10. In theoretical results, this improvement in T_{HOP} results of IFP can be contributed to various factors such as shorter average waiting time before forwarding, less collision occurrences, robust collision resolution mechanism (in case of collisions), and so on. As shown in Figure 3.10, under sparse traffic conditions ($\approx 100\ nodes$), all protocols depict high T_{HOP} values due to time-out occurrences; however, IFP still fares better due to shorter time-out periods before message re-transmission. As the traffic intensity increases further (till 450 nodes for SDB, and 1500 nodes for IFP), T_{HOP} values gradually reduce in both protocols due to shorter average waiting times assigned to forwarders (as nodes are now closer to the boundary of sender's transmission range R). At greater than 450 nodes, SDB's delay values start rising due to increased number of collisions and re-transmissions. On the other hand, IFP is able to reduce the number of collisions, and quickly resolve them in case collisions do occur. An important observation is that under very high traffic conditions (> 1500 nodes), IFP with larger CW-max range [0,2048] results in lower per-hop delay as compared to the shorter range. This phenomenon is explained in detail later in section 3.3.

3.3 Optimal Parameter Choice

In this section, we determine the optimal choice of parameters to maximize the efficiency of IFP. Substituting the variables in equation (3.8) results in the following expression for average per-hop rebroadcast latency (T_{HOP}):

$$T_{HOP} = \frac{\sum_{i=0}^{\lambda} CW_{max,i}}{2\ \lambda^2}\,(T_I + T_C) + T_S + \frac{T_o}{e^{\lambda}} \tag{3.14}$$

where,

$$CW_{max,i} = k\frac{D_{max}}{D_i}\,CW_{base}\Big(\frac{SNR_i - SNR_{thresh}}{\alpha dB}\Big)$$

Table 3.1: D_i vs. SNR_i (Glimpse from the data-set)

D_i **(meters)**	SNR_i **(dB)**
10	35.95
50	23.25
100	17.48
150	15.48
200	14.20
250	13.06
300	11.00

As can be noted from equation (3.14), the average per-hop delay (T_{HOP}) is mainly dependent upon two varying parameters, the CW_{max} and λ (the total number of nodes within the transmission range of the sender that are contending to rebroadcast the message). Therefore, it is necessary to study the values of these parameters to minimize the T_{HOP}. First, we observe that CW_{max} can be optimized using k, α, and CW_{base}. To investigate the behavior of CW_{max}, repeated simulations (almost 100 runs) using the Nakagami propagation loss model were conducted to see how the SNR_i (SNR values at the receivers) varies as the D_i (distance from the sender) increases, while keeping the transmission power constant. Table 3.1 offers a glimpse from the data-set of the relationship between SNR_i and D_i.

Next, by using these (D_i,SNR_i) pairs, along with varying k, α, and CW_{base}, numerical analysis was carried out to determine the minimum values for T_{HOP} under different traffic scenarios. Figure 3.11 portrays a particular scenario in which the average per-hop delay (T_{HOP}) varies as a result of different combinations of k and α, while CW_{base} = 2 and λ = 6. Under such sparse traffic conditions, T_{HOP} decreases to less than 1 ms by choosing values of α >15 and k <20.

However, it is to be noted here that there is no unique range for k, α, and CW_{base} that would result in a minimum T_{HOP} under all traffic conditions and scenarios. For example, in dense traffic conditions, smaller values of k and CW_{base} would result in more collisions as the CW_{max} range becomes significantly smaller, thus causing more delays due to message

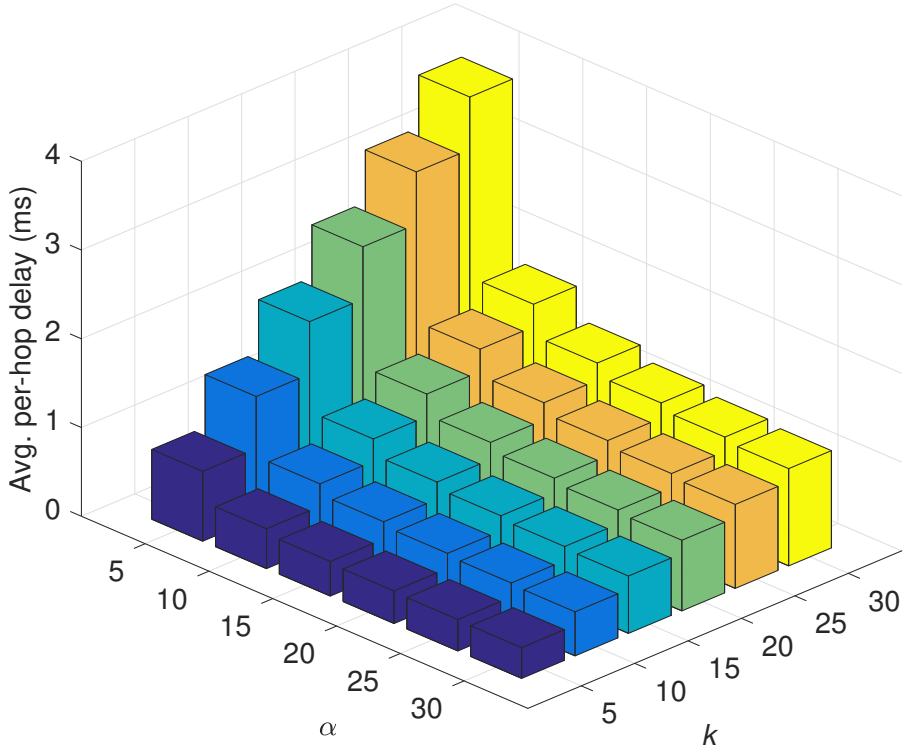


Figure 3.11: Effect of control parameters on per-hop delay.

re-transmissions. On the other hand, very high values of k and CW_{base} would result in longer average waiting times before a rebroadcast as the CW_{max} range increases; hence, increasing the average per-hop delay. Therefore, figuring out a range of values for k, α, and CW_{base} that takes the prevailing traffic conditions into consideration would be the most appropriate measure to incur minimum delays.

As a general rule, for highly congested scenarios (such as traffic rush hours in urban areas), it is suggested to use higher values for k (above 30) and low values for α (less than 15). Under such conditions, CW_{base} size could also be increased (to 3 or higher) to minimize packet collisions. On the other hand, for light traffic conditions, choosing values of $\alpha >$15 and $k <$20 will result in minimum T_{HOP}.

Figure 3.12a presents a comparison of theoretical average per-hop delay (T_{HOP}) results

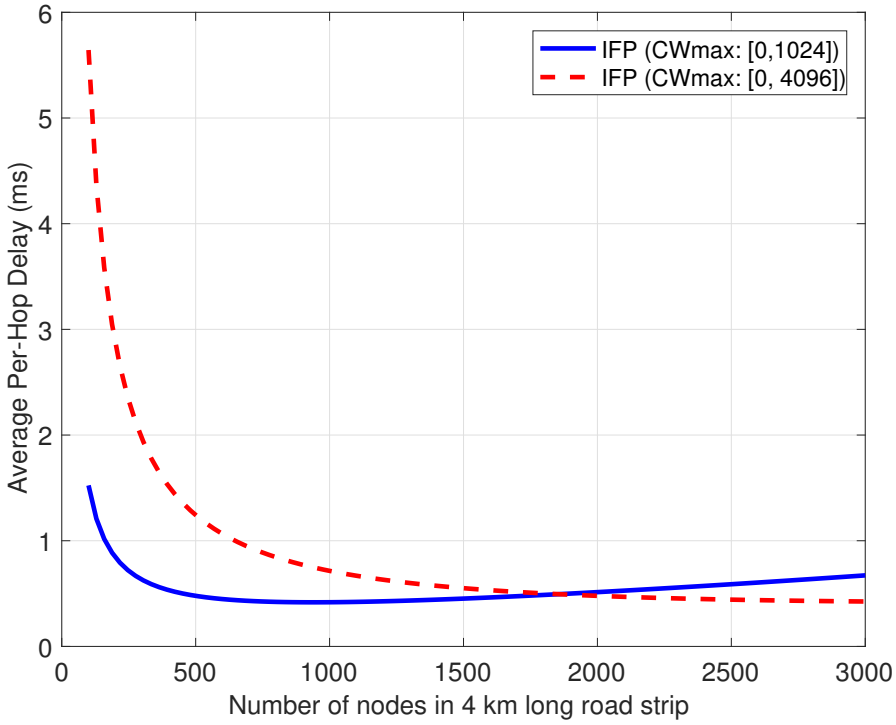
for a shorter CW_{max} range [0, 1024] versus a much longer range [0, 4096]. Figure 3.12a shows that when the CW_{max} range is increased under light traffic conditions (≈ 100 nodes in a 4 km long highway strip), there is a multifold increase in delay due to the likely occurrences of lengthy timeouts (timeout period is correlated to CW_{max}), which occur if no node is found within the transmission range (R) of the sender. Moreover, greater CW_{max} values mean forwarders have to wait much longer, on average, before rebroadcasting the message.

On the other hand, under heavy traffic conditions (> 2000 nodes), a larger CW_{max} range actually results in a better delay performance. This is due to the fact that under such dense traffic conditions, much fewer collisions will occur if a larger CW_{max} range is being used as opposed to a shorter CW_{max} range, resulting in lower delays. The sensitivity analysis of equation (3.14) shows that under lower node intensity, timeout period (T_o) dictates the T_{HOP} values; whereas under higher node intensity, the number of collisions and time to recover from those collisions determine the T_{HOP} results.

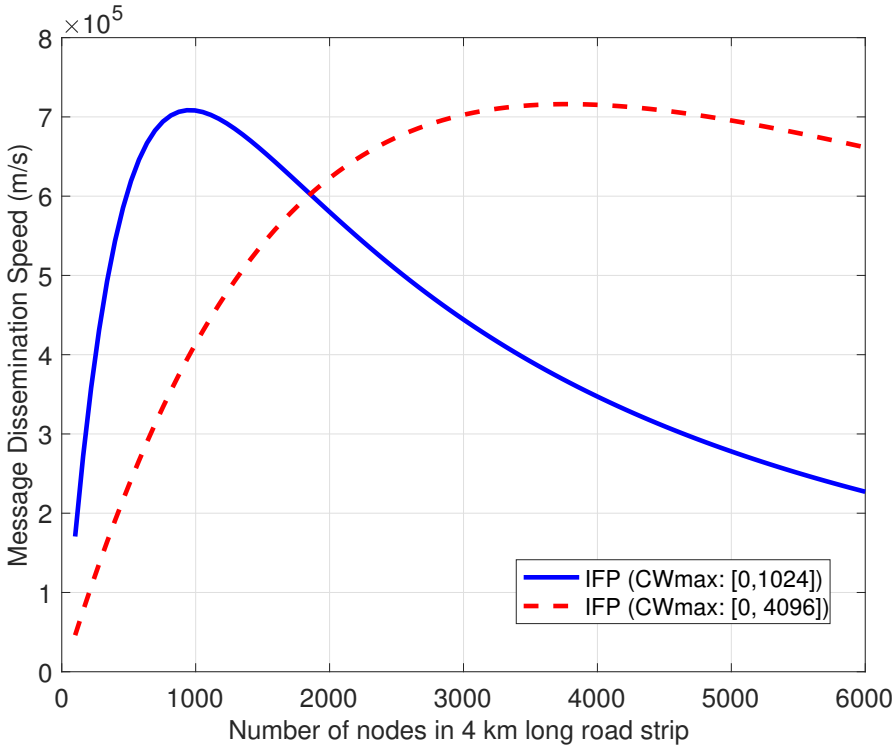
Similarly, Figure 3.12b illustrates the comparison of theoretical results of message dissemination speed between a smaller CW_{max} range [0, 1024] versus a larger range [0, 4096]. Note that for lower traffic intensity, the message propagation speed is higher with a smaller CW_{max} range as opposed to a larger CW_{max} range. This happens because, on average, smaller CW_{max} values result in shorter waiting times for forwarders before rebroadcasting the message, resulting in higher speeds. However, under higher traffic intensity (> 2000 nodes), the larger CW_{max} range actually results in higher propagation speeds as much fewer collisions occur if the larger CW_{max} range is being used. Nevertheless, an interesting observation from the figure is that as the number of nodes keeps on increasing, over the long run, the message dissemination speed ultimately drops, regardless of CW_{max} range, due to the increased occurrences of collisions. Therefore, in the light of the observations from Figure 3.12a and Figure 3.12b, under light traffic conditions (normal road scenario), the smaller CW_{max} ranges should be preferred throughout the network; whereas under

dense traffic conditions (such as during traffic congestion in multiple lane highways or during rush hours in urban areas), the larger CW_{max} range should be used, as stated earlier. In conclusion, the optimal choice of parameters leads to a significant reduction in overall message propagation delays.

This chapter presented an in-depth and thorough study of the design, mathematical analysis, optimization, and theoretical performance gain of Intelligent Forwarding Protocol. In the next chapter, we analyze the performance of IFP under simulation and real-world traffic conditions using the optimized parameters presented here.



(a) Effect of changing CW_{max} range on per-hop delay.



(b) Effect of CW_{max} on average dissemination speed.

Figure 3.12: Effect of CW_{max} range on IFP performance.

CHAPTER 4
PERFORMANCE ANALYSIS OF MULTI-HOP BROADCASTING PROTOCOLS IN SIMULATION AND REAL-WORLD EXPERIMENTAL CONDITIONS

To further evaluate and validate the performance of IFP, which was introduced in Chapter 3, we present a comprehensive comparison of the simulation results of IFP and the popular existing schemes, in this chapter. Additionally, this chapter also presents the results and analysis of the real-world experimentation and field tests that were carried out on Georgia highways (I-75). The results and analysis presented in this chapter also appeared in [13], and [14].

4.1 Simulation Analysis

4.1.1 Simulation Setup

The simulations were carried out using the latest version of ns-3. The parameters chosen in the simulation environment were practical with minimal assumptions to achieve realistic and accurate results. For IFP, we chose the optimized parameters as suggested in Chapter 3. Table 4.1 depicts the simulation parameters used and their respective values. It can be noted that the models and parameters chosen for the simulation environment accurately characterize a typical VANET environment, such as the Nakagami fading model (recommended for VANETs by [59]), two-ray ground path loss model (recommended for VANETs in [60]), and mobility model etc. The nodes are placed randomly on a 4 km long road strip. A maximum of 650 nodes can be accommodated in the simulation environment at any given time due to constraints in computational resources.

In these simulations, IFP was compared against two representative protocols belonging to the delay-based category and the stochastic category, respectively. Since the vast major-

Table 4.1: Simulation parameters

Attribute	Value
Standards	IEEE 802.11p, WAVE
Data rate	6 Mbps (OFDM)
Transmission range (R)	300 meters
Fading model	Nakagami fading model
Mobility model	Constant velocity mobility
Road dimensions	4 km long (2 lanes)
Node density (Per 4 km Strip)	150 - 650 nodes
Time slot	40 μSec
SIFS	10 μSec
SNR_{thresh}	8dB
Emergency Message Size	50 bytes
Simulation Time (per run)	100 seconds

ity of forwarding protocols fall in one of these two categories, it is appropriate to compare IFP against these techniques. In this thesis, we refer to the representative delay-based protocol as Simple Delay-Based (SDB) protocol, while the representative stochastic protocol is called Simple Probability-Based (SPB) protocol. SDB closely follows the techniques proposed by Briesemeister and Hommel [28], IVG [29] , Streetcast [30], ODAM [31], and EDB [34], and uses equation (2.1) for the forwarder selection process. On the other hand, SPB employs the techniques proposed by slotted p-persistence protocol [44]. Table 4.1 summarizes the important parameters chosen for IFP, SDB and SPB.

