

SAFETY-MESSAGE ROUTING IN VEHICULAR AD HOC NETWORKS

A Dissertation
Presented to
The Academic Faculty

By
Faisal Ahmad Khan

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



School of Electrical and Computer Engineering
Georgia Institute of Technology
May 2013

Copyright © 2013 by Faisal Ahmad Khan

SAFETY-MESSAGE ROUTING IN VEHICULAR AD HOC NETWORKS

Approved by:

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

Professor Raheem Beyah
School of Electrical and Computer Engineering
Georgia Institute of Technology

Professor Yusun Chang
School of Electrical and Computer Engineering
Georgia Institute of Technology

Professor Mostafa Ammar
School of Computer Science
Georgia Institute of Technology

Professor Henry Owen
School of Electrical and Computer Engineering
Georgia Institute of Technology

Professor George Riley
School of Electrical and Computer Engineering
Georgia Institute of Technology

Date Approved: December 2012

DEDICATION

To my parents

ACKNOWLEDGMENTS

I would like to express my sincere thanks to Dr. John A. Copeland for being my mentor during my entire graduate studies at Georgia Tech. I am deeply grateful to him for his support, guidance, understanding, and patience during this doctoral research. Thank you Dr. Copeland for being a perfect model for me. I am wholeheartedly thankful to my co-advisor Dr. Yusun Chang for his support, guidance, and supervision throughout my research work. I am very thankful to Dr. Chang for his excellent and diligent guidance that consistently stimulated new ideas for me.

I am grateful to Dr. Reheem Beyah and Dr. Henry Owen for reading this dissertation and providing me their valuable feedback. I would also like to thank Dr. Mostafa Ammar and Dr. George Riley for serving on my dissertation defense committee. I would like to thank the Higher Education Commission of Pakistan and the Fulbright Scholarship program for providing me the opportunity to pursue my doctoral research in an uninterrupted manner.

I am grateful to my friend and colleague Sung Jin Park for his help and discussions throughout my time at the Communications Systems Center (CSC). My special thanks to my friends and colleagues, Gong Chen, Pan Zhou, Jinyoun Cho, Selcuk Uluagac, Moazzam Khan, Shi-In Chang, Luis Miguel, Daniel Lertpratchya, and Joe Benin.

Lastly, I thank my parents and my family. Thank you Lala, Anga, Walala, Ajmal, Akmal, Nini, Gullashta, Zeba, Azlan, and Arwa for everything.

CONTENTS

DEDICATION	iii
LIST OF TABLES	vii
LIST OF FIGURES	viii
SUMMARY	x
CHAPTER 1 INTRODUCTION	1
1.1 Overview of Vehicular Ad Hoc Networks	1
1.1.1 VANET Characteristics	2
1.1.2 Standards for VANET Communications	4
1.2 Routing in Vehicular Ad Hoc Networks	5
1.3 Related Work	9
CHAPTER 2 DELAY IMPROVEMENT	14
2.1 Prelude	14
2.2 Instant Broadcast	15
2.3 Multi-hop Delay Estimation	18
2.4 Simulation Analysis	22
2.4.1 Simulation Setup	22
2.4.2 Results and Discussion	23
CHAPTER 3 COLLISION MITIGATION	30
3.1 Vehicular Communication in Dense-Urban Traffic	30
3.2 Road Width in Vehicular Communication	32
3.3 Broadcast with Lane-based Sectoring	33
3.4 Delay Analysis	35
3.5 Simulation Analysis	37
CHAPTER 4 RECOVERING THE MESSAGE LOSS CAUSED BY INTER- FERENCE	43
4.1 Message Loss from Collisions	43
4.2 System Model and Assumptions	45
4.3 NACK with Smart Neighborhood (NSN)	46

4.4	Analysis of the NSN Algorithm	49
4.4.1	Reliability metrics and base parameters	49
4.4.2	Packet-reception ratio (PRR) formulation	53
4.5	Simulation Analysis	56
CHAPTER 5 MESSAGE DELIVERY TO THE COVERAGE HOLES		63
5.1	Coverage Holes in the Vehicular Scenario	63
5.2	Negative Acknowledgment with Hole Recovery (NSN-H)	66
5.3	Coverage Hole Detection	68
5.3.1	Determining the vehicles obstructing the line of sight	70
5.3.2	Attenuation caused by an obstructing vehicle	71
5.4	Simulation Analysis	74
5.4.1	Simulation Setup	74
5.4.2	Results and Discussion	75
CHAPTER 6 CONCLUSIONS AND FUTURE WORK		86
REFERENCES		90

LIST OF TABLES

Table 1	Simulation parameters for UMB, SB and IB schemes.	23
Table 2	Simulation parameters for NB and LB.	37
Table 3	Simulation parameters for the NSN technique.	57
Table 4	Simulation parameters for NSN-H evaluation.	75
Table 5	Dimensions of vehicles.	75

LIST OF FIGURES

Figure 1	The sequence of packets in the handshake-based broadcast scheme and in the instant-broadcast scheme.	17
Figure 2	Markov-chain model with hidden-node collisions.	19
Figure 3	The average network throughput with variable packet sizes.	24
Figure 4	Average one-hop delay with variable settings of l and N	25
Figure 5	Mean delay with respect to distance.	26
Figure 6	Mean delay with variable message-generation rate	27
Figure 7	Average network load generation by each message.	28
Figure 8	The average success percentage.	29
Figure 9	Back-off-value assignment using lane-based sectoring.	35
Figure 10	Average rebroadcast delay in four and eight lanes (message size = 300 bytes).	39
Figure 11	Average rebroadcast delay in four and eight lanes (message size = 1000 bytes).	40
Figure 12	Average collision percentage.	42
Figure 13	Recovering unrecoverd signal using negative-acknowledgement with smart neighborhood.	48
Figure 14	Omni-directional broadcast in a linear setting.	53
Figure 15	Effect of simultaneous transmissions from nodes in the interference region.	55
Figure 16	Packet loss rate of NSN, UMB and R-OB-VAN methods.	58
Figure 17	Normalized load generated of NSN, UMB and R-OB-VAN methods.	60
Figure 18	Mean one-hop delay of NSN, UMB and R-OB-VAN methods.	61
Figure 19	Mean propagation delay of NSN, UMB and R-OB-VAN methods.	62
Figure 20	Coverage holes in the broadcast range.	64
Figure 21	Recovering message loss in a hole using negative-acknowledgment with smart neighborhood.	66
Figure 22	Determining the intersection between a line segment and a rectangle.	71

Figure 23	Single knife-edge diffraction between vehicles.	72
Figure 24	Multiple knife-edge diffraction between vehicles.	73
Figure 25	Average number of neighbors with obstructed and unobstructed line of sight.	76
Figure 26	Average number of vehicles as obstacles in the line of sight.	78
Figure 27	Average received signal strength for the obstructed and unobstructed line of sight.	79
Figure 28	Radius of smart neighborhood with increasing node density.	80
Figure 29	Average success percentage with increasing node density.	82
Figure 30	Average success percentage with increasing distance from the transmitter.	83
Figure 31	Mean one-hop delay with increasing node density.	84

SUMMARY

Vehicular ad hoc network (VANET) is a collection of vehicles equipped with wireless communication capability, spontaneously forming a network while moving on the road. This research work focuses on the key networking problem of safety-message routing in the vehicular multi-hop scenario. Four novel techniques are presented that ensure the efficient and reliable routing of safety messages in the vehicular ad hoc network (VANET).

Two techniques, namely, the instant broadcast and the lane-based sectoring, are presented to improve the end-to-end message propagation delay and ensure collision avoidance, respectively. With the instant broadcast technique, the safety message is propagated without the use of an handshake mechanism and the related control packets. In case of collision in the forwarding step, instead of using the broadcast start over, the technique chooses the next contending forwarder node to rebroadcast the safety message, thus saving the overhead time incurred by a complex collision resolution. The lane-based sectoring technique, on the other hand, unveils the significance of road width in VANET communication and proposes the sectoring of the transmission range both lengthwise and widthwise to uniquely allocate time slots and alleviate collisions. To address the core issue of ensuring maximum reliability of the message dissemination, a collision-detection and a recovery mechanism called negative acknowledgment with smart neighborhood (NSN) is presented. The reception of the message is ensured by the NSN technique through the use of negative acknowledgement (NACK) mechanism in a confined range called the smart neighborhood. Finally, to ensure the reception of the safety message at vehicles located in the coverage holes, the negative acknowledgment with smart neighborhood - hole recovery (NSN-H) technique is presented that employs a constant observation and recovery of the smart neighborhood by each safety-message receiver.

CHAPTER 1

INTRODUCTION

A vehicular ad hoc network (VANET) provide vehicle-to-vehicle and vehicle-to-infrastructure communication using Dedicated Short-Range Communications (DSRC). The core objective of VANETs is to provide safety message communication among vehicles. Vehicular ad hoc network (VANET) is a collection of vehicles equipped with wireless communication capability, spontaneously forming a network while moving on the road. Vehicles cooperate to deliver safety-related information through multi-hop paths without the need for central administration. The dissemination of safety-related information among vehicles on the road helps drivers to anticipate hazardous events and maneuver accordingly to avoid potential dangerous events. With timely and reliable wireless communication between vehicles, VANET is aimed at providing passenger safety by exchanging real-time traffic-hazard messages among vehicles. In addition to safety-related services, VANET can also offer infotainment services by providing high-speed Internet connectivity onboard the vehicle.

The distinctive VANET topology and its dynamic wireless-signal environment pose a serious challenge in VANET communication. Vehicle movements are bound by street maps, traffic signals and regulations, and the movement of surrounding vehicles. Consequently, the distribution of vehicles is highly non-uniform, and the connectivity among them is highly random. Furthermore, the inevitable use of common control channel for safety applications makes communication highly vulnerable to collisions and interference from both visible and hidden nodes. The unique VANET characteristics cause challenging research concerns in information propagation and routing.

1.1 Overview of Vehicular Ad Hoc Networks

With the exponential increase of vehicles on the road, driving has become increasingly difficult and risky. Ensuring road safety in challenging road scenarios has become a subject

of intense interest and research. One possible way of providing road safety is by notifying hazard events and accidents using safety applications that communicate through wireless networks. Also, with the growth of the number of vehicles on road, the demand for in-vehicle entertainment is increasing. With the recent advancements in computing and wireless communication technologies, networks that can form the basis for such applications can be realized. The networks will offer complete mobility, require minimum or no central coordination, and support the applications in a dynamic and multi-hop topology. Such mobile ad hoc networks (MANETs) have several characteristics [1], including mobile and dynamic topologies, scarce bandwidth, limited energy, and so on. Since MANETs are autonomous mobile networks, the mobile nodes can be located on airplanes, ships, trains, trucks, or cars. Thus, vehicle ad hoc networks (VANETs) are a special kind of mobile ad hoc networks. In VANETs, network can be formed on the road between vehicles with vehicle-to-vehicle (V2V) communication or between vehicles and an infrastructure with vehicle-to-infrastructure (V2I) communication.

VANETs can provide the means for ensuring road safety as acknowledged in numerous projects working toward this goal [2, 3, 4, 5]. In addition, VANETs can be utilized for a wide range of both safety and non-safety applications, such as automated toll payment, intelligent traffic management, enhanced navigation services, location-based services e.g., finding the nearest fuel station, restaurant or travel lodge [6] and infotainment such as providing in-car Internet access.

1.1.1 VANET Characteristics

Apart from sharing general MANET properties, such as short radio-transmission range, self-organization, self-management, and limited bandwidth, VANETs can be distinguished from other kinds of MANETs by its unique characteristics. The unique characteristics of VANETs offer opportunities to increase network performance, and at the same time they pose considerable challenges. Some of the distinguishing VANET characteristics include

highly dynamic but predictable node mobility, frequent network fragmentation, small effective network diameter, and unique security and privacy challenges.

As a result of high speed of vehicles, the connectivity among vehicles lasts for a very brief amount of time. One solution to increase the duration of a link is to increase the transmission power. However, increase in vehicle's transmission range resulting from higher transmission power decreases the overall network throughput. When vehicles are traveling in opposite directions, their link is maintained for a very small period of time. Also, even in the case when vehicles travel in the same direction, with each vehicle having a transmission range of 300 meters, the communication link between vehicles exists on the average for about a minute only [7]. Because of the high degree of vehicle mobility, conventional MANET protocols that rely on node clusters are difficult to implement for a VANET. Nonetheless, the topology of a VANET is also beneficial in the sense that mobility of vehicles is predictable because vehicle movement is constrained by road geometry. The predictability of the position of a vehicle allows an improvement in link selection, albeit the linear topology of VANETs reduces the possible path redundancy.

Another reason for intermittent connectivity in VANETs is that the initial implementation of VANETs will have only a small proportion of vehicles on the road equipped with VANET transceivers. The small number of vehicles with transceivers will cause frequent fragmentation of the network, resulting in a portion of the network becoming unreachable. Even in the case of full penetration of VANET, fragmentation may exist in light traffic such as late night period or traffic in rural areas. Therefore, VANET protocols can not afford to assume that all vehicles on the road can communicate.

An equally crucial issue in VANETs is that of privacy and security. It is highly critical that the anonymity of vehicle and security of the message be preserved in order to gain support for the adoption of VANETs. Different types of attacks against VANET communication include bogus information, cheating with positioning information, identity disclosure,

denial of service, and masquerade. If strong security measures are not incorporated an attacker would be able to inject false data into the network causing the flow of traffic being altered and chaos within the transportation system. For instance, a malicious safety-message reporter may impersonate other vehicles or road-side infrastructure to trigger safety hazards. Consequently, the tampering of safety messages would trigger automobile accidents, which the system was designed to prevent.

1.1.2 Standards for VANET Communications

Several standards exist that relate to wireless communications in vehicular environment. These standards range from specifications that apply to transceiver equipment and communication protocols through to security specification, routing, addressing services, and interoperability specifications.

Dedicated Short Range Communications (DSRC) is a standard that aims to define vehicle-to-vehicle and vehicle-to-roadside communications in North America. Traffic fatalities have been a serious long standing concern in the United States, as in the rest of the world. As an indication of the seriousness of the problem, in the year 1999 about 279,000 motor vehicle accidents were reported that accounted for 41,611 deaths in the United States [8]. In 1991, the US Congress passed the Inter-modal Surface Transportation Efficiency Act that led to the creation of the first generation of Intelligent Transportation System (ITS). In October 1999, the Federal Communication Commission (FCC) allocated 75 MHz of bandwidth in the 5.9 GHz band for DSRC. The aim of ITS program and DSRC is to incorporate technology into the transportation infrastructure to improve passenger safety. DSRC is aimed at providing high data transfers and low communication latency in short range communication zones. Such communications cover a wide range of applications, like vehicle-to-vehicle safety messages, traffic information, toll collection, drive-through payment, and so on.

In 2003, the American Society for Testing and Materials (ASTM) approved the ASTM-DSRC standard that was mostly based on the existing IEEE 802.11a physical layer and

802.11 MAC layer [9]. In 2004, the report issued by the FCC specified service and licensing rules that define the use of the DSRC band. DSRC is a free but licensed band. It is free in the sense that FCC does not charge for the use of the band, but it is licensed meaning that it is restricted in terms of its use [10]. For example, the FCC specifies the use of certain channels and that all radios developed should conform to the standard. The DSRC spectrum comprises seven channels with each 10 MHz wide. One channel is designated for safety communications only while two other channels are designated for special purposes (such as critical safety of life and high power public safety). The remaining channels are free in terms of use and can be used for either safety or non-safety applications [11].

In contrast to the regional standard of DSRC, by incorporating DSRC into 802.11, IEEE 1609—standards for wireless access in vehicular environments (WAVE) (IEEE 802.11p)—is aimed to become a standard that can be universally adopted across the world. IEEE 802.11p is limited by the scope of IEEE 802.11 that strictly works at the media access control and physical layers [12]. The operational functions and application layer specifications related to DSRC are handled by the upper layers of the IEEE 1609 standards. These standards define how VANET applications that utilize WAVE will function in the WAVE environment based on the management functions defined in IEEE P1609.1, the security mechanisms defined in IEEE P1609.2, and the network-layer protocol defined in IEEE P1609.3. The IEEE 1609.4 resides above 802.11p and supports the functioning of higher layers without the need to deal with the physical channel parameters [6].

1.2 Routing in Vehicular Ad Hoc Networks

The core design goal of VANETs is to reliably and efficiently disseminate safety messages to all the related (endangered) vehicles on the road. The intended propagation region could be the immediate transmission range of about 300 meters or the long multi-hop forwarding range spanning more than a kilometer distance depending on the type of safety application.

Highly dynamic VANET topology and wireless signal environment make message propagation and routing a constant challenge. The distribution of vehicles is highly non-uniform, and the connectivity among them is highly random. Furthermore, the inevitable use of the common control channel for safety applications makes message propagation immensely vulnerable to collisions and interference. In the following, some of the challenges faced in VANET safety-message propagation are briefly outlined.

Several safety messages need to be propagated to vehicles beyond the immediate transmission range, e.g., safety alert messages about hazardous driving situations such as dangerous road surface, unexpected road block, accidents, and unexpected fog banks. The propagation of a message beyond the immediate transmission range involves multi-hopping in the highly dynamic network. Consequently, the propagation scenario becomes much more complex since multi-hop increases the chances of collision and also causes the over consumption of radio resource resulting from unnecessary retransmissions. The propagation requires multi-hop forwarding of the message by selected vehicles among a large number of contenders. The problem becomes severe in dense urban traffic where a higher number of contending vehicles results in excessive packet collisions. Since these collisions greatly impact the reliability of reception and the overall message-dissemination speed, it remains the core concern while developing ideas for message routing in VANETs [13].

The lack of feedback mechanism resulting from the broadcast communication scenario is another serious problem in VANET message propagation. The propagation path, either single-hop or multi-hop, involves a number of factors that obstruct some vehicles along the way from receiving the safety-alert message. As a result, the obstructed vehicles either receive the message not intact or are completely oblivious of the activity in the channel. Furthermore, since safety-message dissemination is carried using broadcasting, there is no feedback mechanism to recover the impeded vehicles, thus always compromising reliability.

The collisions and interference resulting from contending and hidden nodes are a major cause of corrupted messages, while oblivious nodes are caused by obstructions in the propagation path. Since failed reception at a given receiver is difficult to detect by the original sender, implementation of any retransmission mechanism in VANETs becomes tedious. A failed unicast transmission is usually detected by the lack of acknowledgment (ACK) packet from the receiver. However, as a result of the broadcasting nature of safety messages in VANETs, it is not practical to receive an ACK from each node for a message transmission. If acknowledgments are used, a problem known as the ACK explosion (or ACK storm) [14] is triggered. Each receiving node would almost at the same time instant send an ACK back to the transmitting node in the same control channel, causing a large number of collisions. Similarly, lack of recovery in message broadcast also precludes contention window (CW) size adjustment for collisions. With a feedback mechanism, the contention window is exponentially increased each time a failed transmission is detected to control congestion. Since there is no detection of failed broadcast transmissions for the sender, unlike unicast traffic the size of the CW fails to change for broadcast traffic. Consequently, excessive collisions are caused, if a large number of nodes are contending for channel access.

Another critical issue in VANET message propagation is the so called hidden-terminal problem. The stretched distribution of nodes in VANETs is highly vulnerable to cause the problem. As the distance from the sender increases, the collision rate, primarily caused by hidden terminal increases. Under saturated conditions, the probability of successful reception of a broadcast message sharply decreases at distance greater than 66% of the transmission range [15]. Also, resulting from the lack of RTS/CTS exchange in broadcasting, the hidden-terminal problem in VANETs becomes an open challenge to solve. The hidden-terminal (or hidden-node) problem [16] is the main cause of collisions in wireless networks. The IEEE 802.11 protocols use RTS/CTS handshake followed by an ACK to guarantee the delivery of a unicast packet. Broadcast communication, on the other hand,

cannot use the RTS/CTS handshake as it would flood the network with traffic. One solution to increase the probability of successful reception is to implement a redundant broadcast where a message is broadcast multiple times. The main drawback of redundant broadcast is that it results in generating excessive traffic in the network.

Coverage holes in the transmission range is an equally critical problem in VANET message propagation. The connectivity of vehicles is affected by obstructions either static (e.g., buildings, vegetation, hills) or mobile (other vehicles on the road). The relative low height of antennas onboard the vehicles implies that the optical line of sight (LOS) can be obstructed by the obstructions, in particular by mobile obstructions, causing transmission holes even within the single-hop transmission range. Most of the studies identify static obstacles as the only source of obstruction in the propagation path [17, 18]. However, since a significant portion of inter-vehicular communication is bound to the road surface, it is imperative to consider other vehicles as obstacles in the LOS between two communicating nodes. The experiments in [19, 20] report that a single vehicle as obstacle in the LOS can cause a drop of as much as 20 dB in the received signal strength. As a result, it is highly likely that in traffic with large public transportation and commercial vehicles such as buses and trucks, a number of coverage holes can be present in the transmission range causing several vehicles completely unaware of the ongoing safety-message transmission. The complete obliviousness of a vehicle located in a transmission hole makes reliability a serious challenge in the broadcast propagation scenario.