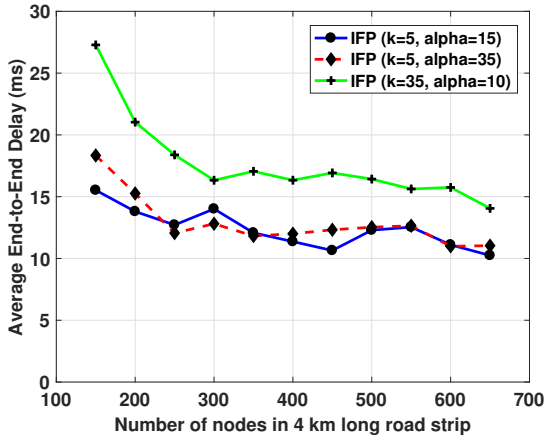
4.1.2 Results and Analysis

As described earlier, fast and reliable delivery of safety messages are the two main design considerations of any forwarding protocol in VANETs. Therefore, to present an effective and fair comparison between IFP, SDB and SPB under these considerations, we classify our simulation results into two main categories: 1) Forwarding Latency determines how quickly the safety message is forwarded in a target region. 2) Packet Delivery Ratio (PDR) measures how efficient each protocol is in ensuring guaranteed message delivery to each node in the target region.

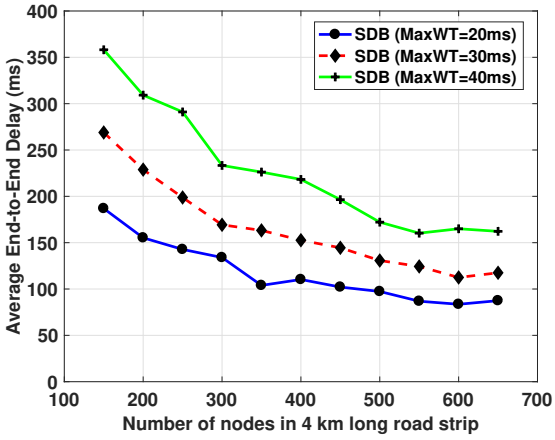
4.1.2.1 Forwarding Latency

First, we measured each protocol's end-to-end delay, which is the time taken to disseminate the safety message throughout the entire target region ($4\ km$ long road strip). Figure 4.1 shows end-to-end delay results of the three protocols as node intensity increases. For each protocol, we vary the control parameters according to recommended optimal values.

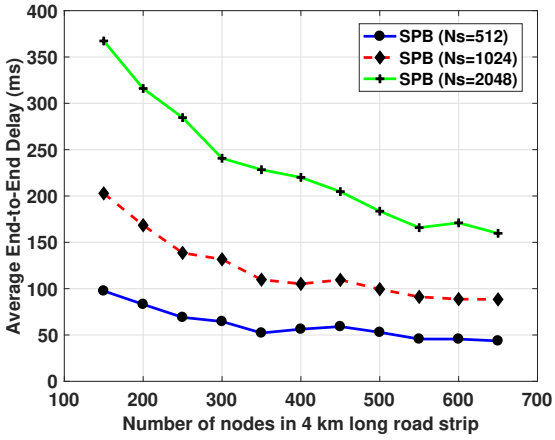
IFP can be optimized by varying CW_{base}, k, and α, as discussed in the previous chapter. However, CW_{base} should only be tuned under extreme traffic conditions ($> 1000\ nodes$ in $4\ km$ long road strip). Therefore, we observe the impact of varying only k and α on IFP delay performance in Figure 4.1a. As shown in Figure 4.1a, the end-to-end delay of IFP decreases, on average, with the increase in node intensity. Under dense traffic conditions, there is a higher probability of having nodes near the boundary of transmission region (with lower CW_{max}), which results in lower average waiting time before each successful rebroadcast, hence, reducing the overall end-to-end delays. Another observation from Figure 4.1a is that under regular traffic conditions, lower k values results in better delay performance. This phenomenon was explained in detail in Chapter 3. On the other hand, SDB is mainly controlled by $MaxWT$, a parameter of equation (2.1). While a smaller $MaxWT$ leads to a lower waiting time being assigned to each node before rebroadcast, it results in a higher collision probability caused by the short difference in the waiting times of neighboring nodes. We choose the values of $MaxWT$ as suggested by the protocols using the SDB approach. Figure 4.1b depicts that the end-to-end delays are reduced at lower $MaxWT$, since nodes have to wait for shorter time before a successful rebroadcast. However, for $MaxWT < 20ms$, the delay starts rising due to a significant increase in collision probability, which result in unnecessary re-transmissions. As the safety message doesn't cover the entire 4 km road strip for $MaxWT < 20ms$ scenarios, we don't consider them in these simulations. Lastly, Figure 4.1c depicts the end-to-end delay of SPB. The main parameter controlling the performance of SPB is the predetermined number of slots (N_s). Since [44] doesn't specify any exact method of calculating N_s, we measured the performance of



(a) IFP



(b) SDB



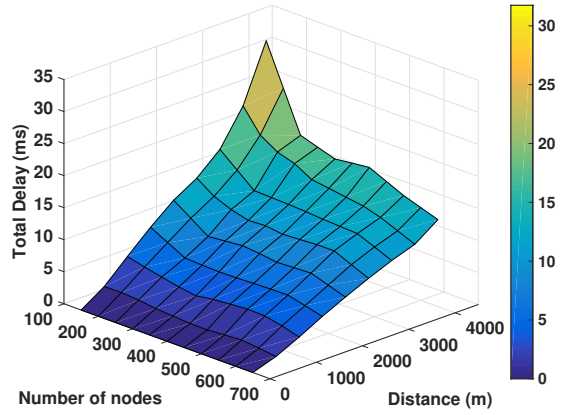
(c) SPB

Figure 4.1: Comparison of end-to-end delay.

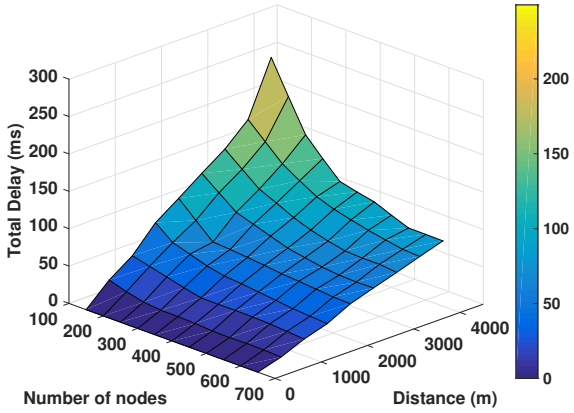
SPB under various N_s. Figure 4.1c shows that a lower N_s results in lower end-to-end delay as each forwarder has to wait for lesser time (number of slots), before rebroadcasting. However, for $N_s < 512$, the packet collisions significantly increases as the probability of multiple nodes choosing the same time slot to rebroadcast a message also increases. In this scenario, a safety message fails to travel the entire target region, and hence, the end-to-end delay cannot be determined.

In Figure 4.1, IFP significantly outperforms both SDB and SPB regardless of the optimal parameter setting. This improvement in the end-to-end delay performance of IFP is a result of: 1) efficient forwarder selection mechanism, 2) shorter waiting times before forwarding, 3) improved collision resolution mechanism, and 4) greater one-hop message progress (average distance covered during each hop). Another observation from Figure 4.1 is that the end-to-end delay of all protocols decreases as the node intensity increases. This happens as each protocol assigns shorter average waiting time to the forwarder candidates that are closer to the boundary of sender's transmission range (which is more probable under higher node intensities). However, at high traffic congestion rates ($> 350\ nodes$), the delays stop reducing further due to the high occurrence of packet collisions, which lead to unnecessary transmissions.

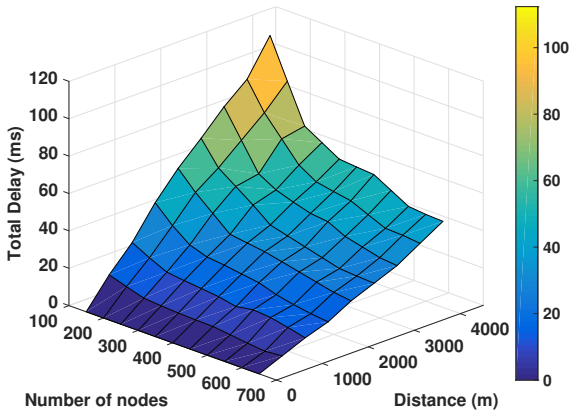
On the other hand, Figure 4.2 shows the delay incurred in propagating a safety message across a certain distance (from the initial sender) using multi-hop communication. For all protocols, the optimal values for control parameters have been selected. The delay results under various node intensities have been recorded for an effective comparison. As seen in Figure 4.2, all protocols depict a similar overall delay trend as the number of nodes vary. For each protocol, the total delay for a message to travel a certain distance is inversely proportional to node intensity. Under dense traffic conditions, there is a higher probability of having a node closer to the boundary of sender's transmission range, resulting in lower waiting times before forwarding as well as greater one-hop message progress; hence, leading to reduced overall delay in propagating the message. Again, IFP exhibits a clear



(a) IFP

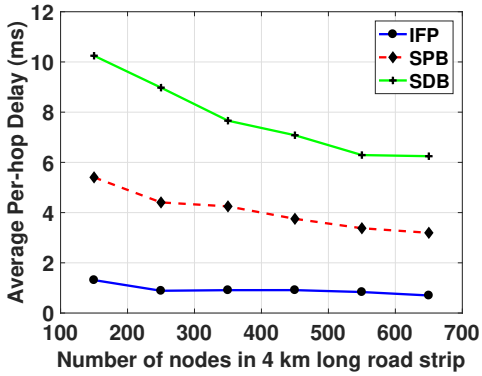


(b) SDB

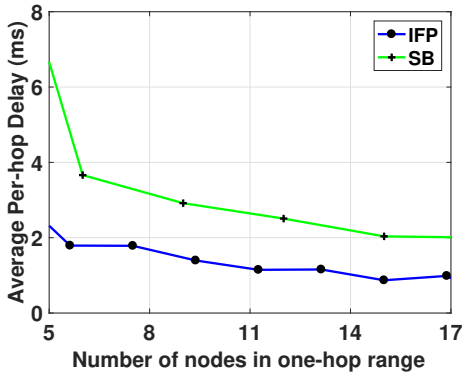


(c) SPB

Figure 4.2: Delay results comparison across a certain distance.



(a) Comparison with SDB and SPB



(b) Comparison with SB (handshaking-based protocol)

Figure 4.3: Comparison of average per-hop rebroadcast latency.

superiority over SDB and SPB in terms of delay performance.

Lastly, Figure 4.3 presents a comparison in terms of per-hop rebroadcast latency (average time spent to rebroadcast a safety message across a single hop). As shown in Figure 4.3a, IFP achieves a significant per-hop delay reduction of almost 88.0% as compared to SDB and 77.2% as compared to SPB. This delay improvement in IFP is quite expected and can be contributed to the following design improvements. First, IFP uses a highly efficient mechanism to select the most optimal forwarder candidate to rebroadcast the safety message. Second, IFP ensures that the shortest possible waiting time is assigned before rebroadcasting at each hop. Furthermore, IFP proposes a novel ACK-decoupling mechanism and an improved collision resolution mechanism. Lastly, IFP generally achieves a greater one-hop message progress (average distance covered during each hop).

Additionally, to compare the delay performance of IFP with handshaking-based protocols, we implemented a well-known multi-hop broadcasting protocol, Smart Broadcast (SB), which was previously discussed in Chapter 2 and Chapter 3. Figure 4.3b shows the per-hop delay comparison between IFP and SB as the number of nodes within a single hop range vary. IFP performs almost 200% better than SB in terms of per-hop delay due to superior design considerations, some of which are listed here. First of all, while SB is highly dependent upon the exchange of handshaking messages (RTB/CTB) before for-

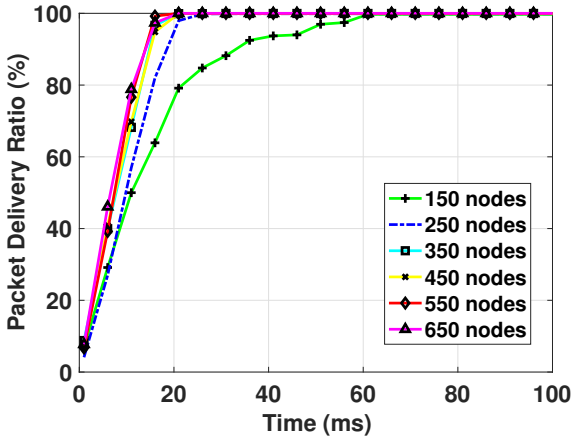
warding messages, the proposed protocol broadcasts messages without prior handshaking mechanisms. Secondly, SB requires the forwarders to send ACKs for collision resolution and ensuring reliability, whereas in IFP, forwarders exploit the combination of SNR and GPS coordinates to either eliminate ACKing procedure or atleast decouple it from the message propagation process, without compromising on the overall reliability.

4.1.2.2 Packet Delivery Ratio

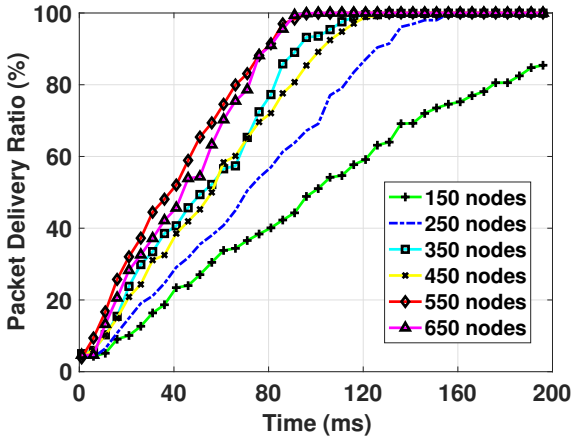
Next, to determine the message reliability (guaranteed message delivery to each node in the target region), we measured each protocol's Packet Delivery Ratio (PDR), which is the ratio of number of vehicles that receive the safety message to the total number of expected receivers. Since reliability is an important criterion for safety message dissemination, it is worthwhile to study the PDR achieved by each protocol.

Due to the time-critical requirement of safety systems in VANETs, delayed information is not very useful. Typically, the reaction time of safety systems should be in the order of milliseconds to have a meaningful impact [61]. Therefore, in Figure 4.4, we analyze how the PDR results (in $\%$) vary in the target region ($4\ km$ long road strip), starting from the time when the safety message is first generated by the original sender. For a fair comparison, in the simulation environment, we place the original sender (message initiator) at the beginning of the road strip to ensure that the message travels the entire length of the target region.

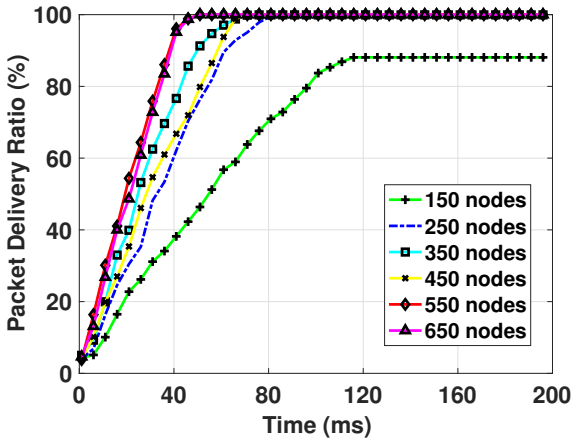
As shown in Figure 4.4, IFP substantially outperforms both SDB and SPB in terms of PDR acheived within a certain time. On average, while IFP is able to achieve a PDR of over 99$\%$ under all node intensities within a 50 ms period (a single control channel interval (CCH)), SDB and SPB are only able to achieve 99$\%$ PDR under a few node intensities, and even in those scenarios, they require almost 120 ms and 75 ms respectively. IFP achieves this significant gain over SDB and SPB in terms of reliability (higher PDR per unit time) due to the following reasons. While SDB and SPB utilize distance and probability based



(a) IFP



(b) SDB



(c) SPB

Figure 4.4: Comparison of Packet Delivery Ratio (PDR) results.

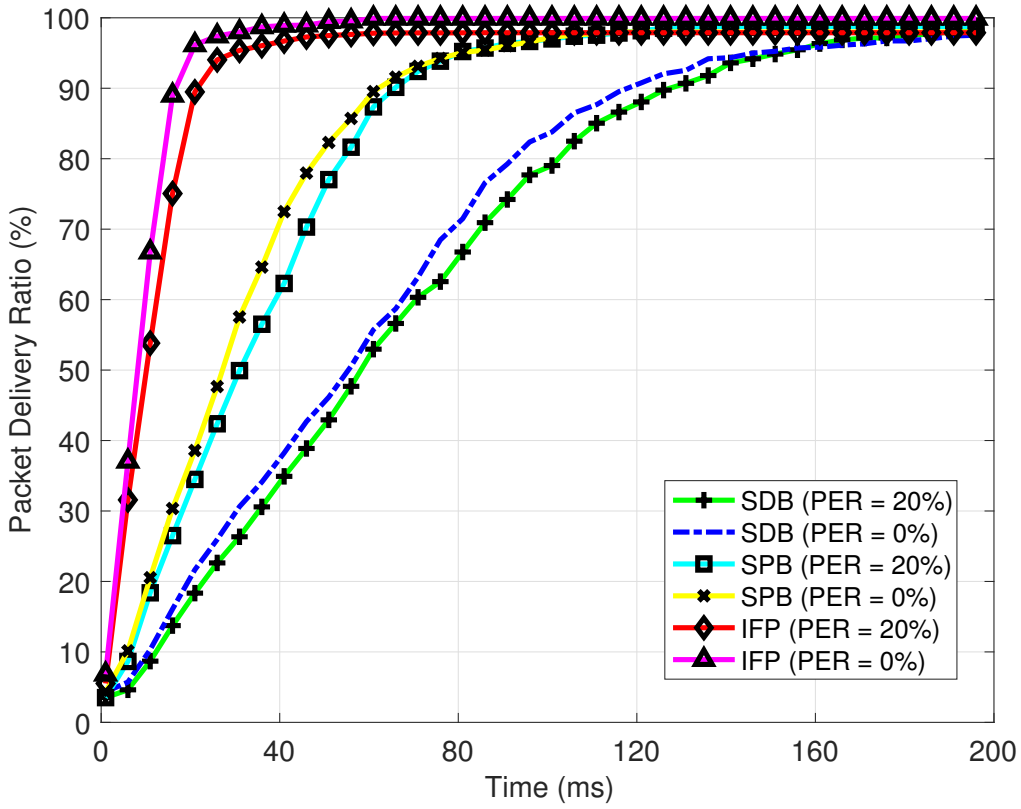


Figure 4.5: Effect of introducing PER on PDR results.

metrics respectively to determine the forwarding nodes, IFP exploits an SNR, GPS, and contention window based forwarder selection mechanism to determine the most optimal forwarder such that the guaranteed message delivery to each node in the target region could be ensured, and message collisions could be reduced. Once a collision does occur, IFP is able to quickly recover from it using the novel collision resolution technique described earlier. Note that in case of packet collisions, SDB and SPB must repeat the entire forwarding process again, causing significant delays.

An observation from Figure 4.4 is that under higher node intensities, the protocols are able to quickly disseminate safety messages to more nodes in the target region due to absence of coverage holes and greater one-hop message progress (average distance covered during each hop). As shown in Figure 4.5, introducing a packet error rate (PER) of 20%

Table 4.2: Time required (in ms) to reach a certain PDR (%)

Nv	**IFP** ($PDR_{>50\%}$)						**SDB** ($PDR_{>50\%}$)						**SPB** ($PDR_{>50\%}$)					
	50%	**60%**	**70%**	**80%**	**90%**	**99%**	**50%**	**60%**	**70%**	**80%**	**90%**	**99%**	**50%**	**60%**	**70%**	**80%**	**90%**	**99%**
150	10.99	14.59	17.99	21.75	33.10	59.01	98.60	122.06	142.37	175	>200	N/A	54.72	67.07	79.56	96.56	N/A	N/A
250	9.83	11.60	13.59	15.59	18.50	23.50	70.56	84.48	101.55	112.05	125.39	153.50	32.72	39.77	45.79	54.32	61.70	79.01
350	7.77	9.54	11.31	13.06	14.82	19.50	52.09	67.64	74.27	82.59	92.15	116.00	24.79	29.64	36.25	42.86	49.85	67.01
450	7.56	9.30	11.03	13.03	15.03	20.01	55.99	65.62	76.79	89.85	102.27	121.00	28.27	35.20	44.11	51.12	58.40	67.01
550	7.43	8.77	10.10	11.74	13.95	15.99	38.40	46.83	56.60	66.09	78.77	110.99	19.35	23.81	28.44	33.01	37.96	47.49
650	6.59	8.12	9.64	11.31	14.01	18.99	43.63	54.16	60.80	71.72	79.23	93.49	21.54	25.64	29.82	34.35	38.79	47.49

$Without\ PER$	**IFP** ($PDR_{>50\%}$)						**SDB** ($PDR_{>50\%}$)						**SPB** ($PDR_{>50\%}$)					
	50%	**60%**	**70%**	**80%**	**90%**	**99%**	**50%**	**60%**	**70%**	**80%**	**90%**	**99%**	**50%**	**60%**	**70%**	**80%**	**90%**	**99%**
Avg	8.17	9.86	11.72	13.97	16.69	46.41	55.36	67.43	78.52	92.19	117.90	N/A	27.17	32.73	39.41	48.33	62.15	N/A

$PER_{=20\%}$	**IFP** ($PDR_{>50\%}$)						**SDB** ($PDR_{>50\%}$)						**SPB** ($PDR_{>50\%}$)					
	50%	**60%**	**70%**	**80%**	**90%**	**99%**	**50%**	**60%**	**70%**	**80%**	**90%**	**99%**	**50%**	**60%**	**70%**	**80%**	**90%**	**99%**
Avg	10.13	12.45	14.80	17.70	21.56	N/A	58.18	70.55	84.88	102.39	127.36	N/A	31.05	39.01	45.80	54.22	65.75	N/A

adversely affects the average PDR levels per unit time. This behavior is explained later in this section.

Similarly, Table 4.2 depicts the time comparison between each protocol to reach a certain PDR (%). The number of vehicles in the target region is denoted by N_v, while packet error rate is represented as PER. N/A refers to the instance when a protocol is not able to reach a certain PDR level. Table 4.2 shows that SDB and SPB either do not reach a PDR of 99% under sparse network conditions (150 nodes) due to the presence of coverage holes, or require a significantly large amount of time to reach a PDR $> 90\%$ under all other network conditions (as compared to IFP) due to their slower and less reliable message dissemination process, as discussed earlier. IFP, on the other hand, is able to recover from coverage holes due to continuous re-transmissions (after each predefined timeout period) until a new forwarder is finally selected when it enters in the previous forwarder's range. Additionally, Table 4.2 shows that introducing a packet error rate (PER) of 20% lowers the average PDR of each protocol while increasing the time required to reach a certain PDR due to extra packet losses and time required to recover from them.

Next, we analyze the performance of IFP under real-world traffic conditions.

4.2 Experimentation

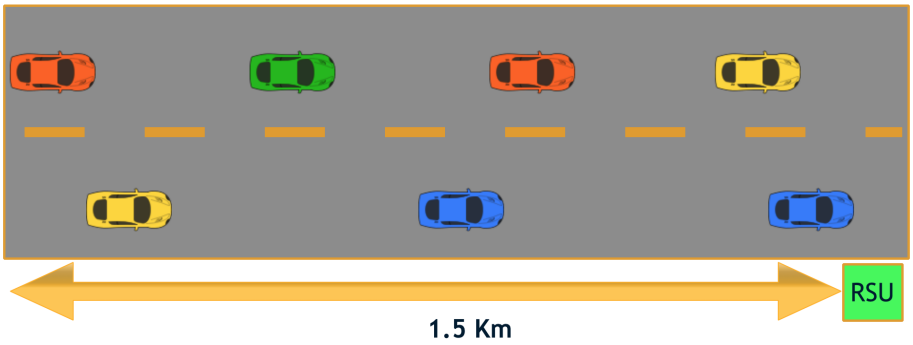
In this section, we present the experimental results of IFP to validate its effectiveness under real-world VANET conditions.

4.2.1 Experimental Setup

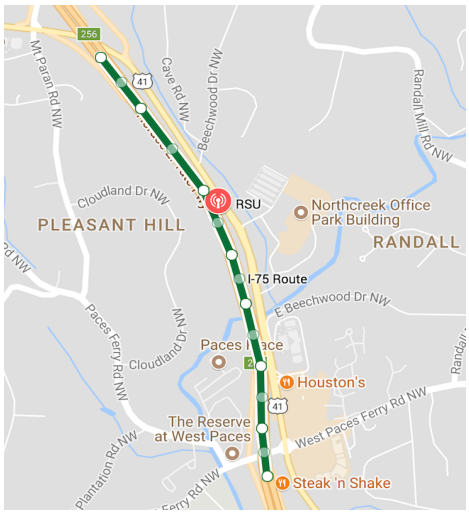
To test the multi-hop performance of IFP, we implemented a test-bed consisting of eight cars and two road-side units (RSUs) near the Georgia Institute of Technology campus. To enable vehicle-to-vehicle (V2V) communication, all cars were equipped with Arada Systems on-board units (OBUs), which operate at the 5.9 GHz frequency band and use IEEE 802.11p and WAVE standards. The protocol implementation was done with the aid

of Arada Systems built-in Locomate library. As shown in Figure 4.6a, the cars were driven past the RSU in the form of a convoy; the last car in the convoy periodically broadcasts a safety message, which then propagates in a multi-hop manner until it reaches the RSU. The distance between the cars is controlled in order to closely study the forwarder selection mechanism of IFP. Figure 4.6b depicts the route selected for the field trials. OBUs and RSUs are shown in Figure 4.6c.We evaluated the protocol under the highway scenario. All cars traveled in the same direction (the average velocity was 100 km/h; road length was 3 km, and a data-rate of 6 Mbps). For each result,we used the average value of ten measurements (ten runs). We evaluate IFP with regard to the following metrics: forwarder selection mechanism, message propagation delay, network throughput, and packet delivery ratio.

To validate the experimentation results of IFP, we compared them with the simulation results. The metrics chosen for both the experimental and simulation environments are similar to minimize any inconsistencies and to achieve a fair comparison. It was not feasible and practical to compare the experimental results of IFP with other multi-hop broadcasting protocols due to numerous reasons. First, the experimental environment presents a number of uncontrollable variables, each of which affects the protocol performance, such as vehicle mobility, spatial location, interference due to terrain and neighboring objects, (*name a few others*) and so on. Therefore, it is not possible to mimic the same conditions under which the different protocols can be tested for a fair comparison. Second, each protocol proposed in the literature is optimized to perform adequately under specific scenarios only; hence it would be unfair and inconclusive to compare the different protocols under our experimental scenario only. Finally, most of the existing protocols in literature lack particular implementation details and specific protocol parameters, which hinder us in qualitatively comparing IFP against other protocols under real-world conditions.



(a) Experimental Topology



(b) Route for Field Trials

(c) Equipment (OBU/RSU)

Figure 4.6: Experimental Environment.

4.2.2 Context

Simulation environments are often considered as not being highly precise as they are idealistic and limited in approach. For example, many models used in simulation such as the signal propagation models, vehicle mobility model, and so on, are a mathematical approximation of the real world conditions. On the other hand, through real-world experimentation, the exact environmental behaviors such as terrain interferance, path loss, mobility pattern, etc. can be captured, resulting in highly realistic and accurate results. However, carrying out the real-world implementation and field trials presents its own challenges. Firstly, since the Arada Systems libraries did not allow for the SINR values to be extracted at the MAC

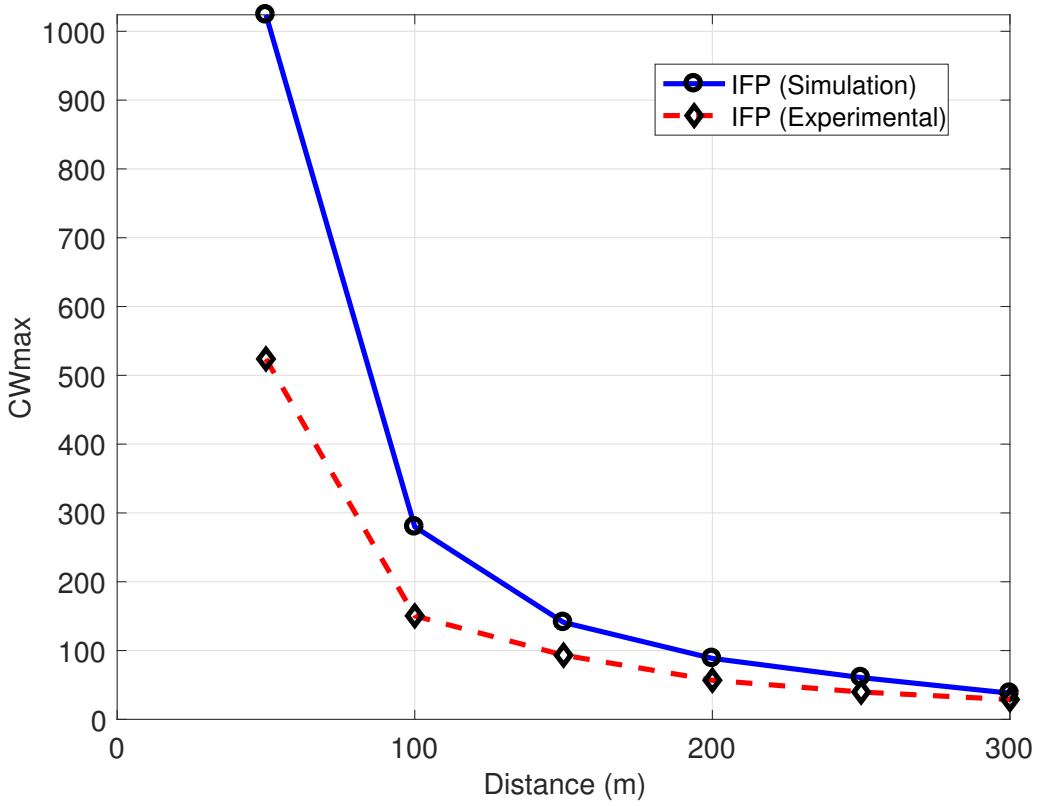


Figure 4.7: Forwarder selection mechanism - Experimental vs. simulation results.

layer of the V2V nodes, we had to extract them at the Application layer in order to make the forwarding decision. This introduced an extra delay at each node. Another complexity associated with the real-world experimentation was that it was extremely tedious to keep a consistent vehicle topology / formation and exactly the same experimental conditions for each different trial, given the dense traffic conditions in the Georgia highways. However, we tried to keep the control parameters and experimental conditions consistent to the best of our ability.