A consequence of having intermittent connectivity in a VANET is that it becomes unrealistic for a node to maintain the complete global topology of the network. The poor connectivity among nodes makes it infeasible to apply existing routing algorithms to VANETs. Traditional network routing algorithms are either proactive or reactive. In proactive routing algorithms each node maintains routes by using tables. Frequent exchanges of route information are needed between nodes to keep the routing table valid. Because the topology in VANETs changes so rapidly, the routes maintained in the routing tables rapidly become

invalid. Traditional table-based routing techniques, such as Destination Sequenced Distance Vector (DSDV), consume a great deal of bandwidth. Another problem with proactive routing approach is that it does not scale well in a VANET because of the intermittent connectivity among nodes. Reactive routing, on the other hand, aims at establishing a route only when it is needed. The problem with reactive technique is that the route must be discovered before the first packet is sent, which incurs extra time to send a message. Neither of these two approaches performs noticeably well in VANETs. In reactive approach, even in case a route to destination is found just before transmitting the message, the route will be very short lived because of peculiar node mobility. In addition, the expected route life decreases as the number of hops increases. A route may cease to exist almost as rapidly as it was discovered. Propagating a message to a distance greater than three or four hops using traditional ad hoc routing algorithm has high likelihood of resulting in a routing error [21]. Traditional concept of routing is not likely to play as large a role in VANETs as it does in other networks. Contrary to traditional ad hoc networks, in a VANET, routing typically concerns guaranteed transmission of a message in one hop, typically employing broadcasting and in multiple hops using broadcasting with multi-hop relay.

The above mentioned issues provide only a quick overview of the impediments in VANET safety-message communication. Considerable work has been carried, particularly in the last one decade, to address message propagation problems in VANETs. However, despite the years long efforts, some core issues remain open in VANET safety-message dissemination that include guaranteed message delivery, contention resolution in rush hour traffic and minimum end-to-end delay. The proposed research attempts to address these three key open problems in VANET safety-message propagation.

1.3 Related Work

Considerable amount of research work has been carried towards the design of broadcasting protocols for VANETs. Earlier works mainly considered the use of mobile ad hoc network

(MANET) techniques in the VANET context (for example [22, 23, 24]). However, later the trend shifted towards the design of VANET scenario specific routing algorithms that account for the peculiar vehicular mobility and its related network topology.

One of the ground breaking works in this regard has been the work of Korkmaz et al. [25], where the authors propose urban multi-hop broadcast (UMB) model that considers both reliability and message propagation delay. The UMB model uses the 802.11 inspired RTS/CTS exchange like mechanism to mitigate both hidden-node problem and confirm the next hop rebroadcast. Unlike 802.11, here the safety-message initiator exchanges RTB/CTB with only one of the recipients among its neighbors. However, it should be noticed that as a result of the small size of VANET safety message (payload length of 100 bytes on average [18]), each safety-message transmission occupies the radio channel for a very brief amount of time as opposed to a data stream. Consequently, in case of message transmission without RTB/CTB handshake, the likelihood of message collision resulting from hidden node is virtually equal to that with the use of RTB/CTB exchange. Also importantly, since vehicular topology has mostly extended distribution of vehicles and multi-hop transmission, the so called gagged-terminal problem and masked-terminal problem are also acute in VANET scenario. Moreover, the extended distribution of vehicles also has frequent instances of hidden terminals outside the transmission range of receivers i.e., the CTB message from receivers is unheard by those hidden terminals, thus causing handshaking ineffective. Likewise, reliance solely on the next rebroadcaster to confirm the reception on behalf of all the endangered nodes does not guarantee high reliability.

One common approach used to provide multi-hop forwarding is to divide the transmission range of message originating vehicle into multiple geographical sectors based on distance [25, 26, 27]. Vehicles in each sector pick a random back-off value from a contention window assigned to that sector. Contention windows are assigned in such a way that vehicles in the furthest sector can transmit first. Forwarding task is assigned to vehicle with minimum back-off. Since contention within a sector is random, it is highly probable in

dense traffic environments that two vehicles within the same sector pick the same back-off value, thus causing collision. Further narrowing the sector length may minimize the effect to a certain degree. However, even with minimum possible sector length—equal to the length of a car and necessary safety following distance—many potential time slot collision nodes are still present in adjacent lanes.

Redundant transmission has remained a common technique of ensuring message delivery to all vehicles by rebroadcasting the same message multiple times. The primitive technique in this regard has been the conventional flooding method where every receiving vehicle rebroadcasts the same message to ensure maximum reception. However, since the technique adversely effects the wireless channel utilization due the so called broadcast storm problem, it remains infeasible in the VANET environment. In [28], Thriveni et al. propose to limit the number of rebroadcasters to alleviate the effect on channel occupation; however, the technique is MANET specific and does not consider the effect of high node mobility. Wisitpongphan et al. in [29] propose a number of techniques to use redundant broadcast and mitigate the broadcast storm problem. Their propositions use a combination of weighted and slotted probability persistence to optimize the number of rebroadcasters and at the same employ redundant broadcast. The technique is successful in minimizing the number of rebroadcasters, however, the higher message transfer reliability still remains dependent on larger number of rebroadcasters.

In [30], the authors introduced a probabilistic rebroadcasting (forwarding) scheme called probabilistic inter-vehicle geocast (p-IVG) that relies on the density of the surrounding traffic. In p-IVG, the vehicle waits for a certain time depending only on the inter-vehicle distance between the sender and the receiver and chooses a random number between $[0,1]$. If the number is less than the reciprocal of the traffic density, the vehicle rebroadcasts the message when its timer expires; otherwise, it will drop the message.

While investigating the reliability of message broadcast, the phenomenon of transmission holes in the broadcast range has been recently considered as a potential cause of message loss in VANETs. In [19, 20], Boban and Tonguz et al. conduct extensive experiments to prove the presence of reception holes in the transmission range. The authors report mobile obstacles (i.e., vehicles), primarily in the LOS, as a major cause of loss in the signal strength, resulting in some portions of the broadcast region being completely uncovered. The studies show that a single obstacle can cause an RSS drop of over 20 dB when two cars communicate at a distance of 10 m; while in NLOS conditions the chances of a successful communication become 90%.

The coverage of transmission *holes* has thus far been dealt in [31, 32]. In [31], Laouiti et al. present the reliable opportunistic broadcast in VANETs (R-OB-VAN) algorithm to ensure the reliable transfer of safety messages. The authors present three variants of their algorithm with the third variant being claimed as the most reliable method. The authors designate each node in the broadcast range to be responsible for all other nodes (neighbors) in the broadcast range to ensure the reliability of reception. Nodes exchange the entire list of their neighbors by appending this information to the periodic beacon messages. Each node after receiving the safety message runs a process of reliability check for all other nodes in the broadcast range. The reliability check determines if there is any node in the range that does not have the message sender in its neighbor list. In case there exists such a node, it is inferred to be located in a hole, and subsequently the message is rebroadcasted for that node. The algorithm creates additional overhead for the existing periodic beaconing messages that use that same control channel primarily intended for safety messages, thus affecting channel contention. Channel contention is also caused as a result of the fact that the algorithm includes all the one-hop neighbors as potential rescuers that can cause excessive contention among the rescuers themselves.

In [32], Ros et al. propose acknowledge broadcast from static to highly mobile (ABSM) protocol that uses the concept of connected dominating set (CDS) to limit the number of

rescuers. If $G(V, E)$ is the graph representing the network topology, where V is the set of nodes in the network and E is the connectivity between them. Then, $V_D \subseteq V$ is said to be dominating if each node in V either belongs to V_D or has at least one neighbor present in V_D . The set V_D is CDS if it is connected. Thus, only nodes within CDS are eligible to retransmit. Each node independently decides whether or not to rebroadcast a received message solely based on the information acquired by vehicles from their neighborhood by means of periodic beacon messages. Each beacon message contains a message identifier of the recently received broadcast message that serves as acknowledgment. In this way each node checks whether all its neighbors successfully received the message. The use of acknowledgment makes the protocol robust in terms of reliability, however, as the authors mention, if the protocol has to wait for the beaconing cycle of each node (i.e., a wait period of at least 100 ms as per 802.11p beaconing frequency requirements), the recovery phase is too slow to be feasible for safety alert applications. Hence, the protocol, as suggested by the authors, is practical for use only in non-safety applications.

CHAPTER 2

DELAY IMPROVEMENT

Building upon the detailed motivation given in Chapter 2, a novel delay-improvement technique called the instant-broadcast is presented in this chapter. The proposed delay-improvement technique is part of the overall design towards an efficient routing technique for the dissemination of safety messages in a vehicular ad hoc network (VANET). As described in Chapter 1, the two critical design aspects of a VANET communication scenario are the efficiency of the message propagation and the reliability of the message reception. The message-propagation efficiency is ensured by improving the broadcast delay and minimizing the node contention. In what follows in this chapter, the instant-broadcast technique is presented that effectively minimizes the end-to-end delay of the safety-message routing in a VANET.

2.1 Prelude

Most of the broadcast methods in a VANET adopt the conventional method of using the request-to-send/clear-to-send (RTS/CTS) handshake before transmitting the actual safety message. The prominent works that use the handshake technique include the urban multi-hop broadcast (UMB) [25] and the smart broadcast (SB) [26]. In the VANET communication, the request-to-broadcast/clear-to-broadcast (RTB/CTB) handshake is used to mitigate the hidden-node problem. The safety-message initiator in a VANET exchanges the RTB/CTB packets with only one of the recipient nodes in the neighborhood. However, unlike the long packet size in a conventional network, the packet size of the safety message in a VANET is very small (payload length of 100 bytes on average [33]). Therefore, each safety-message transmission occupies the radio channel for a brief amount of time as opposed to the long occupancy time of the data stream in a conventional network. As a result of the similar packet size of the handshake packet and the safety-message packet, both the handshake-based broadcast and the instant broadcast have an equal likelihood of

a hidden-node collision. Also importantly, since the vehicular topology has an extended distribution of vehicles with multi-hop transmission, the gagged-terminal problem and the masked-terminal problem are acute in a VANET scenario. The extended distribution of vehicles also has frequent instances of the hidden terminals being located outside the transmission range of the receivers. The CTB message from the receivers is unheard by the hidden terminals, thus causing a concurrent transmission.

While improving the delay in the multi-hop scenario, an additional delay is incurred as a result of the long recovery time after the first forwarding attempt fails. The existing technique of restarting the broadcast incurs an overhead delay of one broadcast cycle. The overhead delay can severely degrade the effective end-to-end delay of the safety message.

In the following sections, the efficiency of the safety-message dissemination using the handshake-based broadcast in a VANET is evaluated. The instant-broadcast technique is proposed to improve the overall delay. In the instant-broadcast technique, the safety message is propagated without using the handshake mechanism and related control packets. In case of a collision in the forwarding step, instead of restarting the broadcast, it is proposed that the next contending forwarder rebroadcasts the safety message, thus saving the overhead time of a complex collision-resolution mechanism. An analytical model based on the Markov-chain modeling is also developed for the message-propagation delay in the instant broadcast. Thorough evaluation and comparisons are performed in the ns-3 simulator, and it is demonstrated that a short propagation delay can be guaranteed by using the proposed instant-broadcast technique.

2.2 Instant Broadcast

The sender (message originator) gains access to the medium by following the carrier-sense multiple access with collision avoidance (CSMA/CA) protocol and broadcasts the entire safety message. The collision at the message origination is resolved by following the

exponential-backoff mechanism. The location information, direction of broadcast, and sectoring information are appended to the safety-message packet as an overhead of 12 bytes. The packet overhead is not specific to the instant-broadcast protocol and is used in all the existing routing protocols. The location information comprises four bytes for the longitude and latitude of the sender (acquired from the onboard GPS device), the hop count and the intended broadcast distance comprise two bytes, the direction of broadcast comprises two bits, while the sectoring information comprises one byte each for the sector width (in meters) and the number of sectors. After receiving the safety message, the nodes will follow the sectoring-based contention procedure [25, 26, 27]; and the relay node will rebroadcast the safety message. In case of a collision, the vehicle with the next minimum-backoff value will rebroadcast the message. The rebroadcast from the relay node is overheard by the sender, which will confirm the successful reception of the safety message. In case when the rebroadcast message is not heard by the sender within the specified time (timeout), the broadcast is repeated by the sender. The movement of a vehicle (50 miles per hour on average) is negligible when compared with the propagation speed of a message (25 meters per millisecond on average according to simulations given later in this section). Therefore, the movement of vehicles is not assumed in the message-overhearing mechanism. In the last hop, the message is retransmitted twice, once by the actual forwarder, and the second time (after the first retransmission is received) by the furthest receiving node from the sender for the purpose of acknowledgement.

In Figure 1, the general sequences of packets are depicted for the handshake-based broadcast method and the instant-broadcast method. An intuitive comparison between the two methods is shown in terms of the packet delay. In the figure, the elimination slots account for the time when the nodes decide the next forwarder among themselves. It can be noticed in the figure that by the time the handshake method broadcasts the message in one hop, the instant broadcast completes two hops in a case where there is no collision. Interestingly, even while comparing a collision case of the instant broadcast with a successful

case of the handshake-based broadcast, the delay of the instant broadcast does not exceed the delay of the handshake-based broadcast. The delay gain in the instant broadcast shown in Figure 1 may seem improbable; however, it is observed that the delay gain of the instant broadcast is effectively twice as the handshake-based method under practical assumptions in the simulation analysis.

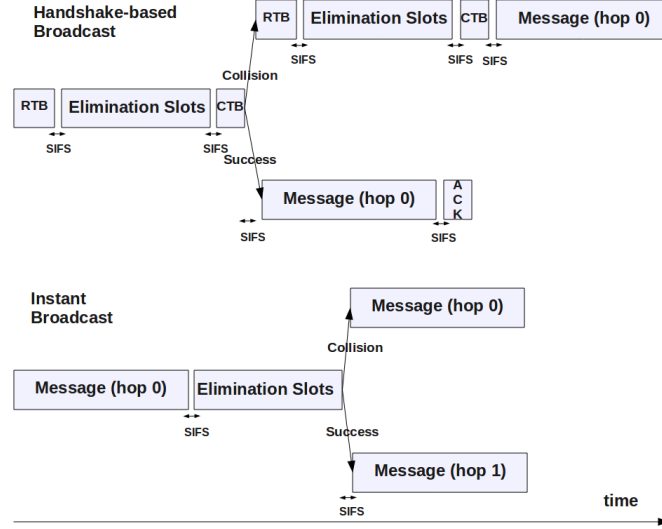


Figure 1: The sequence of packets in the handshake-based broadcast scheme and in the instant-broadcast scheme.

The UMB method, SB method and the proposed IB method use the concept of equally partitioning the coverage area into adjacent sectors around the sender node to decide the next relay node. Each receiving node in the broadcast range determines the sector location by estimating the distance between the receiving node and the sender node using the location information. Each sector is assigned a contention window containing an equal number of time slots:

$$W_n = \{t_1, t_2, t_3, \dots, t_l\} + (N - n), \quad n = 1, 2, \dots, N, \quad (1)$$

where W_n denotes the contention window for sector n . The number of time slots l is equal for all sectors, and its value depends on traffic congestion. The more congested the traffic,

the more the number of time slots. Each window is offset by $N - n$, where N is the total number of sectors, thus making sure that the nodes far from the sender always transmit before the nodes near to the sender. The optimization of the parameters N and l will be shown with the help of simulations in the following sections.

2.3 Multi-hop Delay Estimation

The delay analysis for the vehicular multi-hop scenario using the instant-broadcast method is formulated in this section. As explained in the previous section, the sending mechanism in the first hop (message origination) is different from the sending mechanism in the following hops. In the former case, the sender increases its backoff-window size in case of a collision until a successful transmission occurs; while in the latter case, the sender gives up in case of a collision, and the node with the next minimum-backoff value forwards the message. Therefore, the delay for the first hop is formulated separately from the delay of the following hops.

The analysis for the message-origination hop is presented first. In the following analysis, Bianchi's Markov chain is used with the assumption that the traffic distribution is uniform, and that there are a fixed number of contending nodes (CN) (excluding the sender) and a fixed number of hidden nodes (HN) for each sender. In Bianchi's Markov-chain model [34], the author defines p as the probability that a transmitted packet collides and causes the current window size to increase by a factor of two. The collision, as considered in [34], occurs when contending nodes choose a common time slot at the same time. However, in the given scenario, the collisions resulting from the hidden nodes are also considered. To incorporate the collision effect, a modified Markov-chain model is depicted in Figure 2. The stochastic processes $b(t)$ and $s(t)$ represent the backoff-time counter and the backoff stage, respectively, for a given node at time t .

At any given state $s(t)$, P' is the packet-collision probability. Let t_r be the transmission time of the packet given by

$$t_r = \frac{H_{PHY} + H_{MAC} + \text{Payload}}{R_b} + \delta, \quad (2)$$

where H_{PHY} and H_{MAC} are the PHY header and the MAC header, respectively. The data rate is R_b , while δ is the propagation time. The same data rate is assumed for the transmission of the payload, PHY header, and MAC header. The interval t_α is represented in terms of the number of backoff slots such that a hidden node does not transmit a packet during the interval t_r . The interval t_α is given by

$$t_\alpha = \left\lceil \frac{t_r}{\text{slot time}} \right\rceil. \quad (3)$$

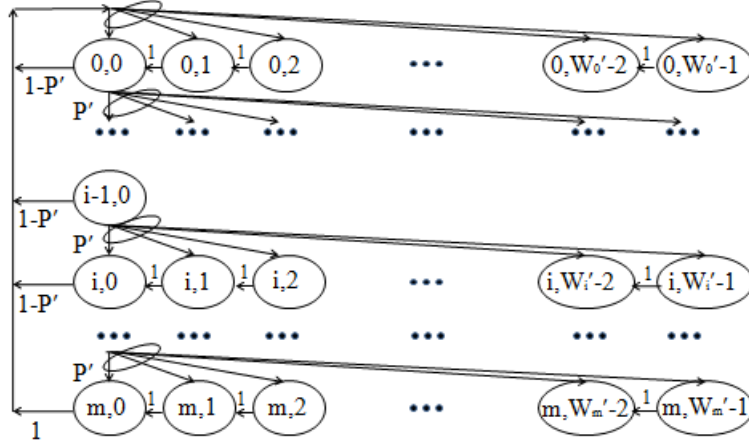


Figure 2: Markov-chain model with hidden-node collisions.

Let τ_c be the transmission probability of a contending node, and τ_h be the transmission probability of a hidden node. The probability that a hidden node does not transmit during the transmission of the sender is $(1 - \tau)^{t_\alpha \cdot HN}$. Consequently, by incorporating the collisions, the probability of an unsuccessful transmission becomes

$$P' = 1 - (1 - \tau_c)^{CN} (1 - \tau_h)^{t_\alpha \cdot HN}. \quad (4)$$

From [34], the probability that a node begins transmission in a given time slot is given by

$$\tau = \frac{2(1 - 2P')}{(1 - 2P')(W' + 1) + P'W'(1 - (2P')^m)} , \quad (5)$$

where W' is the minimum window size and m is the maximum backoff stage. Probabilities τ_c and τ_h can be computed from [34] and Equation 4 using numerical analysis.

The probability that a transmission occurs among contending nodes in a given time slot is given by

$$P_{tr} = 1 - (1 - \tau_c)^{CN+1} . \quad (6)$$

The probability that a packet is successfully transmitted, given P_{tr} (probability that a transmission occurs among the contenders), is given by

$$P_s = \frac{(CN + 1)\tau_c(1 - \tau_c)^{CN}(1 - \tau_h)^{t_a HN}}{P_{tr}} . \quad (7)$$

From [35] and the above equations, the average delay for the message transmission in the first hop (message-origination hop) $E[D]$ can be written as

$$E[D] = E[S]E[slot] , \quad (8)$$

where

$$E[S] = \frac{(1 - 2P')(W' + 1) + pW'(1 - (2P')^m)}{2(1 - 2P')(1 - P')} , \quad (9)$$

$$E[slot] = (1 - P_{tr})\sigma + P_{tr}P_sT_s + P_{tr}(1 - P_s)T_c . \quad (10)$$

$E[S]$ is the average number of time slots for a successful transmission, and $E[slot]$ is the average length of a time slot. The duration of an empty slot is σ , while T_s is the average time the medium is sensed busy because of a successful transmission, and T_c is the average time the medium is sensed busy because of a collision given by

$$T_s = DIFS + \left(\frac{H_{PHY} + H_{MAC} + Payload}{R_b} + E[D'] + \delta \right), \quad (11)$$

$$T_c = DIFS + \left(\frac{H_{PHY} + H_{MAC} + Payload}{R_b} + timeout + \delta \right). \quad (12)$$

As explained in the protocol description, in a given hop, the retransmission in the next hop is considered as an acknowledgment for the transmission in the previous hop. Therefore, in Equation 11, the average next-hop delay $E[D']$ is included as the acknowledgement delay in case of a successful transmission. For the collision event in Equation 12, the acknowledgment timeout of the message originator is included to account for the collision delay.

The analysis of the average delay $E[D']$ of the forwarding hop is as follows. It is assumed that the transmission probability τ_h of a hidden node is the same as considered in the first hop. It is also assumed from the sectoring method that the contention-window size l is fixed for each sector in the propagation scenario. Since the traffic distribution is assumed as uniform, the number of hidden nodes and the number of contending nodes are assumed as equal for each sector. The transmission is cancelled in case of a collision, and the node with the next minimum-backoff value retransmits the message. The probability of transmission in a given time slot is given by $\tau_{c'} = \frac{1}{l}$. Note that unlike in the first hop, the sender does not use exponential backoff in the following hops.

The probability that the packet is successfully transmitted can be computed by using Equation 7. The average delay $E[D']$ for the forwarding hop is finally written as

$$E[D'] = E[d]X, \quad (13)$$

where $E[d]$ is the average delay for a retransmission attempt. The average delay $E[d]$ can be computed by using Equations 8, 9, and 10 with $m = 1$. The variable X is the average number of retransmission attempts in the forwarding hop and is given by

$$X = \sum_{n=0}^{W-1} (1 - P_{s'} P_{tr})^n P_{s'} P_{tr} n . \quad (14)$$

Note that while calculating the forwarding-hop delay, the average next-hop delay is included to account for the acknowledgment in Equation 11. Therefore, the average next-hop delay is included in each forwarding hop until the retransmission in the last hop. In the last hop, as explained in the protocol description, there is a retransmission after the initial forwarding that specifically serves as an acknowledgment without requiring any further confirmation.

2.4 Simulation Analysis

2.4.1 Simulation Setup

To analyze the comparison of the handshake-based broadcast method and the instant-broadcast method, the IB scheme is fully implemented along with the UMB scheme [25] and the SB scheme [26] in the ns-3 simulator, Version 3.9 [36]. The traffic mobility is generated using the VanetMobiSim tool [37]. The common simulation parameters are summarized in Table 1.

The simulation uses a four-kilometers of road-length with unidirectional roads in two lanes. Ten different vehicle densities are tested with densities from five to 50 nodes per 300 meters length of the road (i.e., the one-hop distance). Vehicles are assigned Gaussian-random speed with a mean of 50 miles per hour and a standard deviation of three miles per hour. The minimum safe headway between the vehicles is kept as 1.5 seconds. Jake's model is used to estimate Rayleigh fading for the channel [21]. To best study the performance of algorithms in the existence of the hidden nodes, the scenario is tested for different message-generation rates of 0.01 to one message per vehicle per second, where one message per vehicle per second has a high likelihood of the hidden nodes at almost every broadcast instance.

Table 1: Simulation parameters for UMB, SB and IB schemes.

Description	Value
Transmission range	300 meters
Data rate	3 Mbps
Message payload size	100 Bytes
Protocol overhead	12 bytes
MAC header size	34 bytes
PHY header size	26 bytes
Base protocol	802.11p
RTB, CTB, ACK	20, 14, 12 bytes
Time slot, DIFS, SIFS	20, 50, 10 μs
Road length	4 km (2 lanes)
Vehicle density	5-50 vehicles/300 meters
Vehicle speed	50 miles/h (mean)
Message generation rate	0.01-1 message per vehicle/second
Path loss model	Log-distance model
Fading model	Rayleigh fading model
Simulation time	100 seconds (each run)

2.4.2 Results and Discussion

In Figure 3, an explicit comparison between the handshake-based method and the instant-broadcast method is given in the presence of a variable number of hidden nodes and contending nodes under saturation condition. The two-tuple legend represents the number of contending nodes and the number of hidden nodes, respectively. The average one-hop network throughput is reported against a variable packet-payload size from 100 to 500 bytes.

For the sake of clarity in the plot, the smart broadcast method (being the closer counterpart of the IB method) is depicted in detail, while for the UMB method, the average throughput curve is shown. Clearly, the IB method achieves higher throughput compared to the handshake-based broadcast for the small message size of 500 bytes and below. The throughput gain of the IB method for the message size below 500 bytes is almost constant regardless of the increase of the number of hidden nodes.

The throughput gain of the IB method is understandable for a number of reasons. First, the handshake-based method aims to exploit the small size of the RTB packet to reserve

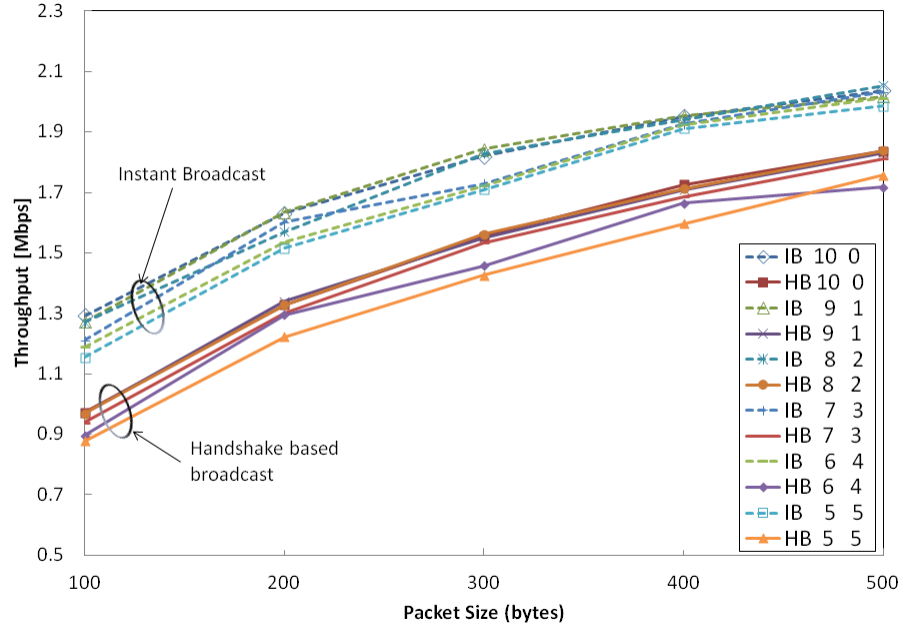


Figure 3: The average network throughput with variable packet sizes.

the channel prior to sending the actual message packet. However, for the small message size, the message itself has low likelihood of collision similar to the RTB packet; the handshake serves as an overhead, resulting in a low throughput. Second, the extended vehicle distribution (topology) on the road has a high likelihood of the gagged-station problem. In the gagged-station problem, the RTB/CTB exchange unnecessarily prevents simultaneous (non-interfering) communication among the neighbor nodes, thus effecting the overall network throughput. Third, the extended distribution of vehicles on the road causes the masked-station problem in the high packet-generation rates. The RTB/CTB becomes ineffective and incurs excessive delay. However, for the message size above 500 bytes, the handshake messages are adequately smaller than the actual message that reserve the channel for a safety-message transfer. Therefore, the handshake mechanism can be effective for the message size above 500 bytes.

In Figure 4, the average one-hop-propagation delay for a general safety-message broadcast is presented under a variable contention-window size l and a variable number of sectors

N . The plot is based on the mean delay with variable node densities. From the figure it can be observed that both l and N are influential on the propagation delay. The higher values of both the parameters avoid collisions, and the collision avoidance is achieved at the cost of an additional delay. On the contrary, too small values of the two parameters also incur excessive delay as a result of retransmissions caused by a large number of collisions. The parameter setting of $l = 7$ and $N \leq 8$ seems optimal for minimum propagation delay. Also, since the same sectoring approach is followed in all the three protocols under discussion, the same optimum values are considered for the remaining simulation experiments in this section, i.e., the window size $l = 7$; the number of sectors $N = 8$.

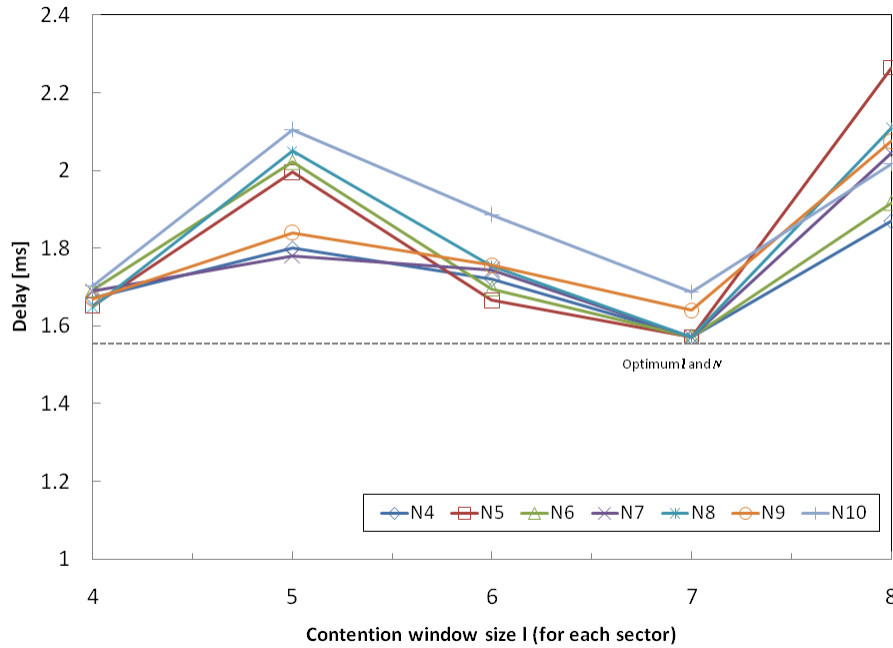


Figure 4: Average one-hop delay with variable settings of l and N .

The mean delay with respect to the distance between the sender and the receiver is depicted in Figure 5. A considerable delay gain is observed for the IB method over the handshake-based methods. Note that the distance interval (300 meters) on the x-axis roughly represents the one-hop-communication range. Therefore, it is observed that the delay gain of the IB method over the handshake-based protocols doubles every hop. In the

fourth hop, the delay gain of the IB method is about 12 milliseconds more than the delay of the handshake-based methods.

Among the two handshake-based methods, the SB method achieves lower end-to-end delay than the UMB method. The lower delay of the SB method is due to the lack of the overhead delay resulting from the collision-resolution mechanism. On the other hand, the UMB method provides higher reliability than the SB method. The UMB method achieves high reliability because of the feedback mechanism that uses the ACK message for each broadcast. In case of a timeout, the sender always rebroadcasts the safety message to ensure the reliability of reception.

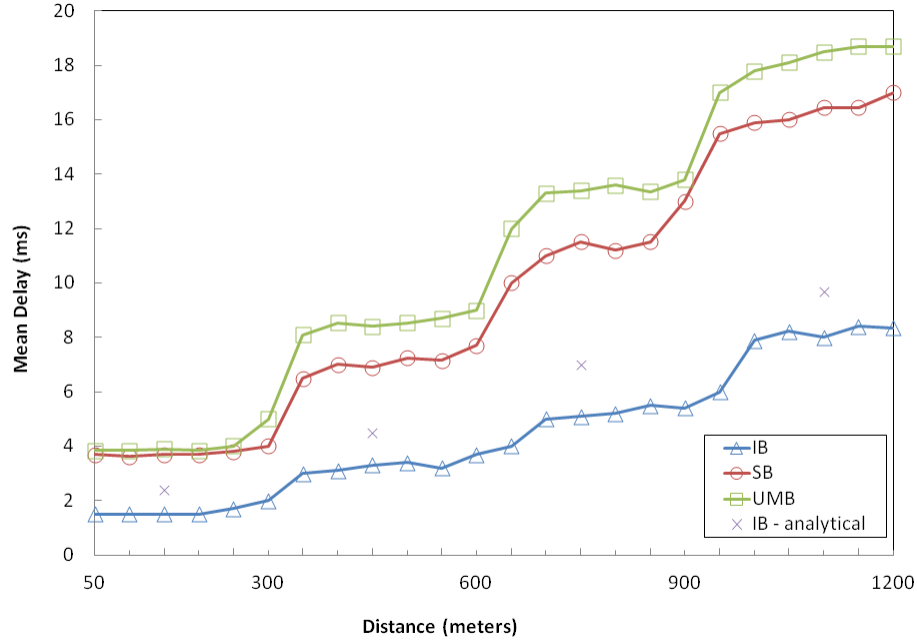


Figure 5: Mean delay with respect to distance.

In Figure 6, the mean one-hop delay is depicted against the variable message-generation rate. From the figure it is obvious that the instant-broadcast method provides a considerable improvement over the SB and UMB protocols in terms of the mean one-hop delay. The delay gain is consistent with message generation rate until slightly above 0.1 message per second per vehicle where the hidden-node problem becomes acute, resulting in the handshake

methods performing equally well. However, the retransmissions due to the hidden-node collisions in the higher message generation case do not significantly effect the IB performance as a result of the small size of the safety message. The delay of the IB method is close to the delay of the handshake-based methods in the high message-generation rates.

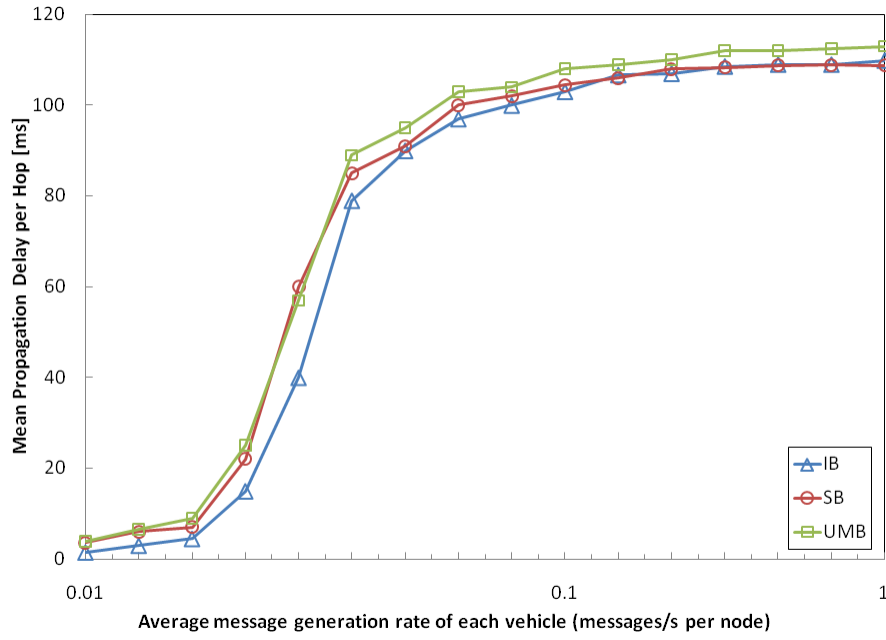


Figure 6: Mean delay with variable message-generation rate

Figure 7 depicts the average load generated by each message in the network against the vehicle density. The figure highlights an important achievement of the IB protocol over the handshake-based protocols. The curves represent the total number of bits transmitted in the network in order to disseminate a safety message to related nodes. In other words, we observe in the plot the channel reservation time per safety event for each protocol. The average load generated per message increases slightly with the increase in the vehicle density for all the three protocols. The load increase is a result of the retransmissions triggered by collisions in the high-density traffic. However, since the IB method involves only the actual message in the propagation mechanism, it generates the least amount of load per message in the network. On the contrary, the handshake-based methods involve the RTB

and CTB overhead packets. Moreover, the handshake-based methods trigger excessive re-transmissions resulting from the gagged-station problem and the masked-station problem. Consequently, the overall load generated per message is higher for the handshake-based broadcast methods.

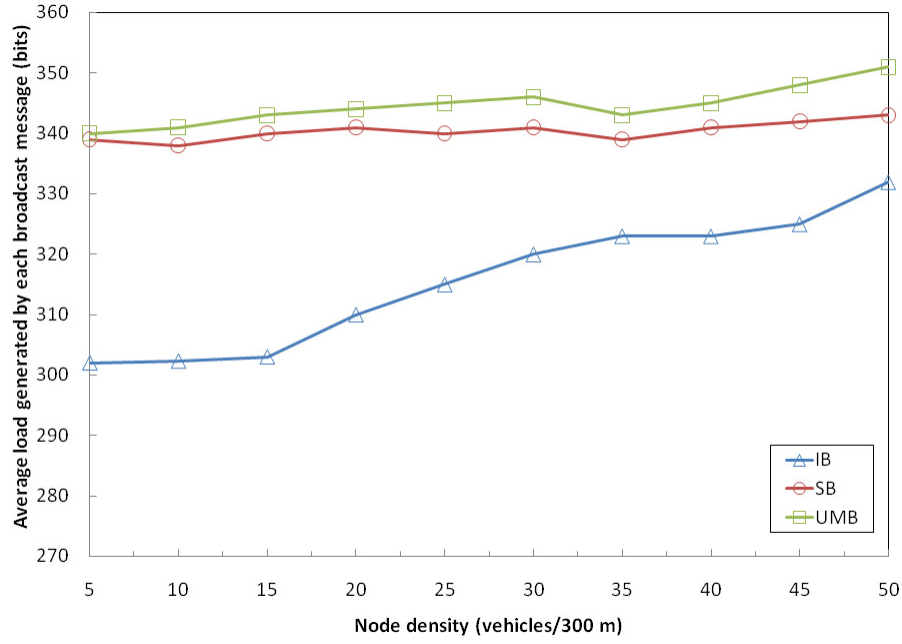


Figure 7: Average network load generation by each message.

The success rate of the three techniques is given in Figure 8. The success rate is the ratio of the number of nodes that receive the safety message to the total number of nodes that are present in the multi-hop-coverage range. The reception by any node is considered as the final successful reception of the message regardless of the number of retransmissions resulting from collisions. As presented earlier in this section, the existence of the hidden nodes is directly proportional to the packet-generation rate. It is observed that the IB method performs equally well as the handshake method with a negligible loss (about 0.2% more than the handshake method) in the high packet-generation rate. Thus, the IB method maintains equal reliability as the protocols with the handshake overheads, while at the same time provides low propagation delay.

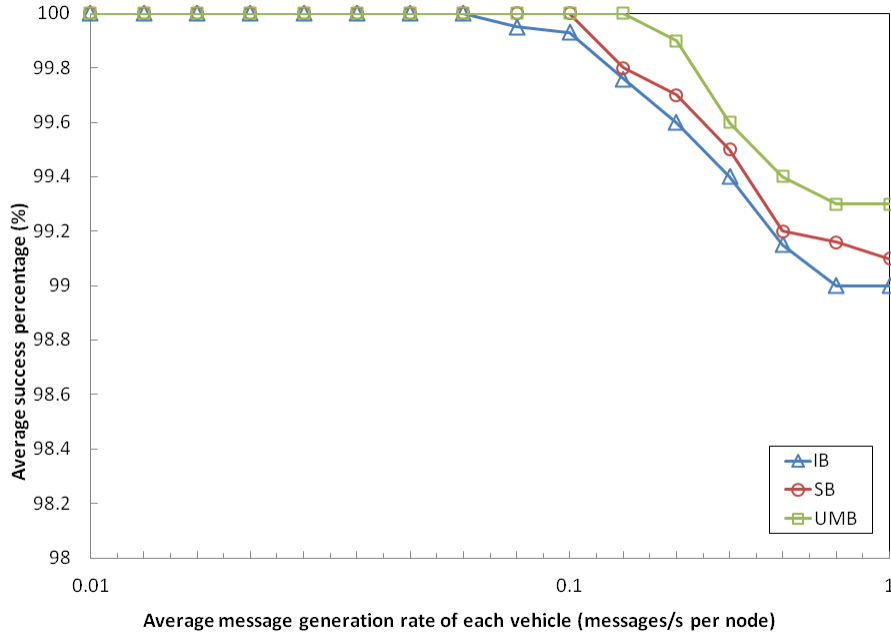


Figure 8: The average success percentage.

The evaluation results show that the instant-broadcast method improves the overall safety-message-propagation speed by avoiding the overhead messages and offers equal reliability as the handshake-based method. The evaluation of the handshake-based methods provides a detailed insight into the design of communication protocols for the VANET scenario.