4.2.3 Results and Analysis

First, we evaluated the performance of IFP with respect to the forwarder selection mechanism, which primarily depends upon CW_{max}, as described in Chapter 3. Figure 4.7 shows

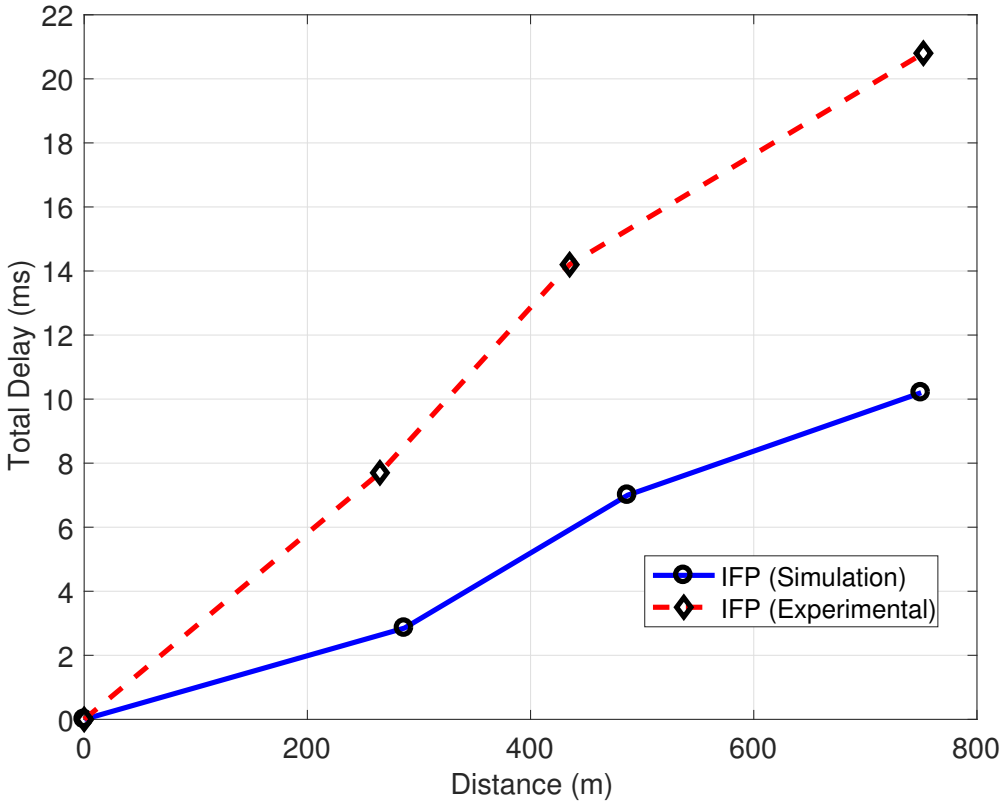


Figure 4.8: Delay comparison across 3 hops.

how CW_{max} size varies as the distance between the sender and a forwarding candidate D_i varies. In order to increase the chances of further nodes to be selected as forwarders (to increase one-hop message progress), there is an exponential drop in CW_{max} values as the distance increases in both experimental and simulation results. While a lower CW_{max} range can result in collisions in a dense network, that is not a problem here as only a couple of nodes exist within a node's transmission range at any particular instance.

As shown in the figure, experimental CW_{max} values are slightly lower in comparison, as the SNR_i values achieved in real-world experimentation for a particular D_i are notably lower than those in simulations. This drop in SNR_i values can be attributed to terrain and object interference, inaccuracies in signal fading model (in simulation environment), and so on. Nevertheless, both the experimental and simulation results in Figure 4.7 have a very

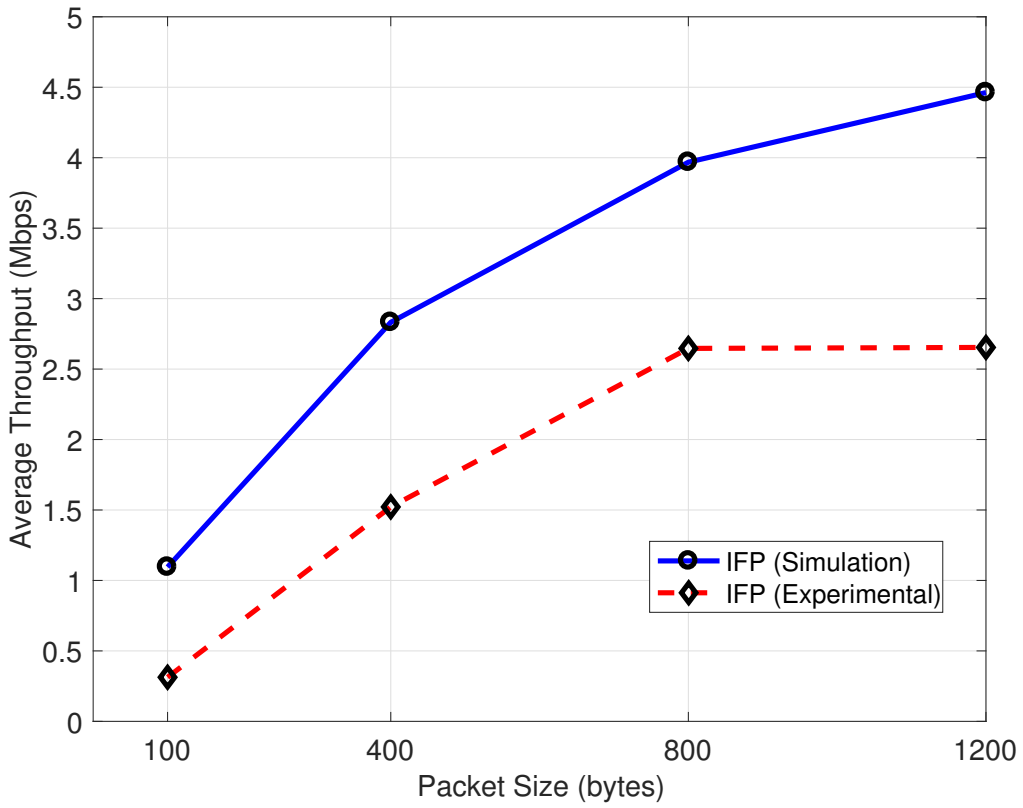


Figure 4.9: Avg. throughput comparison - Experimental vs. simulations results.

similar trend and are conforming.

Next, we measured the message propagation delay across 3 hops (starting from the time when a message is initially broadcast), as shown in Figure 4.8. We chose a maximum of 3 hops only, since that was the maximum number of hops achievable with our limited experimental resources. As expected, both experimental and simulation scenarios depict a steady rise in delay across each hop. Although both set of results have a similar trend, the experimental scenario portrays significantly higher delay values. First, as some design components of lFP are implemented in the Application layer, the message has to traverse additional layers at each hop, resulting in higher delays. Additionally, the different models used in the simulation environment have their own limitations, and thus some delay components might not be accounted for in simulations. Similarly, Figure 4.9 illustrates the

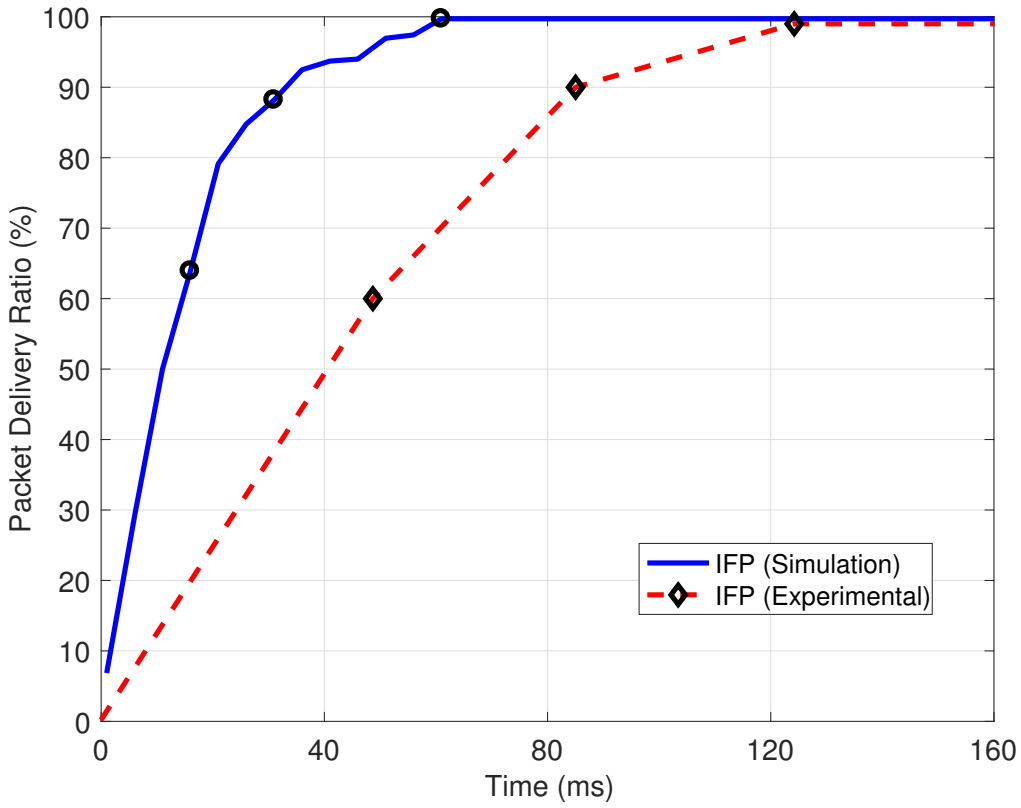


Figure 4.10: PDR comparison - Experimental vs. simulations results.

average throughput achieved in the two scenarios. Both scenarios portray an increasing trend of the throughout values as the size of the safety message increases. With an increase in packet size, more data can be shared in a single transmission, resulting in higher throughput. However, it can be noted that the average throughput of the experimental scenario stops increasing after 2.8 Mbps, since the channel reaches its saturation, resulting in increased packet drops and collisions.

Finally, Figure 4.10 shows the PDR results, which determine the reliability of the protocol. At any particular instance, the experimental results depict a lower PDR as compared to simulation results due to higher occurrences of collisions, packet drops, and un-necessary retransmissions in the real-world conditions. Additionally, since the message propagation delay in experimental scenario is higher, the message progresses slowly through the

VANET, resulting in a lower PDR at any instance. However, in both scenarios, a PDR of almost 100% is ultimately achieved, which ensures the guaranteed delivery of safety messages to every node in the target region.

In this chapter, extensive simulation results of IFP were presented, which establish the superiority of IFP over existing techniques. This chapter also discussed the real-world experimentation and field-trials that were conducted using the IEEE 802.11 p devices to evaluate the performance of IFP under real traffic conditions. The results validate the performance gain achieved by IFP in such conditions.

CHAPTER 5

COOPERATIVE BSM-BASED MESSAGE DISSEMINATION

As discussed earlier, one of the key requirements for human-driven and autonomous vehicles is to have continuous awareness of their surroundings at all times, to detect any potential threats (vehicles, pedestrians, wild-life etc.). This requires continuous cooperation between vehicles by efficiently sharing safety information in a timely manner. However, this is a multi-dimensional and challenging problem due to the unique characteristics and challenges of VANETs. This chapter presents an elegant solution to efficiently share safety information among vehicles by leveraging the Basic Safety Messages (BSM), which are part of the existing V2V standards. Through this approach, vehicles are able to quickly and preemptively identify potential threats, not just in their close proximity, but also those that are further along the roadway by intelligently exchanging safety information between neighboring vehicles. Additionally, the proposed architecture presents a practical approach of incorporating the on-board sensor data with the V2V communications. This results in vehicles having improved visibility and situational awareness even outside of their one-hop range.

First, this chapter provides an overview of the motivation and contribution of the proposed architecture. Next, we present a discussion on the architecture design, and its potential applications. Finally, the performance evaluation and results of the proposed architecture are discussed toward the end of this chapter. The research work presented in this chapter also appeared in [15], and [16].

5.1 Motivation and Contribution

The Dedicated Short-Range Communications (DSRC) standards [5], developed for V2V communication, mandate the periodic broadcast of a Basic Safety Message (BSM) con-

taining each vehicle's position, speed, direction and so on, as explained in Chapter 1. This ensures that each vehicle participating in the V2V communication is aware of its immediate neighbors, so that collisions could be avoided. However, a limitation of just relying on this standard BSM approach to share safety information is that vehicles have a very restricted visibility and awareness of potential threats (limited to one-hop range). Similarly, existing single-hop safety message dissemination techniques are also incapacitated of enabling communication beyond the single-hop transmission range efficiently, as discussed in Chapter 2. While multi-hop broadcasting schemes are ideal for fast and reliable message delivery of small and dedicated safety packets to further regions, they are not efficient in enabling continuous exchange of safety information between vehicles, as multi-hop techniques often incur a high network overhead and increased packet collisions due to flooding the network.

This research proposes an architecture which successfully addresses the above mentioned limitations. The contribution of this research work is to propose a novel architecture that facilitates the effective sharing of safety information in VANETs by intelligently exchanging and storing the data obtained from the neighboring vehicles as well as from the on-board sensor technologies. Since BSMs are mandated by the vehicular standards, and are broadcast very frequently throughout the network, this research leverages the BSM-sharing infrastructure to develop an innovative solution for spreading safety information across the entire VANET with low latency. Additionally, in contrast to many existing safety information delivery protocols that require modifications to the DSRC standards for successful operation, the proposed architecture enables information sharing among vehicles by just exploiting the existing DSRC standards for V2V communication without altering any layer or requiring any modification to the standards. Finally, we also introduce a standard threat format through which any raw sensory data could be represented. Table 5.1 presents a qualitative comparison between the proposed architecture and the existing approaches of safety information dissemination in VANETs.

Table 5.1: Safety information dissemination techniques in VANETs

Category	Characteristics	Benefits	Drawbacks
Single-hop Broadcasting	- Safety messages directed toward immediate neighbors.	- Trivial safety message dissemination scheme for short range (one-hop) communication.	- Message propagation process limited in terms of range to 300 m in a single broadcast cycle.
	- Messages disseminated using periodic broadcasts.	- No broadcast storm problem (i.e. No flooding).	- Packet dissemination to nodes further out either not possible or very slow.
	- Relies on node mobility to store and forward safety information.	- Good for applications requiring large packets to be shared	- Needs an algorithm to route packets beyond one hop range.
			- Existing schemes do not consider on-board sensor data.
Multi-hop Broadcasting	- Safety messages are disseminated by smart flooding.	- Safety information is disseminated quickly to vehicles further away (via multiple hops)	- Needs a complex algorithm to mitigate broadcast storm problem
	- Relies on intelligent forwarder selection algorithm.	- Suitable for applications transmitting safety alerts and emergency warnings.	- Network flooding and collisions.
		- No need to store safety information.	- Difficult real-world implementation.
			- Existing schemes do not consider on-board sensor data.
Proposed BSM Architecture	- Safety information is shared using DSRC-mandated BSM packets.	- Trivial and fast safety information delivery process to all vehicles up to several km away.	- Requires data storage to store information related to potential threats. (However, data storage is presently quite inexpensive).
	- Effectively shares on-board sensor information as well as V2V related data.	- Incorporates and shares on-board sensor data as well.	- BSM frequency and size has to be optimized.
		- Exploits only existing V2V standards.	
		- Complex routing algorithms not needed.	
		- Resistant to broadcast storm and network flooding.	
		- Tremendously improves vehicle's awareness of their environment.	
		- Practical for real-world implementation.	

5.2 Architecture Design

Building on the motivation described above and the discussion regarding BSM-sharing infrastructure in Chapter 1, we now present the architecture design. The proposed architecture enhances the collective awareness of vehicles by efficiently sharing the safety-related data obtained through both on-board sensors and neighboring vehicles. The architecture consists of the following main components:

- Data Collection and Storage
- Sharing Threat Matrix
- Updating Neighboring Threats Table

The remainder of this section describes each of these components in detail.