In this chapter, the instant-broadcast technique is proposed that builds on the instant relay of the safety message without using the RTB/CTB handshake. The proposed technique exploits the small size of the actual safety message to avoid collisions and the hidden-node problem. The technique also minimizes the delay cost of collision recovery by allowing the next priority forwarder to rebroadcast instead of restarting the entire broadcast process. Extensive simulation analyses are performed using the ns-3 simulator. The simulation results suggest that the instant broadcast method significantly improves the message-propagation speed and ensures the reliability of reception by all the nodes in the multi-hop range.

CHAPTER 3

COLLISION MITIGATION

In this chapter, a novel transmission-range sectoring technique called the lane-based sectoring is presented as part of the design towards an efficient routing technique for the dissemination of safety messages in a vehicular ad hoc network (VANET). In dense urban traffic, the safety-message communication encounters severe packet collisions resulting from the excessive number of nodes that are contending to access the control channel. The proposed technique introduces the use of the lane-level location information to achieve a one-vehicle-per-time-slot configuration. The transmission range of a message originator is divided into a grid using the distance and lanes as the two variables. Each block within the grid houses a single vehicle that is assigned a unique time slot, and the contention among the nodes for the same time slot is virtually removed. In what follows in this chapter, a detailed description of the significance of road width in VANETs is presented, and the proposed lane-based sectoring technique is described in detail with theoretical and simulation analyses.

3.1 Vehicular Communication in Dense-Urban Traffic

Multi-hop forwarding of safety messages in dense urban traffic encounters severe packet collisions caused by the excessive number of nodes contending to access the control channel. In such a complex dense and mobile scenario, an ideal single vehicle per time slot has not been achieved thus far. One common approach used to provide multi-hop forwarding is to divide the transmission range of message originating vehicle into multiple geographical sectors based on distance [25, 26, 38]. Vehicles in each sector pick a random back-off value from a contention window assigned to that sector. Contention windows are assigned in such a way that vehicles in the furthest sector can transmit first. Forwarding task is assigned to vehicle with minimum back-off. Since contention within a sector is random, it is highly probable in dense traffic environments that two vehicles within the same sector pick the same back-off value, thus causing collision. Further narrowing the sector length

may minimize the effect to a certain degree. However, even with minimum possible sector length—equal to the length of a car and necessary safety following distance—many potential time slot collision nodes are still present in adjacent lanes. Considering the effect of lanes in VANETs forms the core of the proposed collision mitigation technique.

With road widths fast nearing 100 meters (more than ten lanes each direction) [39], it has become indispensable to consider the effect of road width (or more specifically the road lanes) while designing the message-propagation algorithms for VANETs. The proposed collision mitigation technique primarily considers dense urban traffic environment where traffic in each lane behaves like train trails with constant speeds. The proposed technique is suggested to be incorporated with methods for regular traffic using the currently probed vehicle density learning mechanism. This work introduces the significance of the worst-case rush-hour traffic, whereas the previous works only consider the normal urban traffic as the extreme case. The use of the prevailing Differential Geographic Positioning System (DGPS) is assumed to determine accurate vehicle location. The aforementioned transmission range of a message originator is finely dissected both lengthwise and widthwise using distance and lanes respectively, forming a grid like structure with each block containing a single vehicle at most. Unique backoff values are assigned to each block ensuring only one vehicle in the furthest range forwards the message. Long contention window as a result of fine dissection may suggest high transmission delay, however, in dense traffic there is always a forwarding vehicle present in the furthest range that transmits with minimal back-off (i.e., transmission in the beginning of the window), making the length of the window ineffectual on delay. Additionally, since the overhead delay of the message retransmission resulting from the forwarding collisions is reduced, the overall end-to-end message-propagation time is significantly minimized.

The proposed idea is studied using thorough simulations performed in the ns-3 network simulator [36]. Considerable reduction in the rebroadcast collisions is achieved by using the grid-based technique, and the total collision occurrence is contained to three percent

in the worst case, while the message forwarding delay for each hop is improved by nine milliseconds over the existing sectoring technique.

3.2 Road Width in Vehicular Communication

Road topology is one of the critical foundation elements considered while designing communication mechanisms for VANETs. Some of the important topology factors considered in hitherto VANET literature include vehicle density, vehicle speed, headway distance, road side clutter (for path loss calculation), while the road geometry is assumed either entirely linear or with the inclusion of intersections [26, 27, 21]. In [25, 33] road width is considered, however, their consideration is limited to its effect on vehicle density i.e., geographical separation of lanes is not considered and instead parallel vehicles in different lanes are assumed to be at the same location. Road width is also neglected in VANET mobility pattern generator tools [40, 41, 37], where multiple lanes only account for density while their geographical separation is still ignored.

The exponential increase of vehicles on the road has resulted in the ever increasing road widths to maintain smooth flow of traffic. Consequently, the average width of busy roads in a metropolis has become above six lanes each direction [8]. I-10 East downtown Houston is a compelling example of the significance of road width where the road is as wide as 13 lanes each direction [39]. In such scenarios vehicles in parallel lanes will exacerbate channel contention, and in addition, may effect physical path for radio propagation on the road. This work, however, thoroughly takes into account road width and attempts to exploit vehicles' lane level location information to avoid channel contention problem in multi-hop routing. The goal is to achieve zero collision (among visible nodes) in rush-hour traffic in dense-urban scenario.

3.3 Broadcast with Lane-based Sectoring

In the following, an extension to the instant broadcast technique is presented by introducing lane-based sectoring. Here, rush hour dense traffic scenario is assumed, however, later in simulations it is shown that the idea is also applicable in normal highway traffic where linear car spacing is 17 meters. Since the technique characteristically makes use of road lanes, the scenario is restricted to the usual urban road width of four or above lanes [8].

The sender node (message originator) gains access to the medium by following the 802.11 CSMA/CA policy and broadcasts the entire safety message (with average VANET safety-message size of 100 bytes [38]). The safety message is piggy backed with DGPS position of the sender, direction of broadcast and sectoring information for receiving nodes. Sectoring information, in turn, includes sectoring mode (i.e., linear or grid sectoring mode), and road width (at the sending instant). Sectoring mode is decided by considering current road density, which is learned from the periodic beacon messages of surrounding vehicles or by keeping track of the packet collision history where more collisions determine higher density and vice versa. Furthermore, the road width at the sender's location is considered to cater scenarios where different road widths exist within the multi-hop broadcast range e.g., road widening or narrowing within the multi-hop distance.

The piggy-backed information adds a minimal overhead of about 12 bytes. Similar length overheads are used in most broadcasting methods including UMB and SB protocols in [25, 26]. The location information comprises four bytes each for longitude and latitude of the sender (acquired from the onboard DGPS device), direction of broadcast is two bits, while sectoring information comprises two bits for sectoring mode, one byte for road width (in number of lanes), and one byte for sector length (in meters).

Receiving nodes will enter a contention phase to rebroadcast the safety message and node with the smallest back-off value among the contenders will rebroadcast the safety message to the next hop. Since the receiving node furthest from the sender can provide

longest relay, nodes in the furthest sector will have the least back-off values. In grid sectoring, in addition to lengthwise sectoring of the road based on the distance from the sending node, each sector is further subdivided widthwise into cells. Each sector is assigned a contention window with equal number of time slots (see Equation 1).

The sectoring mechanism and back-off value assignment in lane-based broadcast method is shown in Figure 9. Transmission range of the safety-message sender is divided into equal size sectors with increasing distance from the sender along the road in the message forwarding direction. Each sector is assigned a fixed length contention window W_n as described in Equation 1. Within each sector, the road section is further subdivided widthwise into cells with cell width equal to that of one lane. Each cell is then assigned a fixed time slot from the corresponding contention window. Length of a cell (along the horizontal axis in Figure 9) is significant in the proposed mechanism. One cell in the given scenario strictly holds one vehicle in order to completely avoid collision. Therefore, sector length (or cell length) is cautiously assumed as 13 meters, although [8] reports that the average vehicle spacing in a city freeway is about 16.8 meters (equal to four car lengths; average car length being four meters). Node within each cell backs off for its assigned amount of time. Consequently, in the given scenario the node in N^{th} sector (furthest) sector with time slot t_1 will rebroadcast first. All the remaining nodes with higher back-off values would overhear the rebroadcast and would subsequently quit their rebroadcast step.

The rebroadcast from the relay node is also overheard by the original sender, this overhearing of the message will confirm successful reception of the safety message. In the case where the rebroadcast message is not heard by the original sender within the specified time (timeout), the broadcast is repeated by the original sender. Note that the movement of a vehicle (50 miles per hour on average) relative to the message-propagation speed (25 meters per millisecond on average according to simulations given later in this section) is negligible to influence the message overhearing mechanism because of the immense difference in the relative speeds. The same mechanism is repeated in the remaining hops until the message

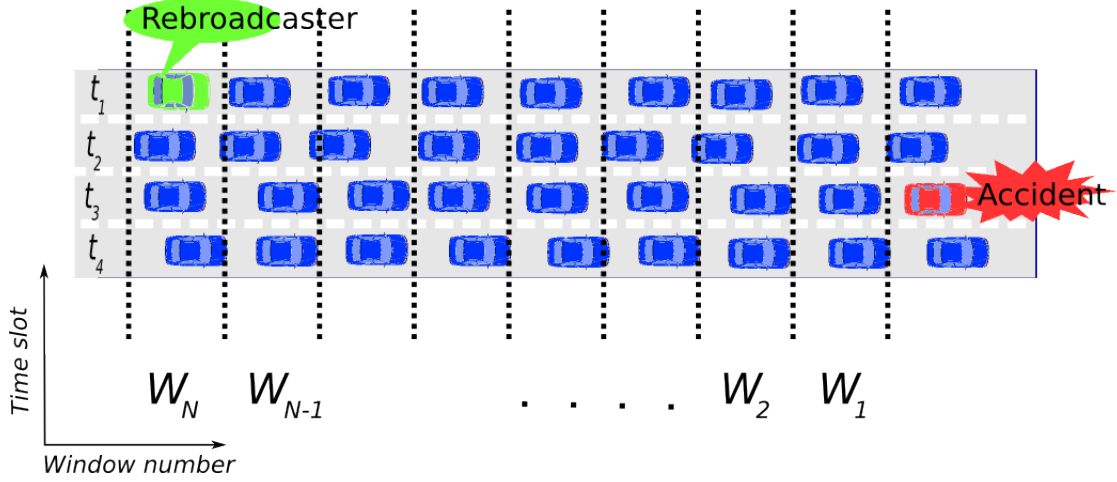


Figure 9: Back-off-value assignment using lane-based sectoring.

propagates across the intended distance.

3.4 Delay Analysis

Following the delay formulation in Section 2.3, let τ_c be the transmission probability of a contending node. The probability of unsuccessful transmission becomes

$$P' = 1 - (1 - \tau_c)^{CN}. \quad (15)$$

From [34], the probability that a node starts its transmission in a given time slot is given by

$$\tau = \frac{2(1 - 2P')}{(1 - 2P')(N + 1) + P'N(1 - (2P')^l)}, \quad (16)$$

where N and l are the number of sectors and the number of slots, respectively, from Equation 1. Probability τ_c can be analytically computed from [34] and Equation 16.

The probability that a transmission occurs among the contending nodes in a given time slot is

$$P_{tr} = 1 - (1 - \tau_c)^{CN+1}. \quad (17)$$

Probability that a packet is successfully transmitted, given P_{tr} , is

$$P_s = \frac{(CN + 1)\tau_c(1 - \tau_c)^{CN}}{P_{tr}}. \quad (18)$$

From [21] and the above equations, the average delay for message rebroadcast $E[D]$ can be written as

$$E[D] = E[x]E[t], \quad (19)$$

where

$$E[x] = \frac{(1 - 2P')(N + 1) + P'N(1 - (2P')^l)}{2(1 - 2P')(1 - P')}, \quad (20)$$

$$E[t] = (1 - P_{tr})\sigma + P_{tr}P_sT_s + P_{tr}(1 - P_s)T_c. \quad (21)$$

In the above equations, $E[x]$ is the average number of time slots for a successful transmission and $E[t]$ is the average length of a time slot; σ is the duration of empty slot, T_s and T_c is the average time the medium is sensed busy because of a successful transmission and the average time the medium is sensed busy because of a collision, respectively, given by

$$T_s = DIFS + t_r + \delta + ACK, \quad (22)$$

$$T_c = DIFS + t_r + timeout + \delta. \quad (23)$$

In case of lane-based sectoring method, the rebroadcast delay $E[D]$ is strictly dependent on the density of nodes. Rush hour traffic has the lowest rebroadcast delay as the smaller back-off value cells, like all other cells, are likely to be occupied, thus causing rebroadcast in the first few time slots of the contention window. Therefore, in rush hour traffic for lane-based sectoring method, as P_{tr} becomes equal to τ_c , and CN approaches zero, the probability of successful transmission P_s approaches near one.

3.5 Simulation Analysis

To analyze the comparison of the normal-sectoring broadcast and the lane-based sectoring broadcast, the general broadcast procedure followed by UMB, SB and IB in [25, 26] and [38] is fully implemented using both normal sectoring as well as lane-based sectoring in the ns-3 simulator, Version 3.9 [36]. The traffic mobility is generated using the tool VanetMobiSim [37]. Simulation parameters are summarized in Table 2.

Table 2: Simulation parameters for NB and LB.

Description	Value
Transmission range	300 meters
Data rate	3 Mbps
Message payload size	100, 300 and 1000 Bytes
Protocol overhead	14 bytes
MAC header size	34 bytes
PHY header size	26 bytes
Base protocol	802.11p
Time slot, DIFS, SIFS	20, 50, 10 μs
Road length	1 km
Vehicle density	2-30 vehicles/lane/300 meters
Vehicle speed	50 miles/h (mean)
Vehicle spacing	10 meters
Message generation rate	0.01-1 message per vehicle/second
Path loss model	Log-distance model
Fading model	Rayleigh fading model

A road length of one-km is considered with unidirectional traffic in four and eight lanes. About 15 different vehicle densities are tested with densities ranging from two to 30 nodes per lane per 300 meters length of the road (i.e., one-hop distance). Vehicles are assigned Gaussian-random speeds with a mean of 50 miles/h and a standard deviation of three miles per hour. The minimum headway between vehicles is kept as 10 meters to account for worst-case scenarios. Jake's model has been used to estimate Rayleigh fading for the channel [21]. To best study the performance of the proposed technique, the scenario is tested for different message generation rates of 0.01 to one message per vehicle per second.

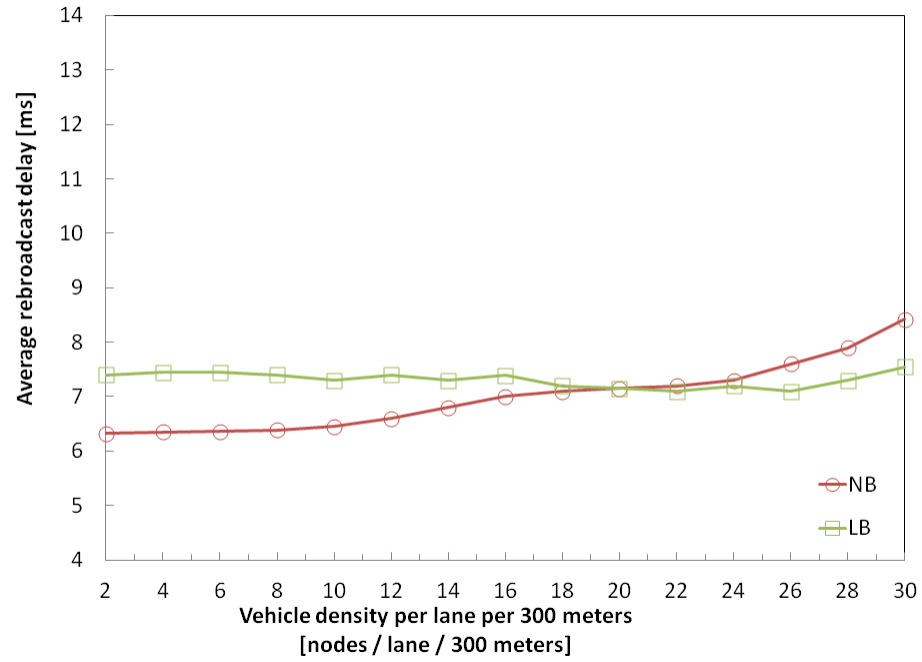
In Figure 10, the average rebroadcast delay in four and eight lane road configuration is

shown with variable vehicle densities. NB in the figure denotes normal-sectoring broadcast, while LB denotes lane-based sectoring broadcast. In Figure 10a, the behavior of both the methods remains unaffected in the low-density scenarios until the vehicle density of 16 nodes per lane per 300 meters. Among the two methods, LB however, slightly falls short in performance in the low density range as a result of the use of longer back-off window than required. Note that the window size for LB has been kept high equal to the number of cells in the scenario (depending on the road width). Nevertheless, a density learning technique can alleviate such additional time slot overhead. For the case of NB, the window size has been varied depending on the density of vehicles. Therefore, NB maintains its advantage in low density scenarios.

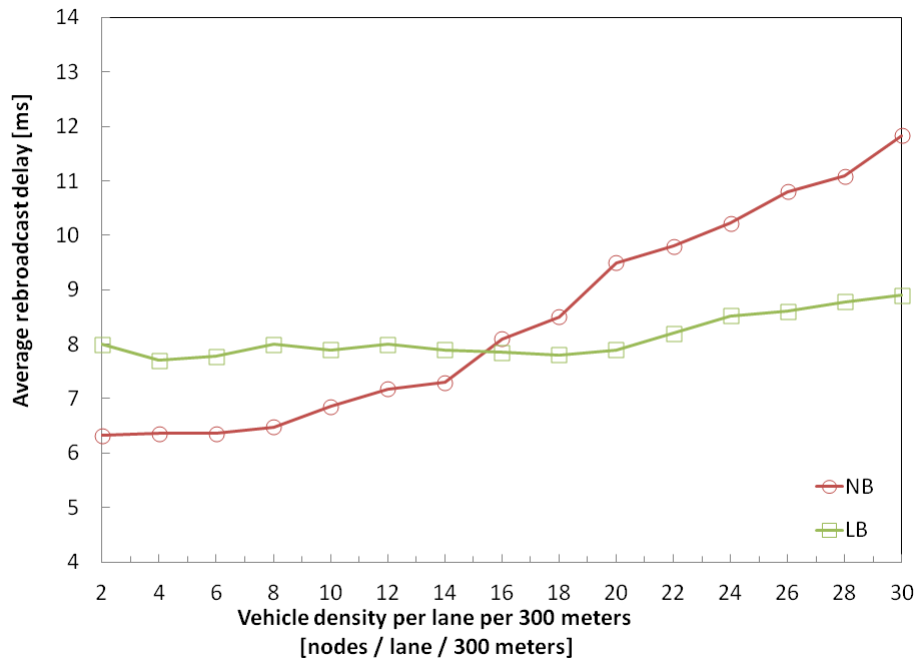
In Figure 10a, as the vehicle density increases above 16 nodes per lane per 300 meters, the additional window size of LB pays off and there is a delay gain of about of two milliseconds per rebroadcast as the density reaches 30. This effect clearly demonstrates the basic principle of LB that as the vehicle density reaches rush hour traffic (i.e., as nearly every cell of the grid is being occupied with vehicles), there is high likelihood that the least back-off value slots are assigned to vehicles and the rebroadcast takes place early in the back-off window.

In Figure 10b, the delay gain of LB over NB becomes clearly compelling. Using eight-lanes road scenario, the NB method sectors the transmission range with narrower sector length, however, the presence of nodes in the parallel lanes is disregarded. Therefore, although the high density of nodes in each sector is considered, the likelihood of back-off value collision among the nodes grows astonishingly higher, thus resulting in resending attempts from the original sender and causing high delay. LB, on the other hand, is affected minimally with higher density and a near one-time-slot per node configuration is achieved. The delay gain reaches as high as five milliseconds per rebroadcast over the normal broadcast method.