5.2.1 Data Collection and Storage

This initial phase of the architecture deals with the efficient collection and storage of safety-related data by the participating vehicles. The V2V-enabled vehicles have two main sources of acquiring knowledge about their surroundings: 1) by receiving the safety messages (e.g. BSMs) from their neighboring nodes, 2) by obtaining the sensing data from the in-vehicle CAN bus or other on-board sensors.

First, as the DSRC standards mandate the periodic broadcast of BSMs containing each vehicle's position, speed, direction etc., this useful information can be utilized by the neighboring vehicles to enhance their understanding of the environment. Secondly, the vehicles with on-board sensors have an added advantage in the sense that they can detect a threat (a potentially hazardous vehicle, pedestrian, or object, which can cause an accident) with very high accuracy. Since each of these sensors produce the raw sensory data in their own respective formats with varying rates (as depicted in Table 5.2), it is important to convert the raw sensory data obtained from different sensors into a standard threat format. The threats

Table 5.2: Active sensor characteristics

Sensor	Output Format	Data Size	Sample Rate
LIDAR	Binary to ASCII(X,Y,Z)	400Bps - 90Mbps	5Hz-180+KHz
Automotive Radar	Echoed Frequency Responses (Pulse & Continuous)	64+Kbps	500KHz-10MHz
Sonar	Sound Wave Responses to ADC Voltage or PWM	0.12Kbps	1Hz-100+KHz
IR	ADC Voltage	1-2 Mb per Sample	1-20Hz
Radio Frequency (RF)	Signal Response Modulation	16+ bits per Sample	4Hz
Magnetic Restive	Voltage Variation	12 Bits per Sample	100Hz
Camera	Continuous Image Frames	1-400Mbps	30-60fps

can then be efficiently stored locally as well as shared with other neighboring vehicles. The threat format is described later in this section.

An important reason for representing the raw sensor data into threats is that storing raw data being continuously generated from different sensing devices could be quite memory consuming. This is true for many sensing technologies such as high-quality cameras, IR, automotive radar, and LIDAR, which provide a continuous stream of data. As observed in Table 5.2, LIDAR alone generates up to 90 megabits per second and therefore, the storage capacity required to hold such huge quantities of data, let alone to share, is impractical and costly.

Once the different threats in the vicinity of a particular vehicle have been identified, they are stored in the vehicle's local database. This local database is referred to as Neighboring Threats Table (NTT). Hence, NTT consists of the threats observed either through the BSM packet reception from the neighboring vehicles or through on-board sensors. A threat is

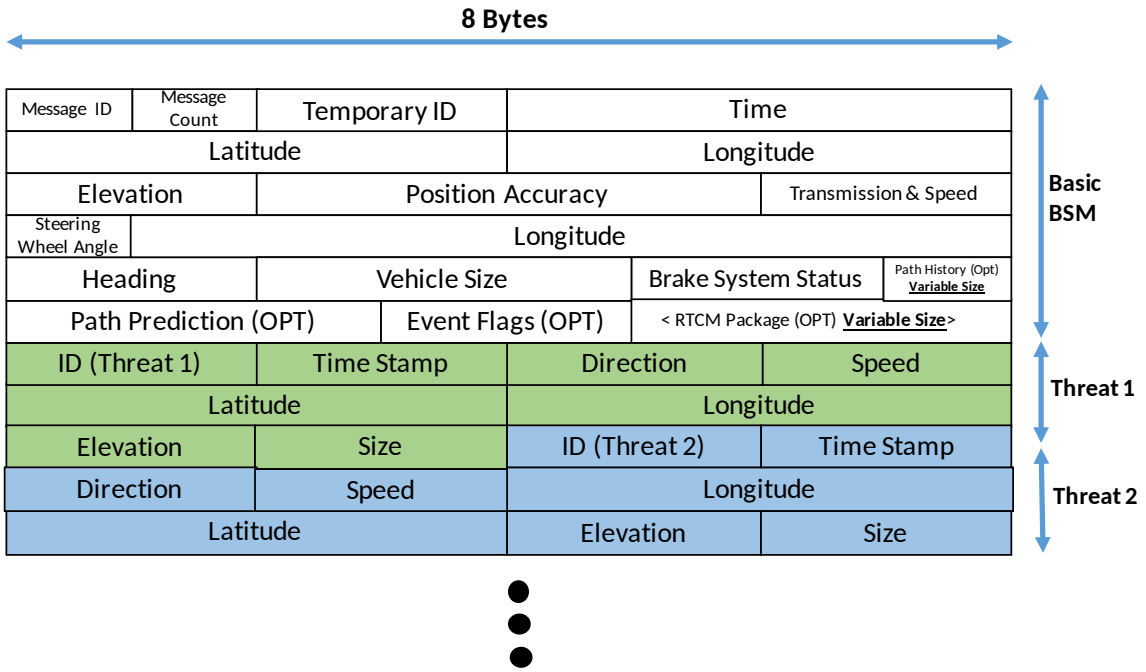


Figure 5.1: A BSM packet incorporating threats.

stored as a single record in the NTT.

According to the proposed standard threat format, each threat is 20 bytes long and has the following format: threat ID (2 bytes), 10 bytes of the position (longitude, latitude, elevation), speed (2 bytes), direction (2 bytes), size (2 bytes), time-stamp (2 bytes). Figure 5.1 depicts such threats being encapsulated in a BSM packet.

Algorithm 1 shows how the raw data from sensors is converted into threats, which are then stored in NTT. Note that the size of NTT grows at a rate proportional to the traffic congestion and the presence of other potential threats such as pedestrians, bicyclists, and so on. Threats appear in the NTT in the decreasing order of relevance i.e. most relevant/dangerous threats appear at the top of NTT. The relevance of a particular threat can be calculated by a number of different parameters such as its Euclidean distance from the detecting vehicle, time-stamp, its speed and direction, and so on. Note that each vehicle maintains its own NTT, which might be different as compared to its neighboring vehicle's NTT.

Algorithm 1 Incorporating sensor data in BSM architecture

Input: Raw Sensor Data
Output: Updated NTT

Transform Raw Sensor Data
for $i = 1$ to $Number\ of\ Sensors$ **do**
  if ($Sensor\ Type\ (i) = SONAR$) **then**
    Convert raw data to object at distance *d* from sensor
  else if ($Sensor\ Type\ (i) = LIDAR$) **then**
    Convert raw (X,Y,Z) data to an object
  else if ... **then**
    ...
  end if
end for
Create *Threats* using the objects detected above
for each *Threat* **do**
  if ($Threat\ exists\ in\ NTT$) **then**
    Recalculate *Threat* relevance and replace it in NTT
  else
    Calculate the *Threat* relevance and add it to NTT
  end if
end for
return $Updated\ NTT$

5.2.2 Sharing Threat Matrix

Since NTT initially contains only the threats detected in a vehicle's one-hop communication and sensing range, it is critical to share this information among neighboring vehicles in a timely manner so that the collective visibility and awareness of each vehicle could be improved in terms of range as well as accuracy and precision. As the NTT often contains a large number of threats, it is not feasible to share such large amount of data using the BSMs, which have a maximum size of almost 800 bytes and thus, can hold a maximum of 38 threats only at once. Therefore, the proposed architecture extracts a vehicle's 38 most relevant threats (at maximum) and bundles them together in the form of a *Threat Matrix*. This *Threat Matrix* is then encapsulated in the optional BSM Part II. Hence, when the vehicle broadcasts its BSM, all the neighboring vehicles which receive the BSM will also receive the encapsulated *Threat Matrix*. Note that in case of a BSM packet collision, the

Algorithm 2 Threat Transmission and Reception

Input: *Threat*
Output: BSM Packet
Threat transmission via BSM
for $i = 1$ to $n\ most\ relevant\ threats\ in\ NTT$ **do**
  Add *Threat* i from NTT to *Threat Matrix*
end for
Encapsulate *Threat Matrix* in *BSM* Part II
Broadcast the *BSM*
return $BSMPacket$

Input: BSM packet
Output: Updated NTT
Receive threats from BSM
for $i = 1$ to $total\ threats\ received\ in\ BSM$ **do**
  if ($Threat\ exists\ in\ NTT$) **then**
    Recalculate *Threat* i relevance and replace it in NTT
  else
    Calculate the *Threat* i relevance and add it to NTT
  end if
end for
Update NTT by removing *Threats* no longer relevant
return $Updated\ NTT$

Threat Matrix will be lost and will only be recovered once the vehicle rebroadcasts the BSM in the next broadcasting interval.

5.2.3 Updating Neighboring Threats Table (NTT)

Upon the successful reception of a *Threat Matrix*, the vehicle will update its local NTT with the most relevant threats. If a threat (with the particular ID) does not exist in the NTT, it gets added to the NTT according to its relevance. However, if a threat with the same ID is already present in the NTT, the threat's relevance gets updated in the NTT. Algorithm 2 depicts these design considerations. In this manner, the NTT can continue to grow without any size constraints, as the V2V-equipped vehicles are assumed to have fairly large size databases. Finally, the proposed architecture design is summarized in Figure 5.2.

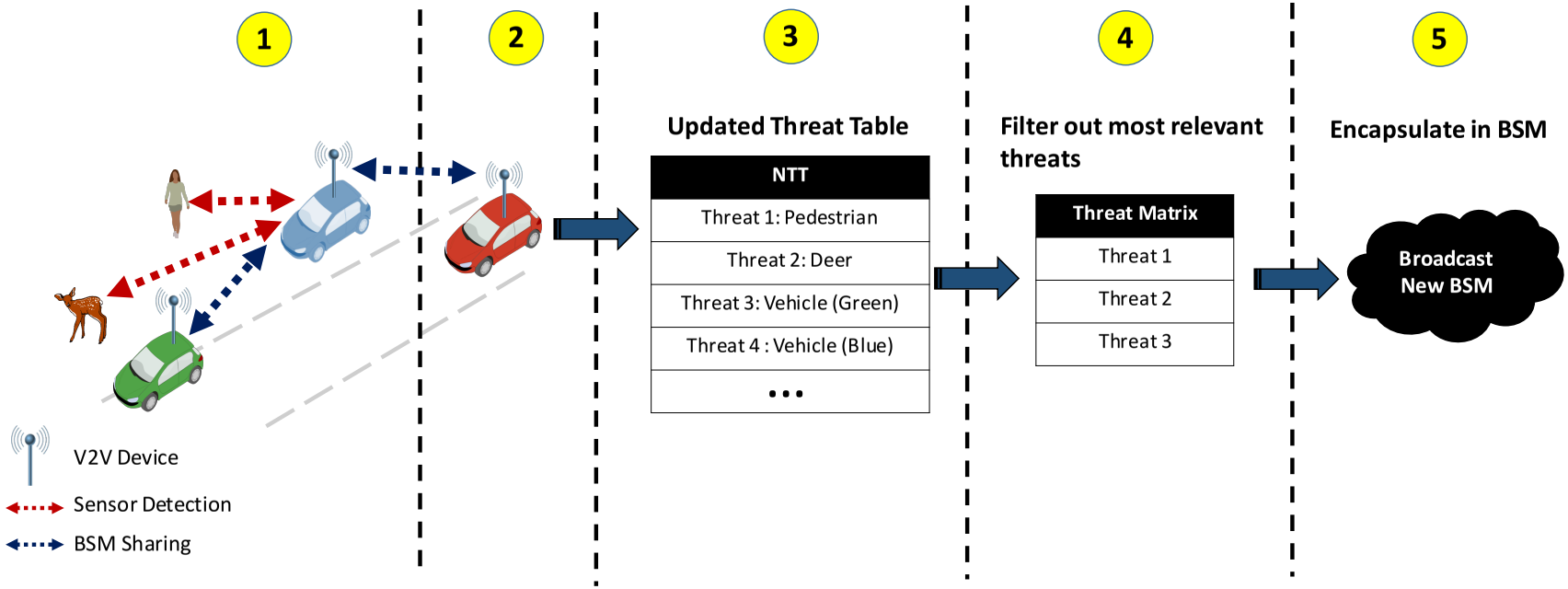


Figure 5.2: BSM-based architecture design – (1) Blue vehicle detects three different threats (pedestrian, deer, and green car) in its path through the on-board sensors as well as V2V communication. (2) It then broadcasts a BSM with this threat information to the red vehicle. (3) Upon reception of BSM, red vehicle updates its NTT with these received threats in the order of relevance. (4) Red vehicle then extracts the most relevant threats from its NTT. (5) It then shares these threats with its neighbors by encapsulating them in the broadcasted BSM.

5.3 Applications

The proposed architecture facilitates several applications of different scope and impact. Among these, some of the most critical applications are briefly discussed here:

5.3.1 Collision Prediction and Avoidance

The additional safety-related information acquired using the proposed architecture in the form of threats can be used to predict and avoid traffic collisions on the roads. For this purpose, the collision detection and prediction algorithms already existing in the literature can be readily applied. Additionally, once a vehicle encounters or predicts a dangerous scenario, it would be able to robustly generate and deliver safety alerts to other vehicles informing them of the impending danger. For this purpose, a multi-hop safety message dissemination algorithm such as Intelligent Forwarding Protocol [14], proposed in the first part of this thesis, can be applied.

5.3.2 Routing

The proposed architecture could also be used to enable efficient routing of packets in VANETs, since each vehicle has an improved visibility with a greater range. For example, those intermediate nodes would be selected as forwarders which form the shortest and most efficient route to the destination. A major challenge with the existing proactive routing schemes in VANETs is that due to the dynamic nature of vehicular environments, they are highly inefficient. However, if the proposed architecture is used instead to route packets, it will depict a much superior performance, since vehicles have a greater awareness of their environment as well as latest information about the existing routes. Another fundamental problem in VANETs is that there is no centralized infrastructure or node which knows the overall topology of the network to calculate the routes, however, the proposed architecture provides each vehicle with a view of the overall topology.

5.3.3 Security

The proposed architecture can also be utilized for improving security in VANETs by confirming that the BSM generated by each vehicle is accurate and not malicious. Through this architecture, it is possible to detect false localization information broadcasts and thus, eliminating the possibility of spoofed data. Having multiple perspectives of the same geographical location from different vehicles can also help in confirming/correcting a vehicle's estimation of its surrounding.

5.4 Simulation Analysis

5.4.1 Simulation Setup

In this section, the simulation results are presented and discussed in order to evaluate the effectiveness and robustness of the proposed architecture. The simulation environment has been set up using ns-3. The parameters chosen for simulation purposes are realistic with minimal assumptions. Table 5.3 presents the parameters used.