Figure 11 shows performance measure with message size of 1000 bytes. The general

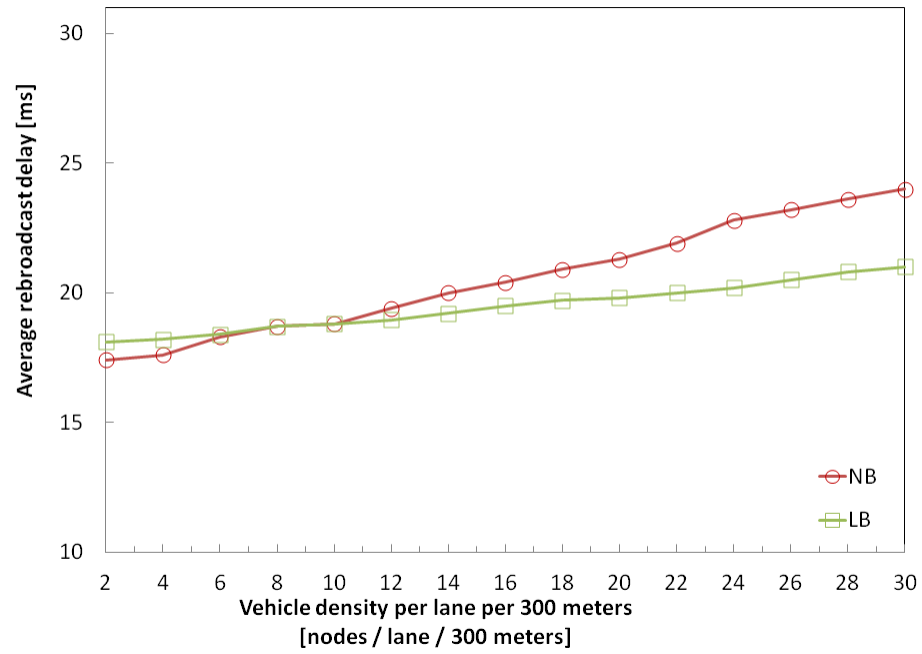


(a) Average rebroadcast delay (using four lanes).

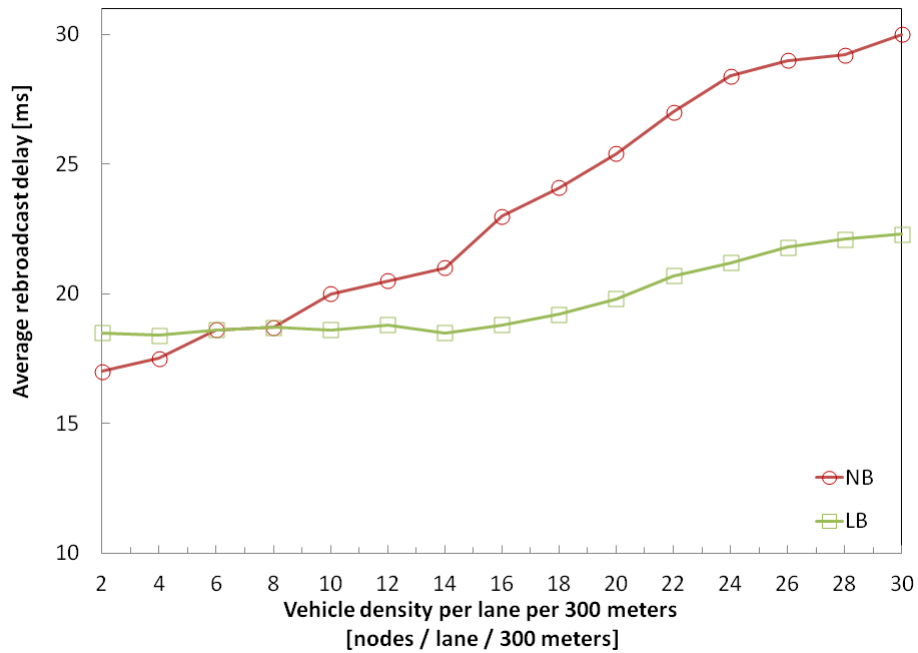


(b) Average rebroadcast delay (using eight lanes).

Figure 10: Average rebroadcast delay in four and eight lanes (message size = 300 bytes).



(a) Average rebroadcast delay (using four lanes).



(b) Average rebroadcast delay (using eight lanes).

Figure 11: Average rebroadcast delay in four and eight lanes (message size = 1000 bytes).

behavior of the two methods follow the same trend as in Figure 10 where the message size is 300 bytes. However, two distinctions are noticed with the higher message size. First, the contention is slightly more sensitive to the node density with higher message size. Second, the overall collision rate is higher for the two methods in both the four- and eight-lane scenarios. The higher message size results in longer medium occupancy by each sender and causing accumulated contenders, thus resulting in more collisions and a resultant longer overall delay. Importantly, the gain of LB over NB method remains significant even with higher message size both in terms of the delay (by nine-milliseconds in the worst case) and collision rate (by two percent in the worst case).

In Figure 12, the average collision percentage is depicted with variable vehicle densities in the four- and eight-lane cases. The figure explicitly depicts the collision-improvement perspective of LB over NB method. Here, collision percentage is the measure of the number of retransmission attempts by the sender. It can be discerned from the figure that the performance of normal-sectoring method NB is severely degraded in high density road traffic. In rush hour traffic where vehicle density increases above 16, the collision rate steeply rises as high as 2.4% in eight-lane scenario. Higher collision directly incurs high-retransmission rate, thus affecting the overall end-to-end delay as well as the message-dissemination reliability. The LB method, in contrast, maintains collision percentage below one even in the worst case of eight lanes with 30 nodes per lane, thus promising high reliability as required for the safety-message communication in VANETs.

In this chapter, we have presented a new technique for the sectoring of the broadcast range for safety-message routing in VANETs. The rush-hour-traffic scenario is considered where most of the hitherto mechanisms are severely affected by collisions and high message-propagation delays resulting from collisions. The hitherto neglected factor of road width is introduced for use as a second dimension for sectoring the transmission range of the message sender. An extensive simulation evaluation is performed using the ns-3 simulator, and the results suggest that the lane-based sectoring significantly improves the

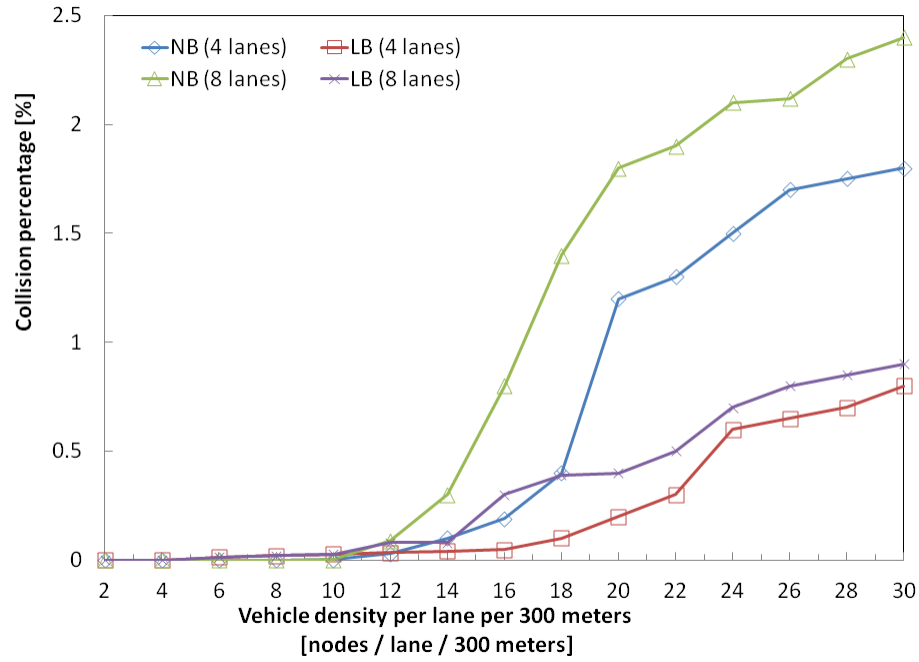


Figure 12: Average collision percentage.

message-propagation delay by as much as nine milliseconds for rebroadcast in each hop and reduces the rebroadcast collisions by two percent over the existing sectoring techniques even in the worst traffic scenario.

Uncovering the importance of the road width for VANETs in this chapter will assist in understanding a more detailed road topology that influences the VANET communication. The idea of segmenting the transmission range into manageable units can also be replicated in the service-channel allocation strategy in VANETs where there is an equally critical concern for the effective channel utilization.

CHAPTER 4

RECOVERING THE MESSAGE LOSS CAUSED BY INTERFERENCE

To address the core design issue of ensuring maximum reliability of reception by all endangered vehicles, a collision detection and recovery mechanism called NACK with smart neighborhood (NSN) is presented in this chapter. By introducing the concept of smart neighborhood, the NSN technique covers the message loss resulting from collisions, and at the same time avoids additional channel reservation for the feedback mechanism.

4.1 Message Loss from Collisions

One of the core design issues in VANETs is the reliable propagation of safety messages to all the related (endangered) vehicles on the road. The intended propagation region could be the immediate transmission range of about 300 meters or the long multi-hop forwarding range spanning more than a kilometer distance depending on the type of safety application. The propagation path either single or multiple hops involves a number of factors impeding some vehicles along the way from receiving the safety-alert message. As a result, the impeded vehicles either receive the message not intact or are completely oblivious of the activity in the channel. Furthermore, since the safety-message dissemination is carried out using broadcasting, there is no feedback mechanism to recover the impeded vehicles, thus always compromising the reliability. The collisions and interference due to the contending and hidden nodes are a major cause of corrupted messages, while the obstructions in the propagation line of sight cause oblivious nodes.

The vehicle movement on a road is bound by street maps, traffic signals and regulations, and the movement of the surrounding vehicles. Consequently, the distribution of vehicles is highly non-uniform and the connectivity among vehicles is highly random. Furthermore, the inevitable usage of common control channel for safety applications makes communication immensely vulnerable to collisions and interference from visible and hidden nodes

[32].

Considerable work has been carried towards the development of the safety-message broadcast algorithms with the aim of reducing collisions and improving message dissemination delay. In this regard, the main focus has been on the message propagation in case of multi-hop relay broadcast, taking for granted the connectivity among all the nodes within the single transmission range (or same hop) [25, 27]. However, the connectivity among nodes in the single transmission range is adversely affected by concurrent transmissions causing interference which is potentially common in the urban scenarios with parallel and overlapping roads, interchanges, overhead bridges and intersections. Additionally, the transmission holes due to obstacles in the LOS are an equally major cause of disconnection among the same hop neighbors. Therefore, in order to ensure maximum reliability of the safety message transfer in VANETs, it is imperative to address and confirm the reception at each individual node level. Thus, coverage of (or recovering) a message loss resulting from collisions and interference forms the core of the NSN reliability algorithm presented in this chapter.

The NSN algorithm aims to guarantee the delivery of safety message to all the related vehicles (endangered by an event) on the road. The delivery of message is ensured through the use of the negative acknowledgement (NACK) mechanism together with a constant observation from the immediate neighbors. Immediate neighborhood is defined as the area around a given node with a radius encompassing two neighbors of the given node (or more than two neighbors if there are more nodes present within the two-node radius). Immediate neighborhood is discussed in detail in later in this chapter. NACK, unlike in the conventional networks, is broadcasted only in the immediate neighborhood to maintain efficient channel utilization. The power controlled NACK broadcast by the given node and the subsequent response from a neighboring node account for the reporting of message received in error and the recovery mechanism, respectively.

The proposed idea is studied using thorough theoretical analysis and ns-3 simulation

implementation. The average packet-reception rate (PRR) is formulated as the performance metric with thorough considerations of the ad-hoc network parameters and effects. It is established that the proposed NACK with Smart Neighborhood (NSN) technique expunges the packet-loss effects resulting from collisions due to hidden nodes.

4.2 System Model and Assumptions

The system under concern involves vehicles moving on the road with one or more lanes (with equal lanes in each direction). The street map includes linear roads with intersections at random lengths on the road. The scenario also assumes the possibility of parallel or service roads, ramps, interchanges, and overhead bridges to include the worst case of interference and packet collisions. The density and speed of vehicles is variable to account for both highway and urban traffic. The size of vehicles is assumed to be variable to include both heavy commercial vehicles and normal cars. Each vehicle is equipped with a global positioning system (GPS) receiver and a digital map. To account for viability of the system, the model does not rely on the presence of roadside units (RSU). Presence of RSU, however, is always helpful in improving the overall performance in VANET communication since with RSU the process of rebroadcaster (or forwarder) elimination becomes straight forward.

A generic safety-message application is considered that may require one-hop or multi-hop transmission along the road. Periodic beaconing messages are considered among vehicles with the preferred frequency as 10 messages per vehicle per second. The suggested beaconing frequency conforms to the IEEE 802.11p specifications. Each beaconing message is assumed to contain vehicle location, speed and direction information as well as a minimal (less than one byte) overhead field describing vehicle type for use in the received signal strength (RSS) estimation.

NSN technique is aimed to guarantee reliability in the existing VANET safety-message routing protocols. It is worth mentioning here that NSN does not assume any specific

safety-message routing protocol for message transmission and multi-hop propagation. Instead, NSN is a generic reliability technique that can be incorporated with any base safety-message propagation method to ensure reliability. Additionally, the integration with a base message propagation method enables NSN to fully inherit the collision avoidance mechanisms of the base protocol including hidden-node problem avoidance and interference mitigation.

4.3 NACK with Smart Neighborhood (NSN)

The original safety-message initiation and forwarding is carried by the base routing protocol. For the sake of explanation, the urban multi-hop broadcast (UMB) [25] is considered as an example base protocol. However, as mentioned above NSN is flexible to be incorporated on top of any base safety-message routing method.

A node originates a safety message after sensing a hazardous event on the road. Upon gaining access to the medium the node broadcasts a safety alert message within its one-hop transmission range. Depending on the type of safety application the message may be intended for all the one-hop neighbors, vehicles following the message originator in the same direction, or vehicles in multiple directions. The goal of a safety message is to reliably alert all the endangered vehicles of the hazard event. If the message is intended for multiple hops then one of the receivers forwards the message to the next hop after following an elimination scheme. The general elimination scheme employed by most of the routing protocols is based on sectoring. The transmission range of the sender is divided lengthwise into multiple sectors based on the density of vehicles. The back-off contention window is divided accordingly into multiple fixed-size sub-windows. The sub-windows are in turn assigned to each sector in a way to ensure that the furthest nodes in the transmission range receive smaller back-off values. Thus, a node in the furthest range rebroadcasts (or forwards) first. Once the rebroadcast takes place by any node, all the remaining nodes with larger back-off values overhear the message and quit their rebroadcast. The same procedure is repeated

in the following hops until the message reaches its maximum distance (or TTL) defined in the header. At each hop of the message propagation, once the broadcast transmission takes place, the crucial role of NSN comes in to play to ensure that the message is received by each node in the intended region. The NSN algorithm tracks each node individually to guarantee the reception of the message. There are two possibilities at each node locally, namely, the case when an unrecoverable signal is received and the case when there is no signal received at all. The discussion in this chapter concerns the former case, while the latter case of recovering the message loss in a coverage hole is presented in detail in the next chapter with the NSN-H algorithm.

Figure 13 depicts the unrecoverable signal scenario with NSN recovery. Node A broadcasts a safety alert message within its transmission range (about 300 meters). This broadcast could be initiation of a new alert message or a relay from a previous hop. The message is intended for all the nodes in the transmission range. However, as a result of the use of single control channel for all safety related communications, there exists a possibility of interference causing some nodes receiving the message in error. Interference is primarily caused by hidden nodes with concurrent transmissions. The existing RTS/CTS like handshake for VANETs has limited advantage in real urban environments in the presence of intersections, over head bridges and parallel road. A single vehicle (e.g., the furthest vehicle) does not necessarily have the same neighbors as other vehicles in the broadcast range. Since the RTS/CTS method proposed for VANETs designates only a single vehicle to send a CTS message, it does not always thwart hidden-node problem for the rest of the neighboring nodes. Thus, in the given scenario as an example, node B is assumed as a node that receives an unrecoverable signal resulting from interference in the common channel, while the remaining nodes receive the message intact. Node B waits for a period of one complete rebroadcast cycle to allow for self recovery (i.e., self recovery by overhearing the same message rebroadcasted by the relay node in multi-hop forwarding). Since NSN is generic for both single-hop and multi-hop forwarding, the wait period is kept fixed. It

is worth mentioning here that the average time of one complete rebroadcast cycle is only about $620 \mu sec$ (including inter-frame spacing and the back-off window); thus, the minimal rebroadcast overhead is not likely to cause delay longer than the effective life of the message. If B does not overhear any safety message during the wait period, it chooses a back-off value window from one to 14 and broadcasts a short NACK message within its immediate neighborhood.

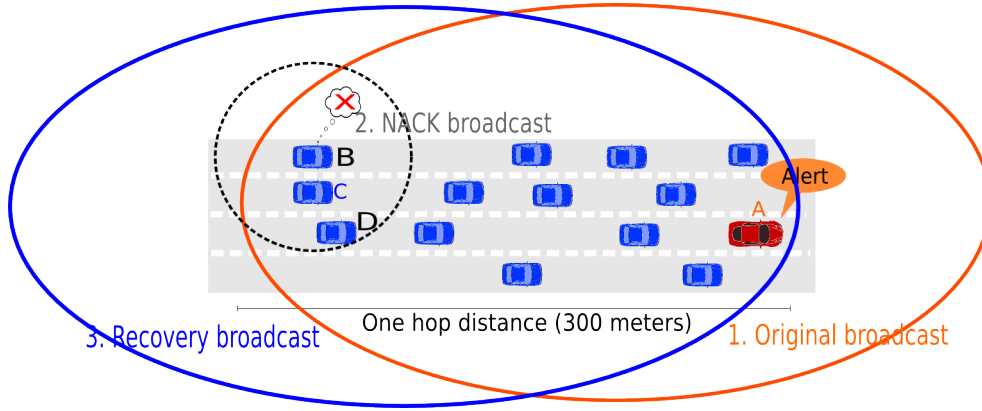


Figure 13: Recovering unrecovered signal using negative-acknowledgement with smart neighborhood.

Immediate neighborhood is defined as the area covered by a circle with radius r around a given node x such that there exist two nodes y and z , where $r = \|x - z\|$ and $\|x - y\| \leq \|x - z\|$. Additionally, $r \leq \|x - n\|$ for any node n , where $n \neq x \neq y \neq z$. Thus, r is the smallest possible radius around a given node that can house two other neighboring nodes. Although one neighboring node may suffice as a rescuer, the aim of keeping additional node in the immediate neighborhood is to provide added reliability at the recovery stage such that in case one node fails to rescue, the second node compensates. Note that it is possible that there are more than two neighbor nodes within the same radius following the above criteria as multiple nodes can have the same distance from the given node.

Node C and D happen to be in the immediate neighborhood of B, and receive the NACK message. Subsequently, C and D contend to rebroadcast the previously received safety message in order to recover B. Each node that receives the NACK message, in this case C and

D, follow the above mentioned sectoring based rebroadcaster elimination; resulting in node further from the original message sender (i.e., from A) winning the contention. Therefore, node C rebroadcasts the safety message in its entire 300 meters transmission range. The reason for the recovery broadcast range being beyond the immediate neighborhood is to cover the case where multiple nodes had received the original message as an unrecoverable signal and have requested a recovery broadcast using NACK with in their respective immediate neighborhoods. The sectoring based elimination and the entire one-hop range for the recovery broadcast makes sure that only one node performs the rescue task and recovers all the nodes in need of the rebroadcast. Thus, node B finally receives the original safety message.

In Algorithm 1, the functioning of NSN recovery is summarized for the two cases of message loss. The algorithm describes the flow of both the NSN recovery phases in a simultaneous manner. For the purpose of easier understanding of the reader, the description of the base routing model in the algorithm is omitted. The reader may refer to Chapter 3 for the description of the base routing algorithm.

4.4 Analysis of the NSN Algorithm

4.4.1 Reliability metrics and base parameters

In this section we evaluate reliability of the proposed NSN technique in one hop. We use packet reception rate (*PRR*) as the performance metric to evaluate reliability. *PRR* is defined as the percentage of nodes that successfully receive the safety packet among all the nodes in the transmission range of the original sender (or forwarder if the hop under study is the next hop in multi-hop forwarding case).

PRR was first introduced for VANETs by Moreno et al. in [42]. Later, thorough analytical models to evaluate *PRR* for safety messages were proposed in [43, 44, 45]. In this section we assume *PRR* as defined in [45] as

Algorithm 1 Pseudo code for NSN.

```
1 Initialize
2  $R_i \leftarrow$  one-hop transmission range of node  $i$ ;
3  $r_i \leftarrow$  radius of immediate neighborhood of node  $i$ ;
4  $I_i \leftarrow$  set containing nodes in the immediate neighborhood of node  $i$ ;
5  $N_i \leftarrow$  rebroadcast sectors around node  $i$ ;
6  $rs_i \leftarrow$  rebroadcast sector of node  $i$ ;
7  $w \leftarrow$  contention window of each sector;

8 Event new safety alert message received from node  $s$ 
9 foreach  $n \in R_s$  do
10   if (to_nack = set) then
11     cancel to_nack;
12   else if (message_id = redundant) then
13     cancel schedule_rebroadcast;
14   else
15     compute  $\|n - s\|$ ;
16     choose  $rs_i$  corresponding to  $\|n - s\|$ ;
17     schedule_rebroadcast with random_backoff  $N_{s,w} - rs_{i,w} + \text{random}(w)$ ;

18 Event new beacon message received
19   compute  $\|n - s\|$ ;
20   if ( $\|n - s\| \leq r_i$ ) then
21      $I_i \leftarrow I_i \cup \{s\}$ ;
22   else if ( $s \in I_i$ ) then
23      $I_i \leftarrow I_i \setminus \{s\}$ ;

24 Event unrecoverable signal received by node  $i$ 
25   set to_nack;
26   wait for rebroadcast_cycle;

27 Event rebroadcast_cycle expires for node  $i$ 
28 if (to_nack = set) then
29   broadcast nack in  $r_i$ ;
30 else
31   if (to_rescue = set) then
32     broadcast recent message in  $R_i$ ;
```

$$PRR(d) = \frac{\text{No. of successful receivers in distance } d}{\text{Total no. of nodes in distance } d}. \quad (24)$$

In our evaluation we make the following assumptions while formulating the analysis for the safety-message broadcast:

1. We consider linear road scenario consisting of randomly distributed nodes on the line. Linear assumption of the road is reasonable as the width of the road is negligible compared to the length of packet transmission.
2. Nodes are placed on the line in a Poisson point process with density λ (in nodes per meter length of the road). Then, the probability $P(i, l)$ of i nodes in a length l is given by

$$P(i, l) = \frac{(\lambda l)^i e^{-\lambda l}}{i!}. \quad (25)$$

3. For the sake of accuracy in our analysis, we assume transmission range, carrier sensing range and interference range as distinct. All nodes have equal transmission/reception range denoted by R . Carrier sensing range is denoted by R_{cs} such that $R \leq R_{cs} \leq 2R$. Again, we assume R_{cs} as constant for all the nodes. While interference range is denoted by R_{int} such that $R \leq R_{int} \leq R_{cs}$. Now, the average number of nodes on the line within the transmission and carrier sensing range are $2\lambda R$ and $2\lambda R_{cs}$, respectively. While the average potential hidden nodes for a given sender can be written as $2\lambda(R + R_{int} - R_{cs})$.
4. Node mobility is not considered in the analysis as with normal communication parameters, the average link loss probability during message transmission is 0.0052 [45]. Moreover, we do not consider the impact of channel shadowing or fading effect due to road surrounding. We focus on packet loss due to visible and hidden node collisions, as well as the effect of other obstructing nodes on the road as obstacles in the path.

Now we layout the main parameters used for our analysis. Assume constant backoff window size W_b for each safety-message broadcasting node. Then, by following the same procedure in [42], the probability that a node transmits in a generic slot is given by

$$\tau = \frac{2(1 - p_0)}{W_b + 1}, \quad (26)$$

where p_0 is the probability that there are no packets ready to transmit in each node, shown later in this section. Let the system data rate as R_b , the average packet length $E[P]$, header length as H_L (including both MAC and PHY layer headers), while DCF inter-frame space as $DIFS$ and the propagation delay as δ . Then, the channel busy time because of an ongoing transmission can be written as

$$T = \frac{(H_L + E[P])}{R_d} + DIFS + \delta. \quad (27)$$

Let p_b as the probability that the channel sensed by the sender is busy. From [45] considering the channel is sensed busy if there is at least one node transmitting in the carrier sensing range of the given node and that the nodes are distributed exponentially on the linear road. Then, p_b can be written as

$$\begin{aligned} p_b &= 1 - \sum_{i=0}^{\infty} (1 - \tau)^i \frac{(2\lambda R_{cs})^i}{i!} e^{-2\lambda R_{cs}}, \\ &= 1 - e^{-2\lambda R_{cs}\tau}. \end{aligned} \quad (28)$$

Now we express the service time distribution nodes in the network. As characterized in [44, 45], we consider each node in the network as an M/G/1 queue with inter-arrival times for nodes as exponentially distributed and the service time as discretely distributed where the smallest time unit of backoff timer is one time slot t' , and the transition of backoff timer decremented with a probability generating function

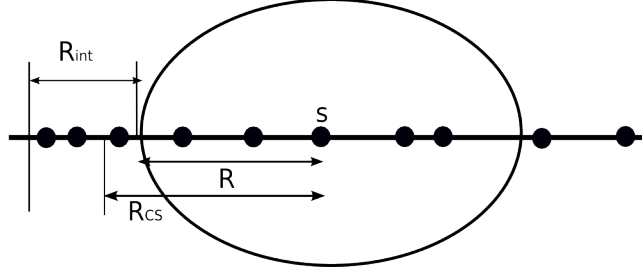


Figure 14: Omni-directional broadcast in a linear setting.

$$H_d(z) = (1 - p_b)z + p_b z^{\lfloor \frac{T}{T'} \rfloor} \quad (29)$$

where the function $\lfloor \cdot \rfloor$ is used to round time to time slot units. The probability generating function for steady state probability that the packet service time is iT' is expressed as

$$Q(z) = \sum_i q_i z^i = \frac{z^{\lfloor \frac{T-DIFS}{T'} \rfloor}}{W_b} \sum_{i=0}^{W_b-1} H_d^i(z) \quad (30)$$

4.4.2 Packet-reception ratio (PRR) formulation

The packet reception percentage can be effected by number of vehicles present in holes, collisions caused by hidden terminals, and collisions caused by concurrent transmission of nodes within the carrier sensing range of the sender.

Let φ be the average loss in signal strength caused by a vehicle and m be the average number of vehicles in the linear propagation path that cause complete obstruction. In other words, φm is the loss that cause the received signal drop below the receiver sensitivity threshold. Then, the average distance from the sender where there exist no reception holes is $L_{nh} = m/\lambda$. Neglecting the effect of hidden nodes and concurrent transmission of visible nodes (both effects are incorporated subsequently), the percentage of receivers that are free from packet loss due to holes can be written as:

$$PRR_{holes} = \begin{cases} 1, & 0 < d \leq L_{nh} \\ 0, & L_{nh} < d \leq R \end{cases} \quad (31)$$

Now we express the effect on PRR caused by the hidden terminals in our safety-message broadcast scenario. If R_s is the range in the potential hidden terminal area where no node transmits, then, the cumulative distribution function (cdf) for x , where x is the distance from the closest potential hidden node, is given by

$$P(X \leq x) = \sum_{i=0}^{\infty} [P(\text{none of } i \text{ nodes in } R_s \text{ transmit for } T_v)], \quad (32)$$

where $T_v = 2(E[P] + H_L)/R_d$ is the vulnerable period during which sender's transmission is vulnerable to the hidden node problem. Following the formulation in [43, 45], the expected number failed nodes NF_h due to hidden node problem can be expressed as

$$NF_h = \lambda(d + R_{int} - R_{cs} - \frac{1}{C})e^{-(R-d)C} + \frac{\lambda}{C}e^{-(R+R_{int}-R_{cs})C}. \quad (33)$$

where $C = \lambda T_{vul} \tau / t_s$, and $t_s = (1 - p_b)t' + p_b T$. While t_s is the average duration of a virtual time slot. Then, percentage of receivers that are free from collisions can be written as

$$PRR_{hn}(d) = \begin{cases} 1, & 0 < d \leq R_{cs} - R_{int} \\ \frac{\lambda d - NF_h}{\lambda d}, & R_{cs} - R_{int} < d \leq R \end{cases}$$

$$= \begin{cases} 1, & 0 < d \leq R_{cs} - R_{int} \\ 1 - (1 - \frac{R_{cs} - R_{int}}{d} - \frac{1}{dC}) e^{-(R-d)C} \\ \frac{1}{dC} e^{-(R+R_{int}-R_{cs})C}, & R_{cs} - R_{int} < d \leq R \end{cases} \quad (34)$$

Now we consider the impact of concurrent transmissions due to visible nodes. In addition to collisions caused by hidden terminals, concurrent transmissions from visible nodes (see Figure 15 for collision impact ranges of concurrent transmissions) can cause collisions during the ongoing transmission of a safety message by the sender. As show in Figure 15,

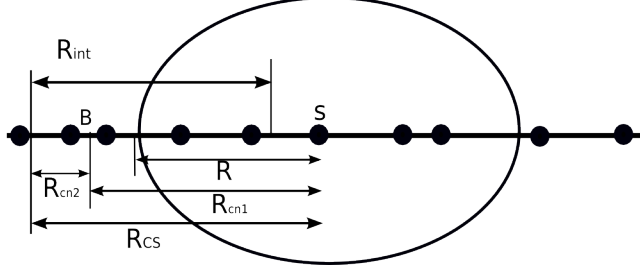


Figure 15: Effect of simultaneous transmissions from nodes in the interference region.

the simultaneous transmission of any node in R_{cs} will cause all nodes in R receiving the packet in error. We follow [42, 44, 45] again and formulate R_{cs} as union of R_{cn1} and R_{cn2} . The ratio of nodes in R free from concurrent transmissions in R_{cn1} is

$$\begin{aligned} PRR_{cn1} &= \sum_{i=0}^{\infty} (1-\tau)^i \frac{(\lambda R_{int} - 1)^i}{i!} e^{-(\lambda R_{int} - 1)}, \\ &= e^{-(\lambda R_{int} - 1)\tau}. \end{aligned} \quad (35)$$

The ratio of percentage of receivers that are free of collisions from concurrent transmissions in R_{cn2} can be written as

$$PRR_{cn2}(d) = \frac{\lambda d - NF_{cn}}{\lambda d}, \quad (36)$$

where NF_{cn} is the number of nodes in R effected by concurrent transmissions from nodes in R_{cn2} . NF_{cn} is expressed from [45] as

$$NF_{cn} = \begin{cases} \frac{1}{\tau} e^{-\lambda(\Delta R - d)\tau} - \\ (\lambda d + \frac{1}{\tau}) e^{-\lambda \Delta R \tau}, & 0 < d \leq \Delta R \\ \lambda(d - \Delta R - \frac{1}{\lambda \tau}) \\ (1 - e^{-\lambda \Delta R \tau}) \\ + \lambda \Delta R, & \Delta R < d \leq R \end{cases} \quad (37)$$

where $\Delta R = R_{cs} - R_{int}$.

Combining (35) and (36), the packet reception ratio effected by concurrent transmissions from any node in the carrier sensing range becomes

$$PRR_{cn} = PRR_{cn1}PRR_{cn2}(d). \quad (38)$$

Finally, combining (31), (34) and (38), the overall packet reception ratio can be expressed as

$$PRR(d) = PRR_{holes}PRR_{hn}PRR_{cn} \quad (39)$$

PRR in (39) calculates the percentage of nodes in transmission range that successfully receive the broadcasted message while considering the packet losses in transmission holes, packet loss due to collisions caused by hidden nodes, and packet loss due to collisions by concurrent transmissions from nodes in the carrier sensing range. For the case of the NSN, the $PRR(d)$ becomes

$$PRR(d) = PRR_{cn}, \quad (40)$$

representing the NSN recovery such that the NSN algorithm recovers both the vehicles in located in holes as well as the vehicles with unsuccessful reception due to collisions from the hidden nodes. Whereas vehicles with unsuccessful reception due to concurrent transmissions from nodes in the carrier sensing range may remain vulnerable to be uncovered.

4.5 Simulation Analysis

To analyze the performance of the proposed NSN method we have fully implemented NSN on top of the IB protocol. In addition, for comparison we have also implemented UMB [25] and R-OB-VAN [31] protocols with their original dissemination mechanism. Simulation is implemented in the ns-3 simulator, Version 3.9[36]. The traffic mobility is generated using the VanetMobiSim tool [37]. General simulation parameters are summarized in Table 3. For details about the simulation setup, the reader can refer to Chapter 3.

Table 3: Simulation parameters for the NSN technique.

Description	Value
Transmission range	300 meters
Data rate	3 Mbps
Message payload size	100 Bytes
Protocol overhead	14 bytes
MAC header size	34 bytes
PHY header size	26 bytes
RTB, CTB, ACK, NACK	20, 14, 12, 10 bytes
Time slot, DIFS, SIFS	20, 50, 10 μs
Road length	4 km (2 lanes, unidirectional)
Vehicle density	2-30 vehicles/300 meters
Vehicle speed	50 miles/h (mean)
Message generation rate	0.01-1 message per vehicle/second
Path loss model	Log-distance model
Fading model	Rayleigh fading model
Simulation time	100 seconds (each run)

In Figure 16, the packet loss rate (PRR) is depicted against the node density. In the figure, the loss of a packet is the event when a node within the broadcast range does not receive a given safety-message. A packet loss is not counted for the node when the node eventually receives the message after a recovery rebroadcast or a forwarding rebroadcast. The packet-loss rate only counts the loss of a safety-message packet, and the overhead and control packets are not considered in the metric. The figure provides a comparison of the core aspect of reliability among the three routing methods. Clearly, the proposed NSN algorithm achieves a promising reliability level of about 0.2% even in the worse-case traffic scenario. The NSN algorithm outperforms the UMB method and the R-OB-VAN method by over 2% and 0.7%, respectively, in terms of the packet-loss rate in the high traffic-density scenario. The high traffic-density scenario has the acute number of packet collisions due to contending nodes, and thus, the scenario is most challenging in terms of ensuring the reliability of packet reception. By employing the efficient feedback mechanism, the proposed NSN algorithm follows each packet to its intended receivers even in a scenario with very dense traffic. In the high density traffic, the minor loss of packets is due to the

exhaustion of the recovery attempts. In the simulation, a limit of one recovery rebroadcast per vehicle has been maintained to avoid excessive use of the channel.

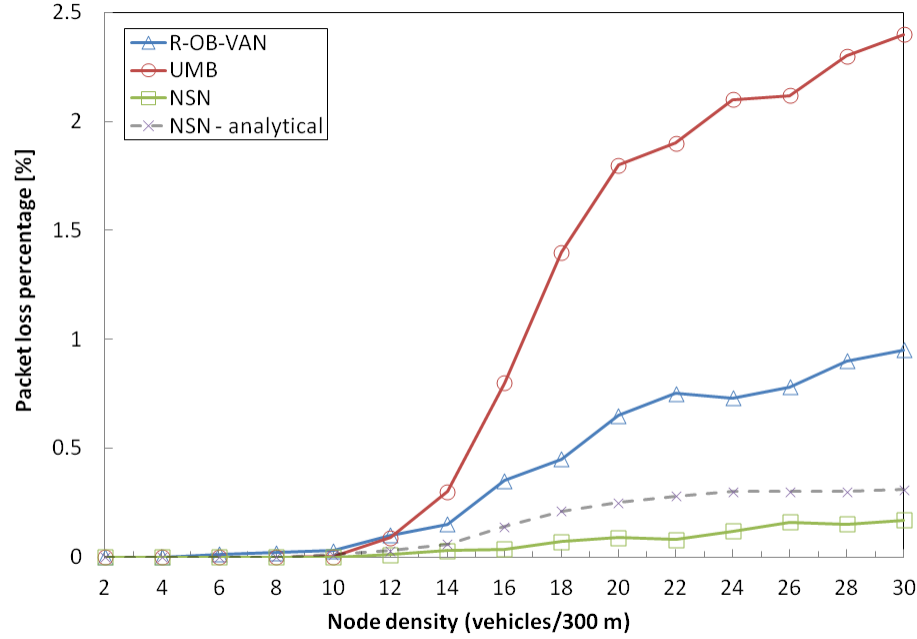


Figure 16: Packet loss rate of NSN, UMB and R-OB-VAN methods.

The R-OB-VAN method performs better than the UMB method in terms of reliability. The R-OB-VAN method provides a recovery mechanism for the packet loss. The recovery method maintains reliability in the low density scenario. However, in the high density traffic, the reliability decreases resulting from the probabilistic recovery response. The recovery broadcast is triggered only when a given node determines a neighbor with less number of neighbor nodes than the given node. The condition requires perfectly uniform density of nodes, which is not always the case in road traffic. Additionally, the R-OB-VAN method lacks a collision avoidance mechanism among multiple contenders of recovery-message broadcast. The lack of collision avoidance mechanism results in further collisions in the high-density traffic. The UMB method, on the other hand, is based on the objective of broadcast efficiency. Therefore, the method lacks any reliability mechanism. The UMB method uses the ACK broadcast message that only ensures the the forwarding broadcast

by the relay node. Therefore, the UMB method suffers packet loss in the acute collision scenario of high-traffic density.

In Figure 17, the normalized link load is depicted against the node density. The normalized link load is the percentage of redundant receptions of the safety-message by the vehicular nodes. The redundant receptions considered in the figure do not account for the redundant receptions caused by the forwarding node. Therefore, the redundant receptions essentially account for the redundant broadcast in the channel resulting from any recovery mechanism. As a result of the overhead caused by the rigorous collision detection and recovery mechanism in the NSN method, a slightly higher link load can be observed for the proposed method as compared to the two existing methods. The increase in the link load is a result of the NACK message and the ensuing recovery-broadcast message. However, the increase in the link load is negligible considering the actual objective of the proposed NSN technique. All the three protocols are equally affected in the high-node-density range as a result of the excessive number of collisions and the resultant rebroadcast packets. In the worse-traffic scenario the link load incurred by the proposed technique is close to the link load of the R-OB-VAN method. The UMB method maintains lower link load among the three methods as a result of the lack of additional overhead packets for the recovery mechanism. The link load incurred by the UMB method is due to the recovery rebroadcast by a given relay node (or a message initiator) in a case where the next relay node fails to rebroadcast the message.

The mean one-hop delay is depicted against node density in Figure 18. The delay accounts for the total time of safety-message propagation from the instant of the broadcast of the message (including the transmission time) from a node in the given hop to the reception of the message among all the nodes in the given hop. The instant of the reception of the message is the instant when the last receiving node in the given hop receives the message (including a node that receives the message after a recovery mechanism). The R-OB-VAN method incurs the highest delay among the three broadcast methods. The excess delay

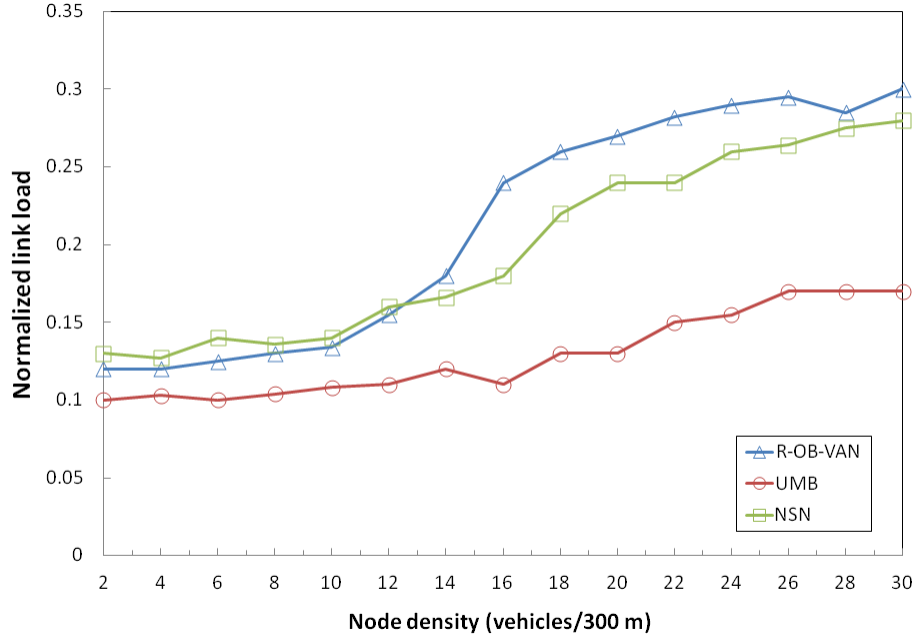


Figure 17: Normalized load generated of NSN, UMB and R-OB-VAN methods.

of the R-OB-VAN method is due to the unnecessary rebroadcasts of the probabilistic loss detection and the resultant collisions in the high node density. Moreover, the collisions caused by the recovery-broadcast contenders incurs additional delay due to the the lack of a contention resolution mechanism. The proposed NSN technique achieves a delay of about 14 milliseconds in the worse-case traffic. The delay of the NSN technique is a mere 2 milliseconds above the delay of the UMB method. Thus, despite the rigorous collision detection and recovery mechanism, the NSN technique achieves a high message-propagation speed as the UMB method.