Table 5.3: Simulation parameters

Attribute	**Value**
Data rate	6 Mbps (OFDM)
Transmission range (R)	300 meters
Fading model	Rayleigh fading model
Mobility model	Constant velocity mobility
Road dimensions	4 km long (2 lanes)
Node density	50 - 250 nodes
Vehicular Speed	120 kph
BSM Regular Size	39 bytes
BSM Maximum Size	800 bytes
BSM Frequency	10 Hz
Simulation Time (per run)	4 seconds

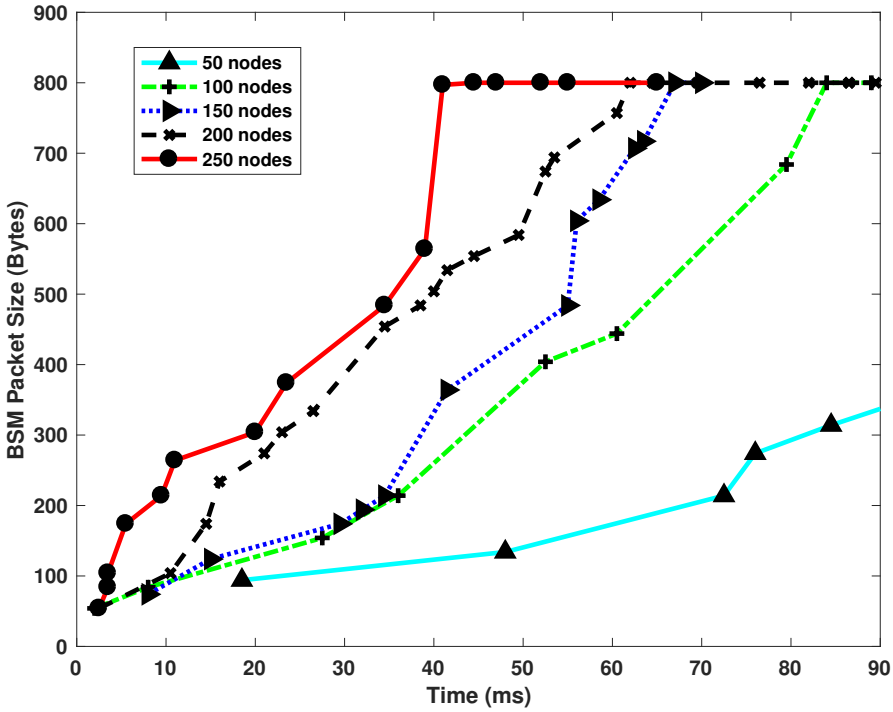


Figure 5.3: BSM packet growth rate.

Since there is no existing protocol which offers a direct comparison to the proposed architecture, we analyze the performance and gains of the proposed architecture by comparing it against the current DSRC standards for V2V communication.

5.4.2 Results & Analysis

First, we measure the effectiveness of the proposed architecture by quantifying the increase in a vehicle's awareness of its surroundings i.e. the number of new threats detected by each V2V-equipped vehicle. The simulation results also determine how quickly a vehicle detects threats in a particular target area.

Figure 5.3 shows the growth of a vehicle's BSM packet size across a short span of time. The significance of this is to illustrate how quickly vehicles build up awareness of threats in their surrounding and then share this information with their neighbors. As a reference point, in the start of the simulation run, it is assumed that vehicles are totally unaware of

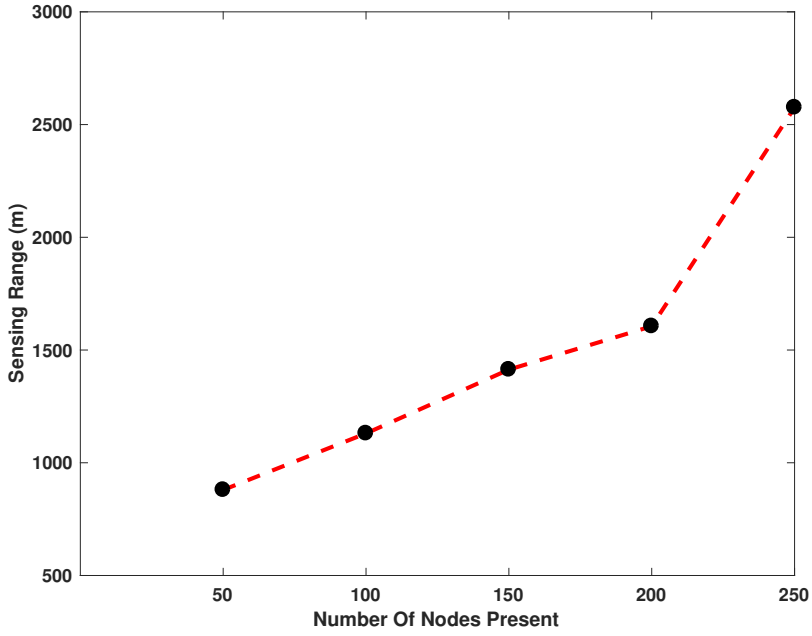


Figure 5.4: Maximum threat detection range in a single CCH interval.

the threats in their environment (i.e. have an empty NTT), and thus share basic BSMs only (with an empty *Threat Matrix*). However, as the time progresses, each vehicle's NTT grows as a result of receiving BSMs (incorporating new threats) from its neighboring vehicles and on-board sensors. Therefore, the *Threat Matrix* of each vehicle starts to swell up with time, which results in more threats being shared between vehicles during each broadcast cycle. In this manner, the BSM size grows sharply. However, since the BSM size is capped at 800 bytes (maximum size allowed), only the 38 most relevant threats ($= (800 - 39)/20$) are shared by a vehicle with its neighbors during each broadcast. A key observation in Figure 5.3 is that traffic scenarios with a high number of nodes (200 or 250 nodes) have a sudden and sharp increase in their BSM packet sizes. This is due to the fact that under such high congestion, each vehicle detects a lot of threats in its vicinity due to the increased number of nodes and BSM broadcasts. Therefore, the *Threat Matrix* gets larger quickly causing the BSM size to increase as well.

On the other hand, Figure 5.4 presents how the maximum threat detection range in a

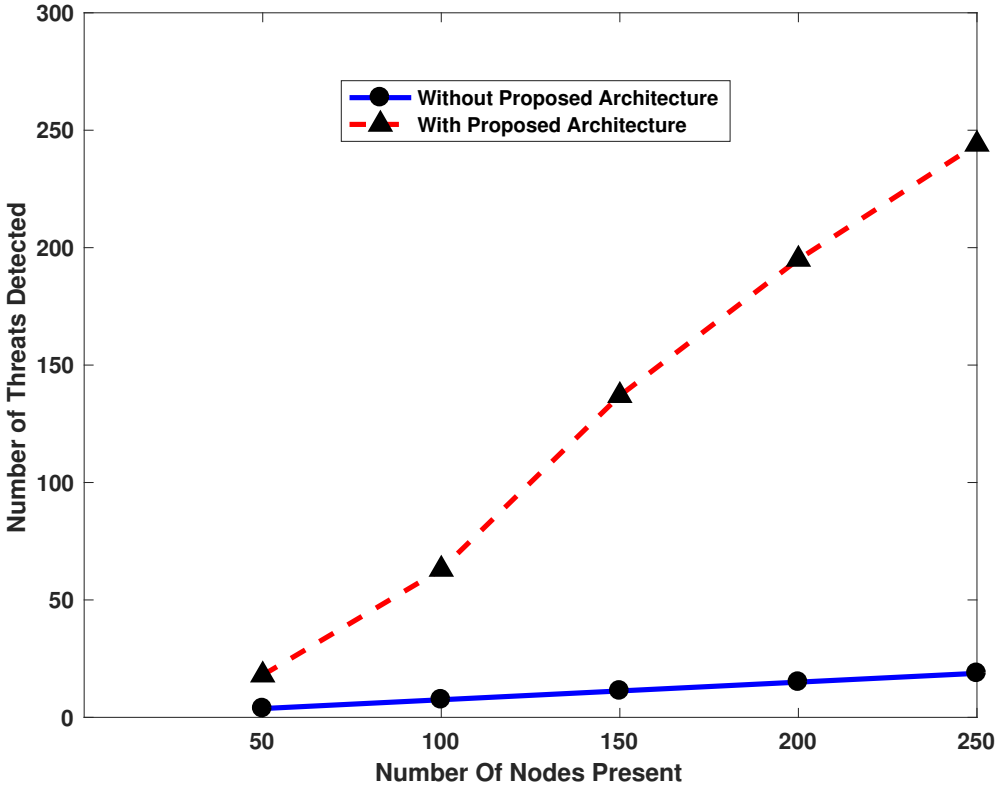


Figure 5.5: Number of threats detected vs. node intensity.

single control channel (CCH) interval (i.e. 50 ms) varies for various node intensities. When there are 50 nodes in the 4 km road strip, a vehicle is able to detect threats as far away as 800 meters within the CCH interval. However, this maximum detection range increases up to 2.5 km when the number of nodes increases to 250 nodes. This occurs because when there are more number of vehicles present, there is a high probability of receiving a greater number of BSMs within a fixed amount of time. Hence, more direct and indirect threats (which are outside the one-hop communication range) can be derived from these BSMs, and stored in the local NTT, thus, increasing the threat detection range. Since, a vehicle can detect threats at such a large distance within a single CCH interval, this tremendously improves the overall transportation safety.

Similarly, Figure 5.5 presents the average number of threats detected by each vehicle

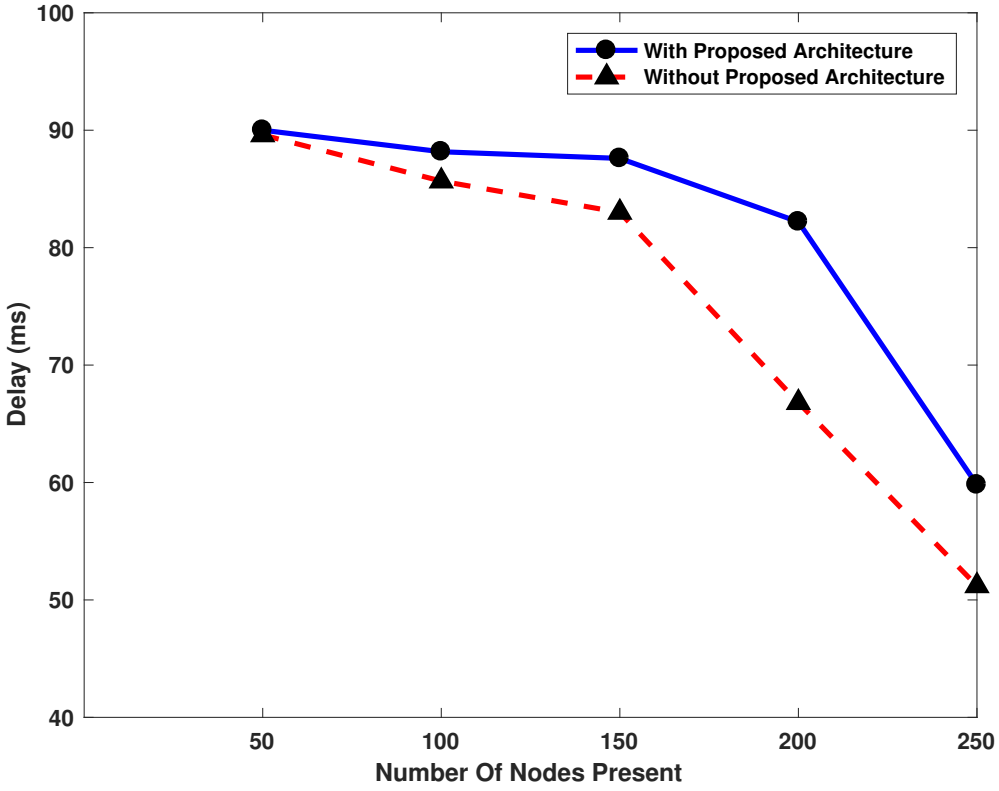


Figure 5.6: End-to-End delay vs. node intensity.

using the proposed architecture as compared to the existing DSRC standards (i.e. using the basic BSM approach) at the end of the simulation runs. It can be noticed that the proposed architecture exhibits a much larger number of threats detected as compared to the traditional approach, since it mandates that each V2V-compatible vehicle shares the information regarding all of the relevant threats with its neighboring vehicles. In this manner, vehicles cooperate to improve their collective awareness of the environment. As can be noted in Figure 5, for 250 nodes in the 4 km road strip, the vehicles with the proposed architecture detect all of the 250 threats, whereas using the traditional approach, they are only able to detect around 20 nodes, which are in their immediate one-hop transmission range.

Finally, Figure 5.6 illustrates the delay it takes for a threat to travel from one end of

the 4 km road-strip to the other. For the proposed architecture, we study the time it takes for a particular threat to cover the 4 km long road-strip, whereas, for the traditional DSRC scheme, the delay refers to the time it takes a threat in a 39 bytes long packet to travel the entire road-strip. It can be noted that the proposed architecture incurs slightly higher delays than the traditional scheme. The reason for this increased delay in proposed architecture is that 800 bytes packets are being shared as compared to the 39 bytes packet in the traditional scheme, and thus it incurs higher transmission delays. Another observation is that for both approaches, when the number of nodes is higher, the end-to-end delay decreases. For our proposed architecture, this behavior can be explained that when there are more number of vehicles present in a region, there will also be a greater number of BSM broadcasts in a certain time interval, and thus, the threat gets relayed at a faster rate. On the other hand, for the traditional scheme, when the node intensity is high, there are more chances of a forwarding node being closer to the boundary of the transmission range, and thus more distance can be covered per hop. This reduces the overall end-to-end delay.

5.5 Experimentation

Next, we conduct a feasibility study of the proposed BSM architecture under real-world VANET conditions.

5.5.1 Experimental Setup

To thoroughly evaluate and analyze the proposed architecture, we implemented a test-bed consisting of up to five cars, and carried out experimentation in urban, highway, and stationary conditions. All cars were equipped with DSRC-based Arada Systems on-board units (OBUs) to enable V2V communications. The implementation of the architecture was done using Arada Systems built-in Locomate library. The cars were distributed in three zones as depicted in Figure 5.7, where each zone was populated with a different number of threats. The distance between the cars is controlled in order to ensure that there exist no

Table 5.4: Experimental parameters

Attribute	Value
Data rate	6 Mbps (OFDM)
Transmission range (R)	300 meters
Vehicular Speed	0-100 kph
BSM Regular Size	39 bytes
BSM Maximum Size	200, 500, 800 bytes
BSM Frequency	2, 5, 10 Hz
Packet Loss Rate	0%, 10%, 20%
External Threats Per Vehicle	4, 5, 6

coverage gaps between vehicles. All cars traveled in the same direction. For each result, we used the average value of atleast ten measurements (ten runs). While most parameters used in experimentation are similar to those in simulations, some of the important ones are listed in Table 5.4. The parameters chosen are realistic, and conform to the typical VANET environment.

We evaluate the proposed architecture with regard to the following important metrics: collision rate, threat detection rate, packet delivery ratio, broadcast frequency, etc. Since

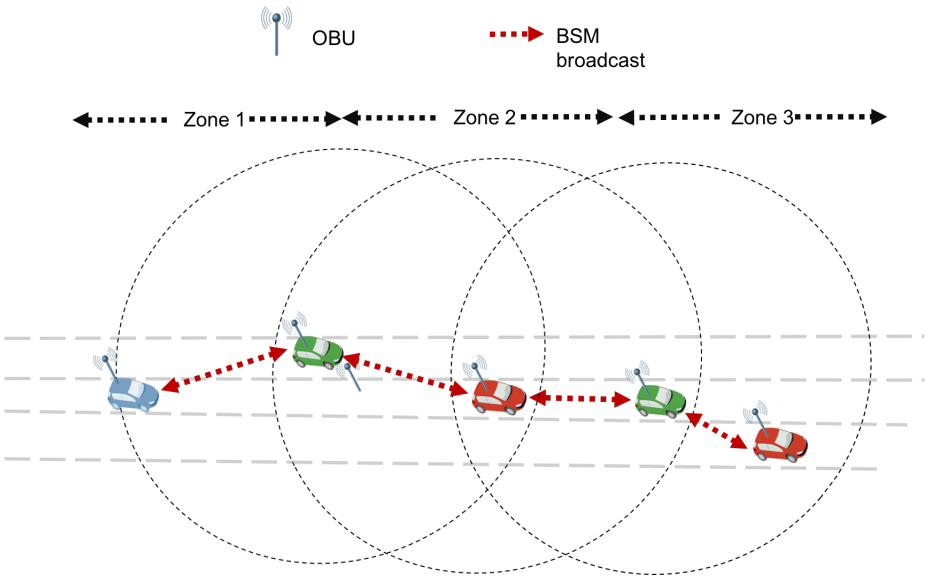


Figure 5.7: Experimental topology.

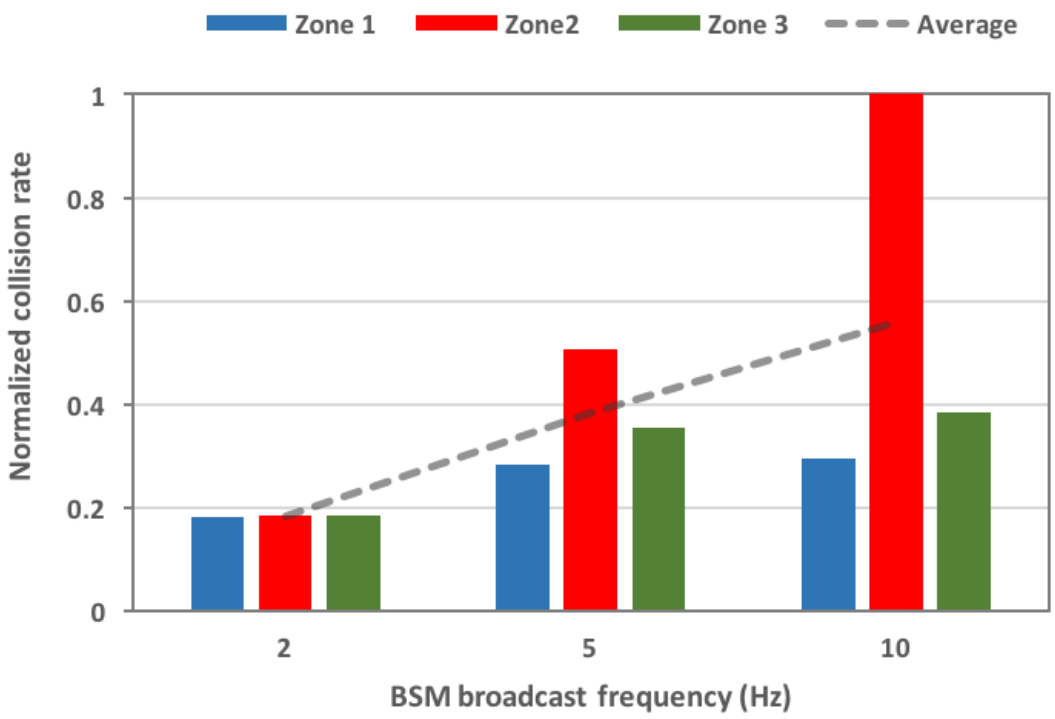


Figure 5.8: Collision rate vs. broadcast frequency.

there is no existing protocol which offers a direct comparison to the proposed architecture, we only present an analysis of the proposed architecture here.

5.5.2 Results and Analysis

First, we study the effect of the proposed architecture on packet collision rate. Figure 5.8 shows the collision rate in each of the three zones as the broadcast frequency varies. It can be noted from the figure that as the broadcast frequency increases from 2 Hz to 10 Hz, the collisions also increase for all three zones. With an increase in the number of BSM broadcasts in a fixed time interval, the CCH gets flooded with transmissions from multiple vehicles, which results in more collision occurrences. Therefore, under high traffic congestion, it is recommended to broadcast BSMs at a lower frequency. Another observation from Figure 5.8 is that zone 2 depicts a higher collision rate as compared to the other zones.

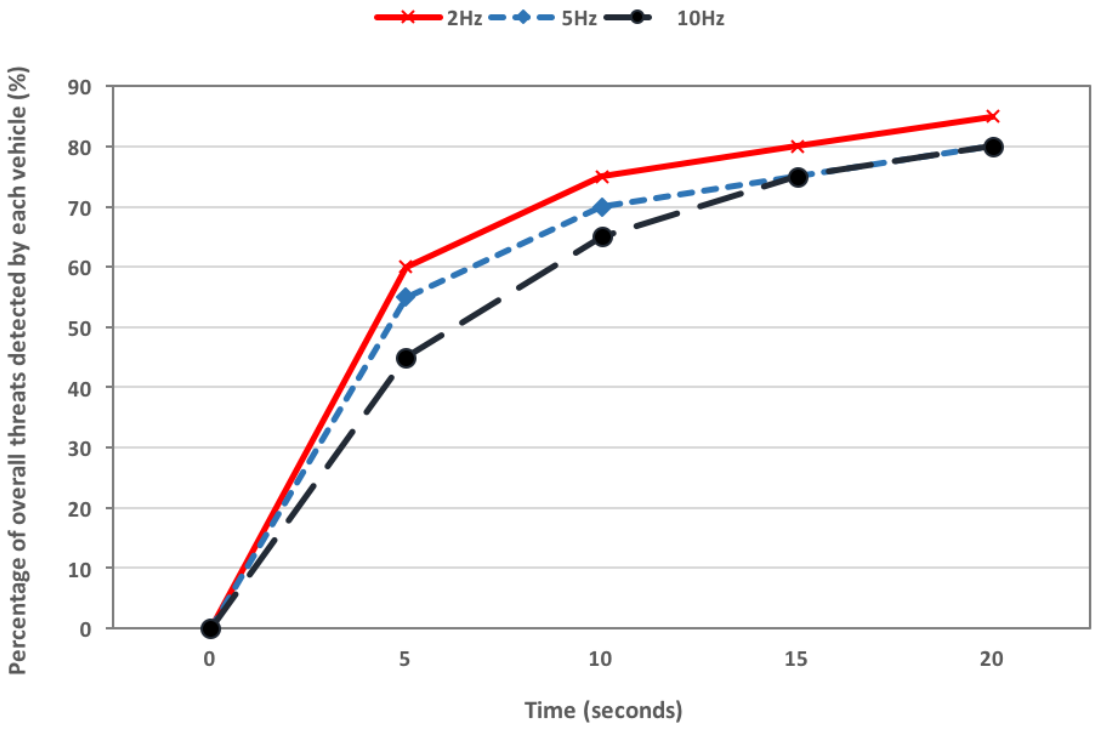


Figure 5.9: Threat detection at different broadcast frequencies.

Since zone 2 lies in the middle of the other two zones, the vehicles in zone 2 are within the communication range of other vehicles in the remaining two zones. Therefore, zone 2 encounters more broadcast interference, which results in a higher collision rate.

Next, we evaluate the threat detection rate under different broadcast frequencies. Figure 5.9 portrays the overall proportion of threats detected by each vehicle using the proposed architecture. Once again, the lowest BSM broadcast frequency of 2 Hz outperforms the higher frequencies, and results in more threats being detected. As previously discussed, a broadcast frequency of 2 Hz results in the least amount of packet collisions, and thus, more threats are effectively shared between vehicles in a given amount of time. Hence, the proposed architecture enables each vehicle to detect about 90% of the total threats in the entire target region within 20 seconds.

In order to ensure the reliable delivery of BSMs to the intended vehicles, we measured

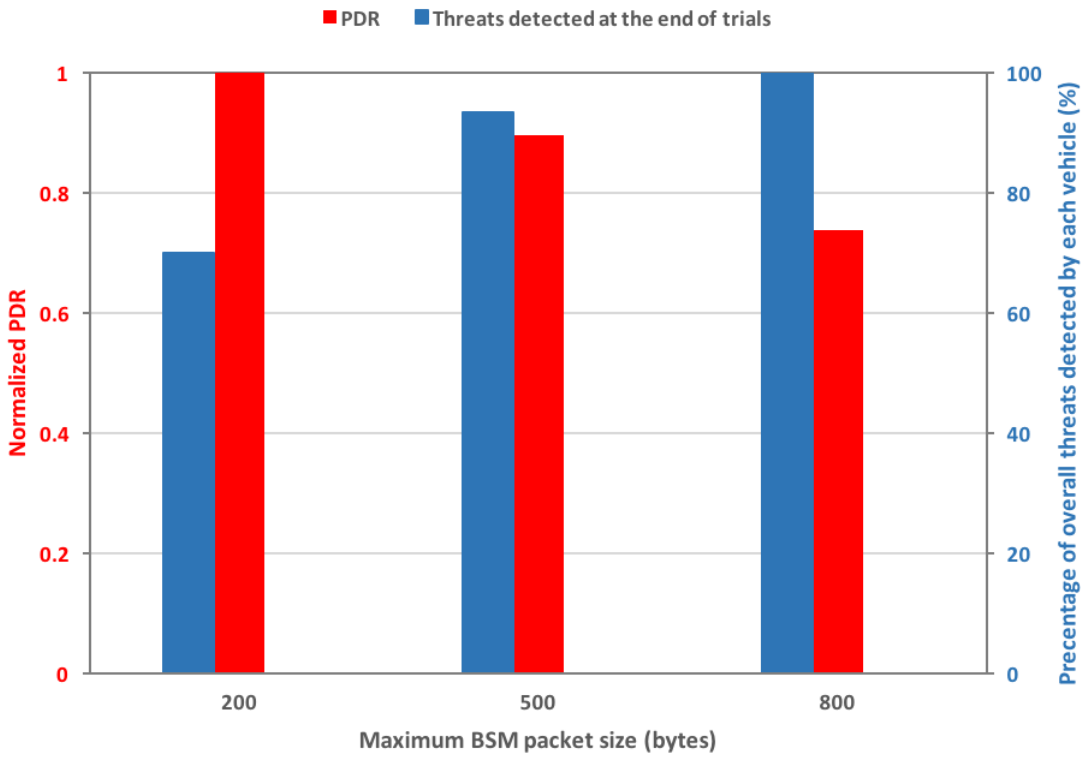


Figure 5.10: Effect of BSM packet size on PDR and threat detection.

the Packet Delivery Ratio (PDR) of the proposed architecture, as the maximum BSM packet size varies in Figure 5.10. Here, PDR refers to the ratio of number of vehicles that actually receive the BSM packet to the total number of expected receivers. The PDR results have been normalized to present a fair comparison between the different experimental trials and settings. As shown in Figure 5.10, the PDR decreases with an increase in the maximum BSM packet size. A larger packet size increases the collision probability, and thus, results in a lower PDR. However, since a larger BSM packet (800 bytes long) encapsulates more number of threats, even with a lower PDR, it results in more threats being shared between vehicles. Therefore, the average number of threats detected at the end of each experimental trial is higher with a BSM packet size of 800 bytes.

Finally, in Figure 5.11, the effect of varying packet loss rate on the PDR and threat detection rate has been studied. With an increase in packet loss rate, the PDR decreases, as

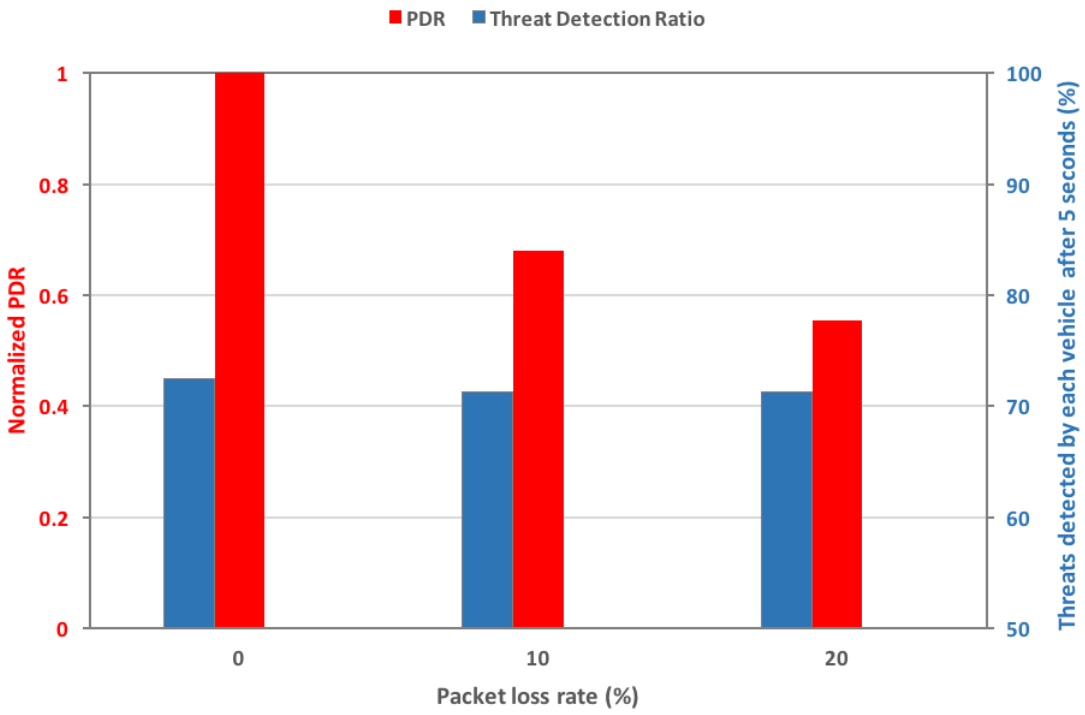


Figure 5.11: Effect of packet loss rate on PDR and threat detection.

lower number of BSMs are actually delivered to the vehicles. However, the average number of threats detected by each vehicle after 5 seconds stays constant regardless of the packet loss rate. Since each vehicle broadcasts the BSM at a regular interval (10 times every second), even with a few packet losses, the threats are still delivered to the neighboring vehicles due to the redundant broadcasts of the same threats. Therefore, the proposed architecture is resilient to a lossy VANET environment.

In this chapter, a novel architecture has been presented that enhances the transportation safety by efficiently sharing safety information among vehicles. By storing and exchanging the information obtained from the neighboring vehicles as well as from other active sensors on the vehicle, safety information can be shared with vehicles beyond the one-hop communication range by utilizing the mandated BSM packets. The proposed architecture was evaluated under both simulation and real-world traffic conditions. The results establish and validate the performance gain of the proposed scheme.

CHAPTER 6
CONCLUSION AND FUTURE WORK

6.1 Conclusion

In vehicular ad-hoc networks (VANETs), fast and reliable dissemination of safety information is a key step toward improving the overall transportation safety. In a highly dynamic VANET environment, safety message dissemination is a challenging and complex problem that has gained significant attention recently. The purpose of this dissertation is to provide innovative and feasible methods for efficient dissemination of safety information in VANETs. In this regard, we have developed two novel schemes as discussed below.

First, this dissertation presents a highly efficient and reliable multi-hop broadcasting protocol for delivering safety messages to vehicles beyond the transmission range of the sender. We refer to this protocol as Intelligent Forwarding Protocol (IFP). IFP proposes a smart mechanism of exploiting both the SNR values and the geographical coordinates of vehicles in the forwarder selection process, resulting in higher per-hop message progress and message reception reliability. Additionally, IFP reduces the forwarding latency by removing the need for costly handshaking mechanisms and by decoupling acknowledgments from the message dissemination process. Furthermore, IFP introduces an improved collision resolution mechanism, such that packet collisions could be resolved quickly. A detailed theoretical model and extensive simulation results of IFP have been presented, which establish the performance gain of IFP over existing techniques. Additionally, real-world experimentation and field-trials were conducted using the IEEE 802.11 p devices to evaluate the performance of IFP under real traffic conditions. The results validate the performance gain achieved by IFP in such conditions. Since IFP allows for a straight-forward and seamless integration in the existing DSRC standards, it could be readily deployed in all

V2V-equipped vehicles to improve the transportation safety. The work related to this protocol has been published in [12] and[13], while some portion of the work is under review in [14].