In Figure 19, the mean one-hop propagation delay is depicted against the variable message-generation rate. The high message-generation rate is a scenario where the collisions among the contending nodes is acute. The result in the figure further asserts the efficiency of the proposed NSN method. In the figure, the delay of the NSN method is close to the delay of the IB method. The IB method is efficient among the three method as a result of the lack of a feedback mechanism. The IB method propagates the safety

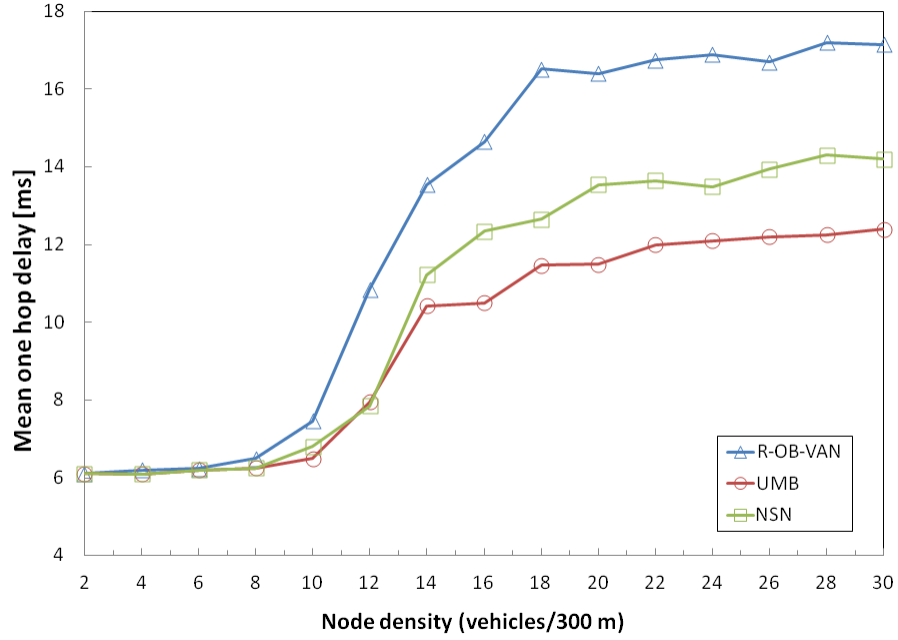


Figure 18: Mean one-hop delay of NSN, UMB and R-OB-VAN methods.

message among the hops and the only case of the rebroadcast is when a relay node fails to forward the message. On the other hand, the NSN technique offers maximum reliability by triggering rebroadcast for every instance of a failed reception. Since the power-controlled NACK feedback and the collision mitigation technique of the NSN method prevents the excessive collisions and the resultant delay, the efficiency of the message dissemination is maintained even in the worst traffic conditions.

In this chapter, we have presented a new technique called NACK with Smart Neighborhood (NSN) to ensure reliability for safety message dissemination in VANETs. The concept of smart neighborhood is presented where we designate neighbors present in a confined immediate neighborhood to carry the responsibility of ensuring successful reception at their corresponding neighbors. We aim to guarantee the reception of safety message to all the related vehicles (endangered by an event) on the road. The reception of message is ensured through the use of negative acknowledgement (NACK) mechanism together with constant observation by the immediate neighbors. Immediate neighborhood is defined as

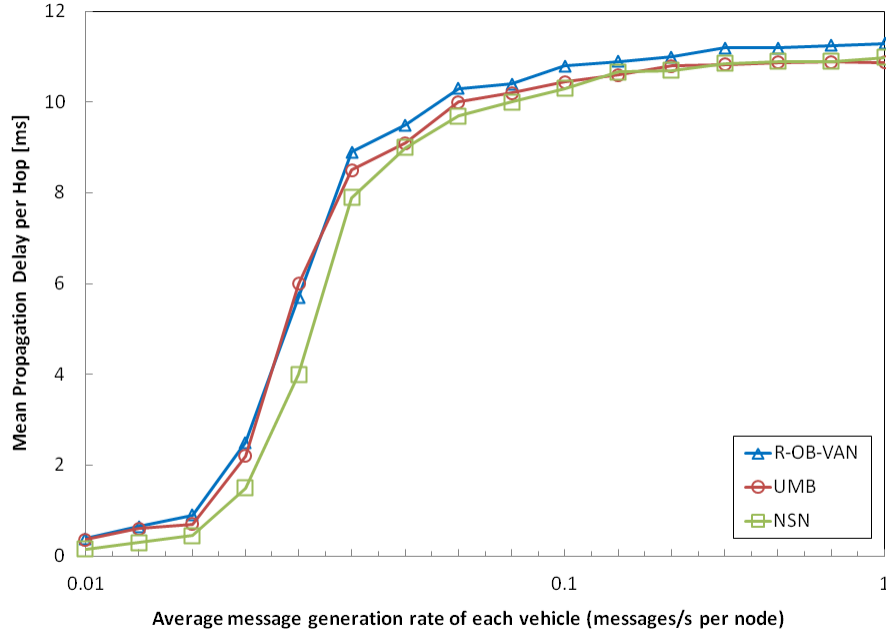


Figure 19: Mean propagation delay of NSN, UMB and R-OB-VAN methods.

the area around a given node with radius encompassing two (or more if there are more than two nodes present within the two node radius) other neighbors. NACK, unlike in conventional networks, is broadcasted only in the confined smart neighborhood to maintain effective channel utilization. Upon the reception of the NACK message, the immediate neighbors of the given node follow sectoring based elimination mechanism to decide a unique rescuer. The rescuer node rebroadcasts the safety message in the neighborhood and recovers the message loss at the given node. The NSN technique ensures the reliability of reception in the cases where a given node encounters message loss due to interference. However, the NSN technique lacks support for the cases where a node is located in a coverage hole. In the following chapter, the scenario of coverage holes in the vehicular scenario is addressed in detail, and a coverage hole detection and recovery mechanism is presented to ensure the reception of the safety message by all the vehicles in a given neighborhood.

CHAPTER 5

MESSAGE DELIVERY TO THE COVERAGE HOLES

Building on the idea of providing maximum reliability presented in the previous chapter, the critical problem of ensuring the delivery of safety messages in the coverage holes is addressed in this chapter. An extension to our NSN algorithm is presented to cover the vehicles located in the transmission holes. Vehicles in the immediate neighborhood detect an immediate neighbor located in the transmission hole by estimating the propagation loss for the neighbor. The NSN recovery broadcast is performed after detecting a neighbor located in the coverage hole. The NSN algorithm together with the hole detection and recovery mechanism guarantees the delivery of safety messages in a VANET.

5.1 Coverage Holes in the Vehicular Scenario

The connectivity of vehicles is affected by the obstructions either static (e.g., buildings, vegetation, hills) or mobile (other vehicles on the road). The relatively low height of antennas onboard the vehicles implies that the optical line of sight (LOS) can be obstructed by the obstructions, in particular by the mobile obstructions causing transmission holes even within the single hop transmission range. Most of the studies identify static obstacles as the only source of obstruction in the propagation path [17, 18]. However, since a significant portion of the inter-vehicular communication is bound to the road surface, it is imperative to consider other vehicles as obstacles in the LOS between two communicating nodes. The experiments of [19, 20] report that a single vehicle as an obstacle in the LOS can cause a drop of as much as 20 dB in the received signal strength. As a result, it is highly likely that in traffic with large public transportation and commercial vehicles such as buses and trucks, a number of coverage holes are present in the transmission range causing several vehicles completely unaware of the ongoing safety message transmission. The complete obliviousness of a vehicle located in a coverage hole makes it highly challenging to be covered by a broadcast mechanism even with the use of a feedback technique.

In Figure 20, a typical coverage-hole scenario is depicted for the vehicular traffic. The vehicle with the safety alert broadcasts a safety message in the neighborhood. Most of the vehicles in the transmission range receive the safety message except the three encircled vehicles that are located in the coverage holes. The vehicles located in the coverage holes are obstructed by a number of vehicles in the line of sight to the sender. A single large truck in the vehicular traffic can cause a signal loss up to 20 dB. As depicted in the figure, the trucks present in the line of sight to the sender results in high propagation loss, and three nodes in the neighborhood do not receive the safety message.

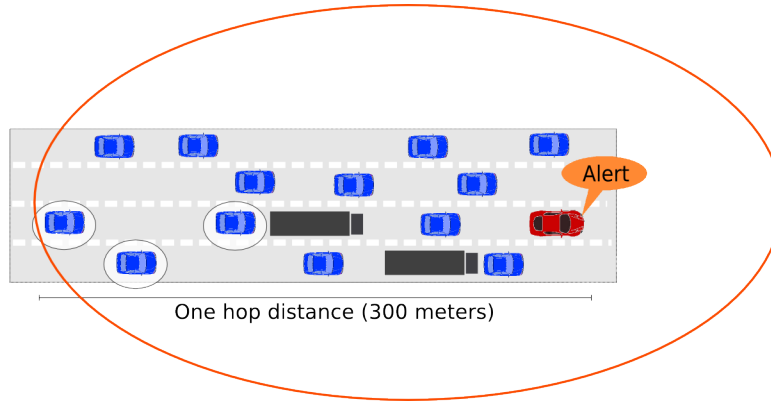


Figure 20: Coverage holes in the broadcast range.

The phenomenon of transmission holes in the broadcast range has been recently considered as a potential cause of message loss in VANETs. In [19, 20] Boban and Tonguz et al. conduct extensive experiments to prove the presence of reception holes in the transmission range. The authors report mobile obstacles (i.e. vehicles), primarily in the LOS, as the major cause of loss in the signal strength resulting in some portions of the broadcast region completely uncovered. The studies show that a single obstacle can cause RSS drop of over 20 dB when two cars communicate at a distance of 10 m; while in the NLOS conditions the chances of successful communication become 90%.

The coverage of transmission holes is thus far dealt in [31, 32]. In [31] Laouiti et al. present Reliable Opportunistic Broadcast in VANETs (R-OB-VAN) algorithm to ensure reliable transfer of safety messages. The authors present three variants of their algorithm

with the third variant being the most reliable. The authors designate each node in the broadcast range as responsible for all other nodes (neighbors) in the broadcast range to ensure reliability of reception. Nodes exchange the entire list of their neighbors by appending this information to the periodic beacon messages. Each node after receiving safety message runs a process of reliability check for all other nodes in the broadcast range and identifies if there is any node in the range that does not include the message sender in its neighbor list. In case there exists such node, it is inferred to be located in a hole and subsequently the message is rebroadcasted for that node. The algorithm creates extra overhead to the existing periodic beaconing messages that use that same control channel primarily intended for safety messages, thus effecting channel contention. Channel contention is also effected due to the fact that the algorithm includes all the one hop neighbors as potential rescuers which can cause excessive contention among the rescuers themselves.

Coverage of nodes located in the transmission holes is a challenging problem in any wireless scenario. The nodes located in the transmission holes are completely oblivious of the activity in the wireless channel. Consequently, the detection of a packet loss becomes challenging considering the limitation of the use of a feedback mechanism in a broadcast scenario. The proposed extension to the NSN technique employs constant observation of the immediate neighborhood by each vehicle. Each vehicle maintains topology information of the entire one-hop range by using the location, speed and direction information received from other vehicles contained in the periodic beacon messages. Upon reception of a safety message, each vehicle verifies whether its immediate neighbors received the recent safety message above the reception sensitivity threshold by estimating received signal strength (RSS) for each of its immediate neighbors. The RSS calculation is based on the topology information by also taking into account the mobile obstacles in the propagation path. Upon detecting a node with message loss either due to interference (detected by NACK reception) or by being located in a hole (detected by the RSS estimation technique), the immediate neighbors of the given node follow sectoring based elimination mechanism to decide a

unique rescuer. Thus, the proposed technique ensures the delivery of the safety-message to every vehicle in the vicinity of a hazard event on the road.

5.2 Negative Acknowledgment with Hole Recovery (NSN-H)

The scenario of recovering safety message in a hole is depicted in Figure 10. Here, three vehicles (encircled white) are assumed as completely oblivious of the original broadcast by node A caused by strong obstacles in their LOS path, these vehicles are termed as nodes in holes. All the remaining vehicles with in the broadcast range successfully receive the safety message. Upon reception of the safety message each receiver node verifies whether or not its immediate neighbors received the recent safety message.

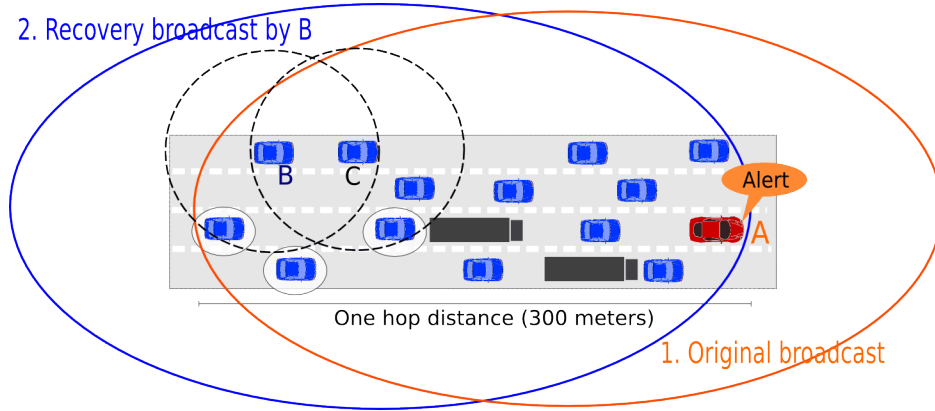


Figure 21: Recovering message loss in a hole using negative-acknowledgment with smart neighborhood.

Each node is already equipped with topology information for the entire broadcast range gathered from periodic beaconing from all the surrounding nodes. The beacons also contain vehicle type information to be used in calculating the vehicle's effect as an obstacle. Additionally, as mentioned earlier, each vehicle is equipped with a digital map and GPS. During the verification phase each node generates the road topography snapshot with vehicles positioned on the map by using their respective location, speed and direction information. Each node can now determine its immediate neighbors and will run the received signal strength

(RSS) estimation for each of its immediate neighbors. RSS is estimated using the angle between the given receiver (immediate neighbor) and the sender (verifier node is aware of the original sender node and its respective location). Any node in the direct LOS path between sender and receiver is counted as obstacle with its impact on the signal loss depending on the its vehicle type [19, 20]. Loss caused by road surroundings and road geometry can also be included for additional accuracy in RSS estimation (e.g., the propositions of [17, 15]).

In Figure 10, for the sake of clearer delineation, the verification process carried by only two nodes B and C is exemplified. Immediate neighborhoods of node B and C are depicted with dashed circles. Both B and C, upon reception of the original safety message from A, execute the RSS estimation for their immediate neighbors. As depicted in the figure, both B and C detect one neighbor each located in a hole i.e., the estimated RSS for the neighbor is below the receiver sensitivity threshold. Therefore, nodes B and C contend to rebroadcast the safety message to cover their respective neighbors located in hole. Here again, the proposed technique ensures unique rebroadcast to avoid collisions and at the same time single recovery for multiple nodes in holes. Therefore, node B and C wait for one complete rebroadcast cycle and then follow the sectoring based rebroadcaster elimination process as described in the recovering the unrecoverable signal case of NSN. Since node B is the furthest node with respect to the original sender, therefore, B rebroadcasts the safety message in its entire transmission range that is overheard by all the three nodes previously present in transmission holes. After receiving the recovery broadcast only receivers with previously scheduled recovery broadcast (only node C in Figure 10) repeat the RSS verification step in order to confirm reception at its previously detected immediate neighbor in hole.

In Algorithm 2, the functioning of the NSN-H technique is summarized. The algorithm builds on the original NSN technique and includes the coverage hole case. Upon the reception of a beacon message, the node updates its list of immediate neighbors. While upon reception of a safety alert the nodes check if the message is a NACK or a new safety alert. In the case of a NACK message, the given node aborts its NACK broadcast (if there was a

NACK scheduled). In the case of a new safety the node schedules its rebroadcast based on its distance from the message sender. The node also computes the received signal strength for its immediate neighbors and schedules a rescue rebroadcast in case the received signal strength is below the receiver-sensitivity threshold rss_{th} . The rescuer node rebroadcasts the safety message in the entire neighborhood upon expiry of the backoff period. The remaining potential rescuers confirm the reception of the safety alert at their immediate neighbors that were located in holes previously and cancel their scheduled rescue rebroadcast.

5.3 Coverage Hole Detection

As described earlier, a node located in a coverage hole is completely oblivious during the broadcast of a safety message. In such a scenario, the reliable coverage of nodes becomes challenging even with the use of a feedback mechanism. Requesting ACK from every receiving node as a confirmation of reception is not feasible in the broadcast scenario. The ACK messages can storm the radio channel resulting in acute collisions.

The proposed hole detection technique relies on the existing information available at each node. The technique uses the location, speed, direction, and vehicle dimensions of all the neighbor nodes in the broadcast range. The required information is received from all the neighbor nodes in the form of beacon messages as part of the IEEE 802.11p specifications. The only additional information contained in the beacon message is the vehicle dimension information that is specific to the proposed technique. The beacon generation frequency for a given vehicle ranges from one message per second to 10 messages per second. Based on the beacon information received from each neighbor the given vehicle calculates the geometric topology of all the vehicles on the road in the broadcast range. The given vehicle determines its immediate neighbors by simply estimating the distance between the given node and the beacon sender. If the node exists at a distance less than or equal to the radius of the immediate neighborhood, the node is considered as an immediate neighbor. The radius of the immediate neighborhood is the area covered by a circle with radius r around a

Algorithm 2 Pseudo-code for the NSN-H algorithm.

```
1 Initialize
2  $R_i \leftarrow$  one-hop transmission range of node  $i$ ;
3  $r_i \leftarrow$  radius of immediate neighborhood of node  $i$ ;
4  $I_i \leftarrow$  set containing nodes in the immediate neighborhood of node  $i$ ;
5  $N_i \leftarrow$  rebroadcast sectors around node  $i$ ;
6  $rs_i \leftarrow$  rebroadcast sector of node  $i$ ;
7  $w \leftarrow$  contention window of each sector;
8  $RS S_i \leftarrow$  estimated received signal strength for node  $i$ ;
9  $rss_{th} \leftarrow$  receiver sensitivity threshold;
10  $H_i \leftarrow$  set containing nodes located in holes detected by node  $i$ ;

11 Event new safety alert message received from node  $s$ 
12 foreach  $n \in R_s$  do
13   if (to_nack = set) then
14     cancel to_nack;
15   else
16     compute  $\|n - s\|$ ;
17     choose  $rs_i$  corresponding to  $\|n - s\|$ ;
18     schedule_rebroadcast with random_backoff  $N_s.w - rs_i.w + random(w)$ ;
19   foreach  $i \in r_n$  do
20     compute  $RS S_i$ ;
21     if ( $RS S_i < rss_{th}$ ) then
22       set to_rescue;
23        $H_n \leftarrow H_n \cup \{i\}$ ;

24 Event new beacon message received
25   compute  $\|n - s\|$ ;
26   if ( $\|n - s\| \leq r_i$ ) then
27      $I_i \leftarrow I_i \cup \{s\}$ ;
28   else if ( $s \in I_i$ ) then
29      $I_i \leftarrow I_i \setminus \{s\}$ ;

30 Event copy of safety alert message received by  $n$  from node  $s$ 
31   if (to_rescue = set) then
32     foreach  $i \in H_n$  do
33       compute  $RS S_i$ ;
34       if ( $RS S_i \geq rss_{th}$ ) then
35         cancel to_rescue;
36          $H_n \leftarrow H_n \setminus \{i\}$ ;

37 Event unrecoverable signal received by node  $i$ 
38   set to_nack;
39   wait for rebroadcast_cycle;

40 Event rebroadcast_cycle expires for node  $i$ 
41   if (to_nack = set) then
42     broadcast nack in  $r_i$ ;
43   else
44     if (to_rescue = set) then
45       broadcast recent message in  $R_i$ ;
```

given node x , such that there exist two nodes y and z , where $r = \|x - z\|$ and $\|x - y\| \leq \|x - z\|$. Additionally, $r \leq \|x - n\|$ for any node n , where $n \neq x \neq y \neq z$. Thus, r is the smallest possible radius around a given node that can house two other neighboring nodes. Thus, each vehicle maintains the geometric topology of the entire one-hop transmission range and maintains a list of its immediate neighbors.

Upon reception of the safety message, a given vehicle verifies the reception of the message at each of its immediate neighbors without the exchange of any additional packets. Since the unsuccessful reception caused by interference is recovered by the basic NSN technique, the verification procedure accounts for detecting the vehicles present in coverage holes. The given vehicle estimates the received signal strength (RSS) for each of its immediate neighbors and determines that a neighbor is located in a coverage hole if the estimated RSS for the neighbor is below the receiver sensitivity threshold.

The RSS estimation is carried in two steps. First, the vehicles obstructing the line of sight between the sender and the given receiver are identified using line segments and rectangles in \mathbb{R}^2 . Second, the signal loss caused by the obstructing vehicles is computed using the multiple-knife-edge-diffraction model.

5.3.1 Determining the vehicles obstructing the line of sight

Each vehicle maintains the geographical topology of the one-hop neighborhood. The topology is maintained in the form of rectangles representing vehicles on a plane in \mathbb{R}^2 . The length and width of a vehicle is exchanged in the beacon messages, along with the height of a vehicle. The height of a vehicle will be considered while computing the signal loss using knife-edge diffraction. A vehicle causing obstruction in the line of sight between the sender and the receiver is determined by testing if an intersection exists between the line segment (joining the sender and the receiver) and the rectangle representing the vehicle in the path.