Next, this research proposes a novel architecture that employs a proactive approach for sharing safety information in VANETs to increase the visibility and awareness of the vehicles. Through this architecture, vehicles are able to identify potential threats in their environment (such as vehicles, pedestrians, wild-life etc.) by intelligently exchanging and storing the data obtained from neighboring vehicles as well as from on-board sensor technologies. Since BSMs are mandated by the DSRC standards, and are broadcast frequently throughout the network, this research leverages the BSM-sharing infrastructure to share safety information in VANETs with low latency. In contrast to many existing safety information delivery protocols that require modifications to the DSRC standards for successful operation, the proposed architecture enables information sharing among vehicles by just exploiting the existing standards for V2V communication, and without requiring any modification to these standards. Moreover, we also introduce a standard threat format through which any raw sensory data could be represented. The proposed architecture was evaluated under both simulation and real-world traffic conditions. The results demonstrate the performance gain achieved by the proposed scheme in terms of threat detection rate, message reception reliability, etc., while placing minimum overhead and complexity on the network. The work pertaining to this architecture has been published in [15], while some portion of the work is in preparation for submission in [16].

6.2 Future Work

To further improve the safety message dissemination process, we discuss some important ideas for future work below:

- The techniques proposed in this dissertation currently exploit the control channel only for safety message dissemination. For future work, we plan to extend these

techniques for service channels in order to reduce the congestion of the common control channel and reduce packet collisions. However, since vehicles are allowed to tune in to any one of the six service channels, there exists a need for a mechanism to select appropriate service channels such that safety information can be optimally delivered to all vehicles.

- In order to further optimize the proposed schemes for different traffic scenarios, the experimental test-bed should ideally be expanded to include more V2V-equipped vehicles and road side units.

- With the projected increase in the deployment of road-side units in the urban roadways in the near future, there is a need for actively involving road-side units in the safety message forwarding and safety information sharing processes.

- With the recent expansion of LTE services to enable V2X communication in 3GPP Release 14 [62], the protocols presented in this dissertation can be extended to the LTE-based V2X communication platform, such that optimal paths can be selected for safety message delivery. This will ultimately lead to lower end-to-end delays, less packet collisions, and a more reliable message delivery mechanism.

REFERENCES

[1] National Highway Traffic Safety Administration. "Traffic safety facts - 2014 crash data key findings: A brief statistical summary". In: *Report no. DOT HS-812-219, US Department of Transportation* (November 2015).

[2] L. Blincoe et al. "The economic and societal impact of motor vehicle crashes, 2010 (Revised)". In: *Report no. DOT HS-812-013, National Highway Traffic Safety Administration* (May 2015).

[3] Roy L Courtney. "A broad view of ITS standards in the US". In: *Intelligent Transportation System, 1997. ITSC'97., IEEE Conference on*. IEEE. 1997, pp. 529–536.

[4] Elena Fasolo, Andrea Zanella, and Michele Zorzi. "An effective broadcast scheme for alert message propagation in vehicular ad hoc networks". In: *Communications, 2006. ICC'06. IEEE International Conference on*. Vol. 9. IEEE. 2006, pp. 3960–3965.

[5] John B Kenney. "Dedicated short-range communications (DSRC) standards in the United States". In: *Proceedings of the IEEE* 99.7 (2011), pp. 1162–1182.

[6] Sooksan Panichpapiboon and Wasan Pattara-Atikom. "A review of information dissemination protocols for vehicular ad hoc networks". In: *IEEE Commun. Surveys & Tutorials* 14.3 (2012), pp. 784–798.

[7] Georgios Karagiannis et al. "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions". In: *IEEE communications surveys & tutorials* 13.4 (2011), pp. 584–616.

[8] Rex Chen, Wen-Long Jin, and Amelia Regan. "Broadcasting safety information in vehicular networks: issues and approaches". In: *IEEE network* 24.1 (2010).

[9] Daniel Jiang and Luca Delgrossi. "IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments". In: *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*. IEEE. 2008, pp. 2036–2040.

[10] Roberto A Uzcátegui, Antonio Jose De Sucre, and Guillermo Acosta-Marum. "Wave: A tutorial". In: *IEEE Communications magazine* 47.5 (2009).

[11] Yasuto Kudoh. "DSRC standards for multiple applications". In: *Proceedings of 11th world congress on ITS*. 2004.

[12] Voicu, R. C. and Abbasi, H. I. and Fang, H. and Kihei, B. and Copeland, J. A. and Chang, Y. "Fast and reliable broadcasting in VANETs using SNR with ACK decoupling". In: *Communications (ICC), 2014 IEEE International Conference on*. IEEE. 2014, pp. 574–579.

[13] Hamza Ijaz Abbasi et al. "Performance optimization of a contention based broadcasting algorithm in VANETs". In: *Global Communications Conference (GLOBECOM), 2015 IEEE*. IEEE. 2015, pp. 1–7.

[14] Hamza Ijaz Abbasi et al. "Towards Fast and Reliable Multihop Routing in VANETs". In: *submitted to IEEE Transactions on Mobile Computing* (2018).

[15] Hamza Ijaz Abbasi et al. "Cooperative BSM architecture to improve transportation safety in VANETs". In: *Wireless Communications and Mobile Computing Conference (IWCMC), 2017 13th International*. IEEE. 2017, pp. 1016–1022.

[16] Hamza Ijaz Abbasi et al. "Cooperative BSM-based architecture to enhance safety information sharing in VANETs". In: *in preparation for submission to IEEE Transactions on Intelligent Transportation Systems* (2018).

[17] Jinhua Guo and Nathan Balon. "Vehicular ad hoc networks and dedicated short-range communication". In: *University of Michigan* (2006).

[18] Barlomiej Blaszczyszyn, Paul Muhlethaler, and Yasser Toor. "Performance of MAC protocols in linear VANETs under different attenuation and fading conditions". In: *Intelligent Transportation Systems, 2009. ITSC'09. 12th International IEEE Conference on*. IEEE. 2009, pp. 1–6.

[19] Ting Zhong, Bo Xu, and Ouri Wolfson. "Disseminating real-time traffic information in vehicular ad-hoc networks". In: *Intelligent Vehicles Symposium, 2008 IEEE*. IEEE. 2008, pp. 1056–1061.

[20] Tamer Nadeem et al. "Trafficview: A scalable traffic monitoring system". In: *Mobile Data Management, 2004. Proceedings. 2004 IEEE International Conference on*. IEEE. 2004, pp. 13–26.

[21] Takeshi Fujiki et al. "Efficient acquisition of local traffic information using inter-vehicle communication with queries". In: *Intelligent Transportation Systems Conference, 2007. ITSC 2007. IEEE*. IEEE. 2007, pp. 241–246.

[22] Qiangyuan Yu and Geert Heijenk. "Abiding geocast for warning message dissemination in vehicular ad hoc networks". In: *Communications Workshops, 2008. ICC Workshops' 08. IEEE International Conference on*. IEEE. 2008, pp. 400–404.

[23] Lars Wischhof, André Ebner, and Hermann Rohling. “Information dissemination in self-organizing intervehicle networks”. In: *IEEE Transactions on intelligent transportation systems* 6.1 (2005), pp. 90–101.

[24] Swarun Kumar et al. “Carspeak: a content-centric network for autonomous driving”. In: *ACM SIGCOMM Computer Communication Review* 42.4 (2012), pp. 259–270.

[25] Hongseok Yoo and Dongkyun Kim. “ROFF: RObust and Fast Forwarding in vehicular ad-hoc networks”. In: *IEEE Transactions on Mobile Computing* 14.7 (2015), pp. 1490–1502.

[26] Min-Te Sun et al. “GPS-based message broadcast for adaptive inter-vehicle communications”. In: *Vehicular Technology Conference, 2000. IEEE. 52nd*. Vol. 6. IEEE. 2000, pp. 2685–2692.

[27] Tatsuaki Osafune, Lan Lin, and Massimiliano Lenardi. “Multi-hop vehicular broadcast (MHVB)”. In: *2006 6th international conference on ITS telecommunications*. IEEE. 2006, pp. 757–760.

[28] Linda Briesemeister and Günter Hommel. “Role-based multicast in highly mobile but sparsely connected ad hoc networks”. In: *Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing*. IEEE Press. 2000, pp. 45–50.

[29] Abdelmalik Bachir and Abderrahim Benslimane. “A multicast protocol in ad hoc networks inter-vehicle geocast”. In: *Vehicular Technology Conference, 2003. The 57th IEEE Semiannual*. Vol. 4. IEEE. 2003, pp. 2456–2460.

[30] Chih-Wei Yi et al. “Streetcast: An urban broadcast protocol for vehicular ad-hoc networks”. In: *Vehicular Tech. Conference, 2010 IEEE 71st*, pp. 1–5.

[31] Abderrahim Benslimane. “Optimized dissemination of alarm messages in vehicular ad-hoc networks (VANET)”. In: *IEEE International Conference on High Speed Networks and Multimedia Communications*. Springer. 2004, pp. 655–666.

[32] Wantanee Viriyasitavat, Fan Bai, and Ozan K Tonguz. “UV-CAST: an urban vehicular broadcast protocol”. In: *Vehicular Networking Conference (VNC), 2010 IEEE*. IEEE. 2010, pp. 25–32.

[33] Yu-Chee Tseng et al. “The broadcast storm problem in a mobile ad hoc network”. In: *Wireless networks* 8.2/3 (2002), pp. 153–167.

[34] Da Li et al. “A distance-based directional broadcast protocol for urban vehicular ad hoc network”. In: *2007 International Conference on Wireless Communications, Networking and Mobile Computing*. IEEE. 2007, pp. 1520–1523.

[35] Y-T Yang and L-D Chou. “Position-based adaptive broadcast for inter-vehicle communications”. In: *ICC Workshops-2008 IEEE Int. Conference on Commun. Workshops*. IEEE. 2008, pp. 410–414.

[36] Gökhan Korkmaz et al. “Urban multi-hop broadcast protocol for inter-vehicle communication systems”. In: *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*. ACM. 2004, pp. 76–85.

[37] Gökhan Korkmaz, Eylem Ekici, and FÜsun Ozguner. “Black-burst-based multihop broadcast protocols for vehicular networks”. In: *IEEE Transactions on Vehicular Technology* 56.5 (2007), pp. 3159–3167.

[38] Giovanni Ciccarese et al. “On the use of control packets for intelligent flooding in VANETs”. In: *Wireless Communications and Networking Conference, 2009. WCNC 2009. IEEE*. IEEE. 2009, pp. 1–6.

[39] Jagruti Sahoo et al. “Binary-partition-assisted MAC-layer broadcast for emergency message dissemination in VANETs”. In: *IEEE Transactions on Intelligent Transportation Systems* 12.3 (2011), pp. 757–770.

[40] Mostafa MI Taha and Yassin MY Hasan. “VANET-DSRC protocol for reliable broadcasting of life safety messages”. In: *Signal Processing and Information Technology, 2007 IEEE International Symposium on*. IEEE. 2007, pp. 104–109.

[41] Yu-Tian Tseng et al. “A vehicle-density-based forwarding scheme for emergency message broadcasts in VANETs”. In: *Mobile Adhoc and Sensor Systems (MASS), 2010 IEEE 7th International Conference on*. IEEE. 2010, pp. 703–708.

[42] Ramon S Schwartz et al. “A simple and robust dissemination protocol for VANETs”. In: *Wireless Conference (EW), 2010 European*. IEEE. 2010, pp. 214–222.

[43] Qiong Yang and Lianfeng Shen. “A multi-hop broadcast scheme for propagation of emergency messages in VANET”. In: *Communication Technology (ICCT), 2010 12th IEEE International Conference on*. IEEE. 2010, pp. 1072–1075.

[44] Nawaporn Wisitpongphan, Ozan K Tonguz, Jayendra S Parikh, et al. “Broadcast storm mitigation techniques in vehicular ad hoc networks”. In: *IEEE Wireless Commun.* 14.6 (2007), pp. 84–94.

[45] Hamada ALshaer and Eric Horlait. “An optimized adaptive broadcast scheme for inter-vehicle communication”. In: *Vehicular Technology Conference, 2005 IEEE 61st*. Vol. 5. IEEE. 2005, pp. 2840–2844.

[46] Axel Wegener et al. “AutoCast: An adaptive data dissemination protocol for traffic information systems”. In: *Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th*. IEEE. 2007, pp. 1947–1951.

[47] Sangho Oh, Jaewon Kang, and Marco Gruteser. “Location-based flooding techniques for vehicular emergency messaging”. In: *Mobile and Ubiquitous Systems-Workshops, 2006. 3rd Annual International Conference on*. IEEE. 2006, pp. 1–9.

[48] Khaled Ibrahim, Michele C Weigle, and Mahmoud Abuelela. “p-IVG: Probabilistic inter-vehicle geocast for dense vehicular networks”. In: *Vehicular Technology Conference, 2009. IEEE 69th*. IEEE. 2009, pp. 1–5.

[49] Khalid Abdel Hafeez et al. “A new broadcast protocol for vehicular ad hoc networks safety applications”. In: *GLOBECOM 2010, 2010 IEEE*. IEEE. 2010, pp. 1–5.

[50] Stefano Busanelli, Gianluigi Ferrari, and Sooksan Panichpapiboon. “Efficient broadcasting in IEEE 802.11 networks through irresponsible forwarding”. In: *GLOBECOM 2009. 2009 IEEE*. IEEE. 2009, pp. 1–6.

[51] Anna Maria Vegni, Ahmad Mostafa, and Dharma P Agrawal. “CAREFOR: Collision-aware reliable forwarding technique for vehicular ad hoc networks”. In: *Computing, Networking and Communications (ICNC), 2013 International Conference on*. IEEE. 2013, pp. 773–777.

[52] Rudolf Ahlswede, Ning Cai, et al. “Network information flow”. In: *IEEE Trans. on information theory* 46.4 (2000), pp. 1204–1216.

[53] Li Li et al. “Network coding-based broadcast in mobile ad-hoc networks”. In: *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*. IEEE. 2007, pp. 1739–1747.

[54] Shuhui Yang and Jie Wu. “Efficient broadcasting using network coding and directional antennas in MANETs”. In: *IEEE Transactions on Parallel and Distributed Systems* 21.2 (2010), pp. 148–161.

[55] Nour Kadi and Khaldoun Al Agha. “Mpr-based flooding with distributed fountain network coding”. In: *Ad Hoc Networking Workshop (Med-Hoc-Net), 2010 9th IFIP Annual Mediterranean*. IEEE. 2010, pp. 1–5.

[56] Celimuge Wu et al. “Efficient broadcasting in vanets using dynamic backbone and network coding”. In: *IEEE Tran. on Wireless Comm.* 14.11 (2015), pp. 6057–6071.

[57] Celimuge Wu et al. “Joint fuzzy relays and network-coding-based forwarding for multihop broadcasting in vanets”. In: *IEEE Transactions on Intelligent Transportation Systems* 16.3 (2015), pp. 1415–1427.

[58] Mi-Ryong Park, Dongwon Kim, and Sang-Ha Kim. “A simple SNR based linear back-off to propagate multi-hop emergency messages on the distributed VANETs”. In: *Computer Applications for Modeling, Simulation, and Automobile* (2012), pp. 34–41.

[59] Marc Torrent-Moreno, Daniel Jiang, and Hannes Hartenstein. “Broadcast reception rates and effects of priority access in 802.11-based vehicular ad-hoc networks”. In: *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*. ACM. 2004, pp. 10–18.

[60] Mate Boban, Wantanee Viriyasitavat, and Ozan K Tonguz. “Modeling vehicle-to-vehicle line of sight channels and its impact on application-layer performance”. In: *Proceeding of the tenth ACM international workshop on Vehicular inter-networking, systems, and applications*. ACM. 2013, pp. 91–94.

[61] Hyun-Sook Kim et al. “A relay vehicle selection scheme for delivery of emergency message considering density and trajectory of moving vehicles for VANET”. In: *Advanced Computer Science and Information Tech.* Springer, 2011, pp. 257–266.

[62] Christian Hoymann et al. “LTE release 14 outlook”. In: *IEEE Communications Magazine* 54.6 (2016), pp. 44–49.