Let \overline{SR} be the line segment representing the line of sight between the sender and the receiver, and $ABCD$ be the rectangle representing the vehicle in the propagation path. If

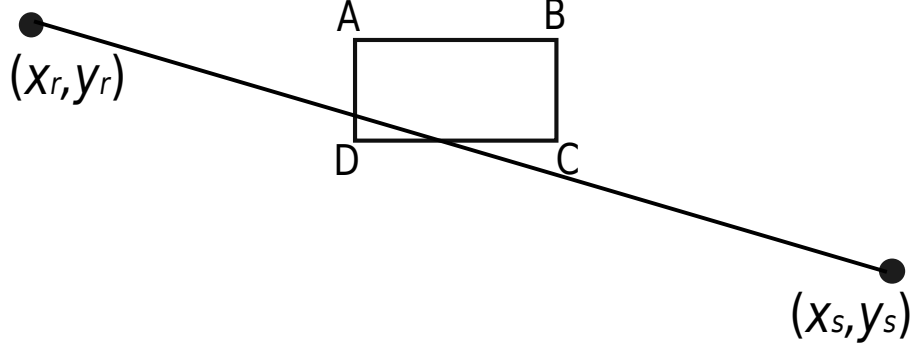


Figure 22: Determining the intersection between a line segment and a rectangle.

the endpoints of the line segment \overline{SR} are (x_s, y_s) and (x_r, y_r) , then a point (x, y) is on the same straight line iff $u.x + v.y + w = 0$ with $u = y_r - y_s$, $v = x_s - x_r$, and $w = x_s y_r - x_r y_s$. The two half planes defined by the line are $u.x + v.y + w > 0$ and $u.x + v.y + w < 0$.

Additionally, it is also ensured that the vehicle (rectangle) lies within the segment of the line between the sender and the receiver, and not at a point on the line beyond the sender or the receiver. To ensure this condition, the \overline{SR} and $ABCD$ intersection verification is performed after the following conditions holds true: $(x_{ob} > x_r \text{ and } x_{ob} < x_s) \text{ or } (x_{ob} < x_r \text{ and } x_{ob} > x_s) \text{ or } (y_{ob} > y_r \text{ and } y_{ob} < y_s) \text{ or } (y_{ob} < y_r \text{ and } y_{ob} > y_s)$, where (x_{ob}, y_{ob}) is the location of the obstacle.

Thus, if $u.v + v.y + w > 0, \forall ABCD$; or if $u.v + v.y + w < 0, \forall ABCD$, there exists no intersection between the line segment \overline{SR} and the rectangle $ABCD$. Therefore, the given vehicle does not obstruct the line-of-sight path between the sender node and the receiver node. The given vehicle is considered as an obstruction otherwise.

5.3.2 Attenuation caused by an obstructing vehicle

After determining that a given vehicle lies in the line of sight between the send and the receiver, the impact of the vehicle on the signal loss is estimated. The attenuation in the radio link increases as vehicles obstruct 60% of the first Fresnel zone between the sender and the receiver. The attenuation is due to the diffraction that depends on the obstruction level, the carrier frequency, the shape of the obstruction, and the amount of the obstruction in the path between the sender and the receiver. We use the multiple knife-edge diffraction model

to estimate the effect of vehicles as obstructions. The prerequisite for the applicability of the knife-edge diffraction model is that the wavelength should be significantly smaller than the size of the obstacle. Therefore, the application of the model in the VANET scenario is reasonable because the DSRC frequency of 5.9 GHz has a wavelength of approximately 5 cm, which is significantly smaller than the size of a vehicle.

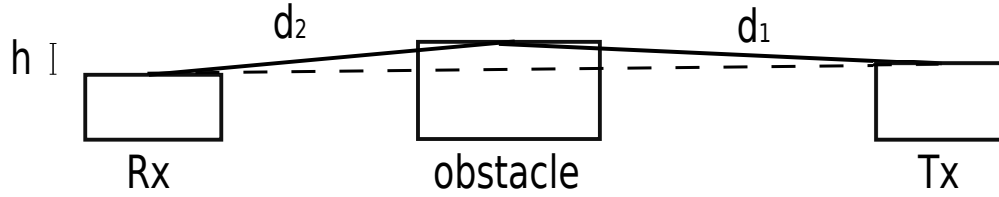


Figure 23: Single knife-edge diffraction between vehicles.

The attenuation is estimated using the knife-edge diffraction model described in the ITU-R recommendation [46]. The scenario is depicted in Figure 23. The obstacle is viewed perpendicular to the radio link between the sender and the receiver vehicles. The approximation of the attenuation (in dB) caused by a single knife-edge obstacle L can be obtained using the following equation:

$$L = \begin{cases} 6.9 + 20 \log[\sqrt{(v - 0.1)^2 + 1} + v - 0.1], & v > -0.78 \\ 0, & \text{otherwise,} \end{cases} \quad (41)$$

where

$$v = h \sqrt{\frac{2}{\lambda} \left[\frac{1}{d_1} + \frac{1}{d_2} \right]}. \quad (42)$$

The extension of the single knife-edge diffraction model to multiple edge obstacles is not immediate. We follow the ITU-R method, where correction factors are added to the attenuation to improve the approximation. The method consists of applying single knife-edge diffraction successively to multiple obstacles, with the top of the preceding obstacle acting as a source of diffraction for the following obstacle. The case of multiple

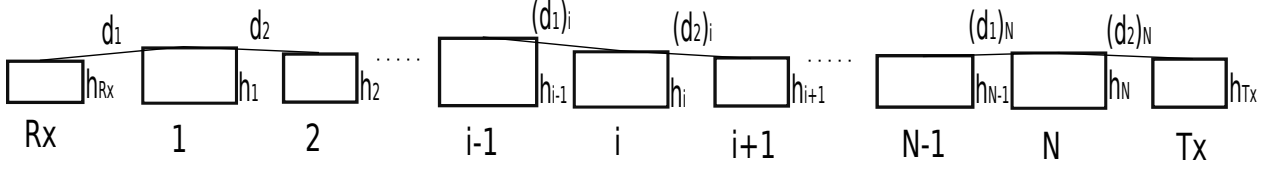


Figure 24: Multiple knife-edge diffraction between vehicles.

obstructions in the line of sight is depicted in Figure 24. The total attenuation caused by multiple vehicles, following the multiple knife-edge diffraction model, is given by

$$L_t = \sum_{i=1}^N L_i + 20 \log C_N, \quad (43)$$

where L_i is the diffraction loss over the i th vehicle, assuming the source to be at the edge of the $(i - 1)$ th vehicle. The function C_N is a correction factor dependent on the parameters shown in Figure 24. The correction factor is given by

$$C_N = \sqrt{\frac{P_a}{P_b}}, \quad (44)$$

where

$$P_a = d_1 \prod_{i=1}^N [(d_2)_i] \left(d_1 + \sum_{j=1}^N [(d_2)_j] \right), \quad (45)$$

$$P_b = (d_1)_1 (d_2)_N \prod_{i=1}^N [(d_1)_i (d_2)_i]. \quad (46)$$

Using the correction factor, the total attenuation caused by the vehicles in the line of sight path is calculated from Equation 43. The attenuation L_t , along with the free-space propagation loss, gives the total path loss between the sender vehicle to the receiver vehicle. The estimated received signal strength becomes

$$RSS = P_{Tx} + G_{Tx} - L_{ld} - L_t + G_{Rx}, \quad (47)$$

where P_{Tx} is the transmitted output power of the transmitter, G_{Tx} is the transmitter antenna gain, L_{ls} is the log-distance path loss, L_t is the diffraction loss in the propagation path, and G_{Rx} is the receiver antenna gain. The vehicle is considered to be located in a coverage hole when the sensitivity threshold is $RSS < -98 \text{ dBm}$ [47].

5.4 Simulation Analysis

5.4.1 Simulation Setup

To analyze the performance of the NACK with smart neighborhood - hole coverage (NSN-H) algorithm, the NSN-H algorithm is fully implemented along with the UMB scheme and the SB scheme in the ns-3 simulator[36]. The traffic mobility is generated using the VanetMobiSim tool [37]. The common simulation parameters are summarized in Table 4. The ns-3 simulator lacks the multi-knife diffraction model, and as part of this work, we have implemented a generic multi-knife edge diffraction for ns-3. The code is in the process of review for submission to the upcoming version 3.16 of the ns-3 simulator.

The simulation implements the three dimensional propagation scenario in detail. Each vehicle is considered with its three dimensions information of height, width, and length. Four different vehicle categories are used with vehicle dimensions as described in Table 5. The simulation uses a four-kilometers of road-length with unidirectional roads in two lanes. Six different vehicle densities are tested with densities from five to 30 nodes per 300 meters length of the road (i.e., the one-hop distance). Vehicles are assigned Gaussian-random speed with a mean of 50 miles per hour and a standard deviation of three miles per hour. The minimum safe headway between the vehicles is kept as 1.5 seconds.

Log-distance path-loss model is used with path loss exponent equal to 3 [21]. The physical channel is characterized in detail using the multi-knife diffraction loss model. The propagation is followed along the entire path between the sender and the receiver. The effect of each vehicle as obstacle along the path is considered. Each vehicle along the path is first evaluated using the obstruction detection technique described in Section 6.3.1, and the attenuation caused by the vehicle is estimated using the knife-edge diffraction model.

Table 4: Simulation parameters for NSN-H evaluation.

Description	Value
Transmission range	300 meters
Data rate	3 Mbps
Message payload size	100 Bytes
Protocol overhead	14 bytes
MAC header size	34 bytes
PHY header size	26 bytes
RTB, CTB, ACK, NACK	20, 14, 12, 10 bytes
Time slot, DIFS, SIFS	20, 50, 10 μs
Road length	4 km (2 lanes, unidirectional)
Vehicle density	2-30 vehicles/300 meters
Vehicle speed	50 miles/h (mean)
Message generation rate	0.01-1 message per vehicle/second
Path loss model	Log-distance path loss model
Diffraction model	Multiple knife-edge diffraction model
Simulation time	100 seconds (each run)

Table 5: Dimensions of vehicles.

Vehicle	Dimensions (meters)		
	Height	Width	Length
Lincoln LS	1.453	1.59	4.925
Pontiac Vibe	1.547	1.763	4.371
Ford E-250	2.085	2.029	5.04
General trailer truck	4.25	2.5	20

To best study the performance of algorithms in the existence of the hidden nodes, the scenario is tested for different message-generation rates of 0.01 to one message per vehicle per second, where one message per vehicle per second has a high likelihood of the hidden nodes at almost every broadcast instance.

5.4.2 Results and Discussion

In Figure 25, the proportion of vehicles with the LOS and NLOS communication is depicted for one-hop neighborhood. The figure shows the average number of vehicles in the line of sight or non-line of sight to the sender with varying distance from the sender. The result depicted in the figure represents the average based on evaluation over varying vehicle density between five nodes and 30 nodes per 300-meter distance of the road. In the

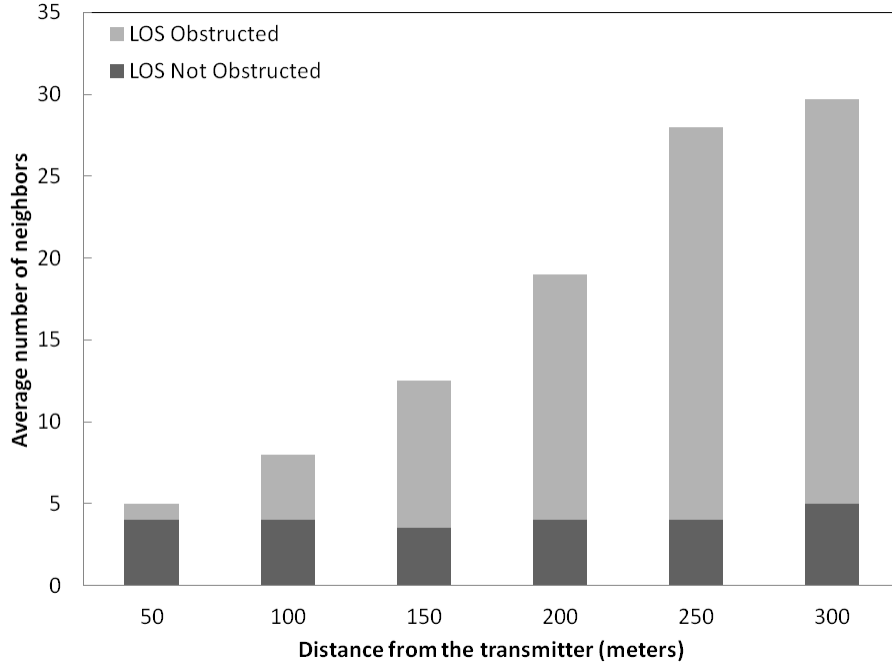


Figure 25: Average number of neighbors with obstructed and unobstructed line of sight.

figure, it is noticed that the ratio of vehicles with unobstructed and obstructed line of sight increases with increasing distance between the sender and the receivers. At a distance of 50 meters, most of the vehicles are in line of sight with the transmitter, and the propagation loss is only affected by the attenuation in the free-space. However, at a distance of 100 meters and beyond, the majority of the receivers are in non-line of sight with the transmitter, which can incur excessive diffraction loss due to vehicles along the path. Therefore, characterizing the physical channel of the vehicular scenario by considering the free-space and the road surrounding objects as the only parameters affecting the propagation can result in inaccurate coverage estimation. Moreover, the non-line of sight path for majority of receivers at farther distances has high likelihood of coverage holes, where a given vehicle fails to receive the safety message.

To further quantify the existence of vehicles as obstacles in the propagation path, the average number of obstacles is depicted against the distance from the transmitter in Figure 26 . The average number of obstacles along the propagation path are shown for three

different node densities. In the figure, the propagation path is mostly a direct LOS at a distance close to the transmitter. However, with increasing distance, in addition to the path being mostly obstructed by the surrounding vehicles, the number of obstructing vehicles also increases. Similarly, increasing the density of traffic has a direct affect on the number of obstructing vehicles. Therefore, at a distance of beyond 200 meters from the transmitter and at a density of 30 nodes per 300 meters, the average number of vehicles acting as obstacles in the propagation path for a given receiver is over eight vehicles. Considering the potential attenuation caused by an obstructing vehicle (depending on the type of the vehicle), there is a high likelihood that a given receiver does not receive the safety message due to excessive attenuation along the path. It is also noted that the effect may be dominant at a farther distance from the transmitter, however, coverage at a closer distance of 100 meters can potentially be effected by excessive attenuation due to vehicles as obstacles. At a close of distance of 100 meters, even though the number of vehicles as obstacles can be four or less, however, larger obstructing vehicles (e.g., a trailer truck) can result in acute attenuation of up to 18 dB per vehicle. Thus, vehicles located at a closer distance to the transmitter are also susceptible to being located in the coverage holes.

In Figure 27, a thorough comparison is presented for the signal reception in the line of sight and non-line of sight path. In the figure, line of sight represents the case where the vehicles are not considered to be causing obstruction and attenuation, while the obstructed case accounts for the average received signal strength (RSS) where the attenuation caused by each vehicle along the propagation path is considered. Since the number of obstacles in the close vicinity of the transmitter are near negligible, the average RSS is almost equal for the two cases in the close vicinity of the transmitter. However, the attenuation due to obstacles is pronounced over farther distances and the difference in the measured signal for the two paths increases with distance. Note that the figure also illustrates the minimum measured RSS for the obstructed path that clearly confirms the notion of holes being present all across the one-hop neighborhood. In other words, even at close distances, there are

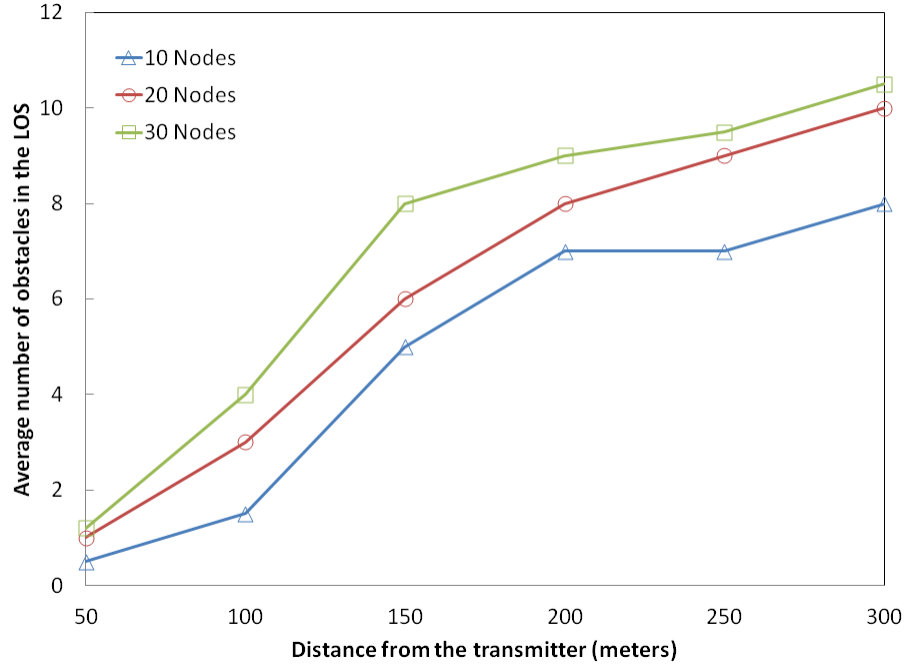


Figure 26: Average number of vehicles as obstacles in the line of sight.

instances where the attenuation caused by vehicles is strong enough to prevent coverage of a particular location in the path. The reason for such an effect, as stated previously, is the type of vehicles obstructing the path. For example, a combination of a trailer truck and smaller vehicles can cause high attenuation even with a few number of vehicles as obstacles in the propagation path. The existence of holes in the broadcast range results in some vehicles being oblivious of a safety message broadcast, and not performing the necessary safety maneuver. Therefore, it becomes indispensable to cover nodes being located in the coverage holes to ensure the critical VANET requisite of reliability of the delivery of the safety message.

Before we present the performance evaluation of the proposed NSN-H algorithm in terms of reliability, a general idea of the radius of the smart neighborhood is presented in Figure 28. The average radius of smart neighborhood is depicted against varying node density. The average radius is presented for three different types smart neighborhoods based on the number of neighbors required. One smart neighbor represents a scenario where each

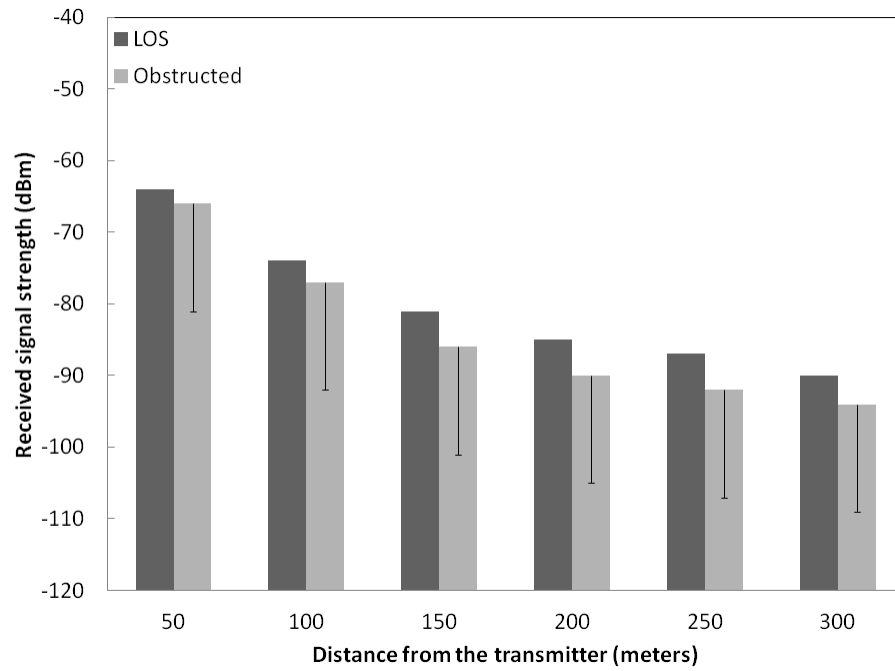


Figure 27: Average received signal strength for the obstructed and unobstructed line of sight.

given vehicle takes care of one other neighbor that is at located closest to the given vehicle. Similarly, two and three smart neighbors represent the case where a given takes care of one and two other neighbors, respectively. In the figure, the radius of smart neighborhood decreases with increasing node density. The radius of smart neighborhood for the three scenarios converges with increasing node density, and in the high-density case of 30 nodes per 300 meters of broadcast range the radius for all the three smart neighborhood scenarios is close to about 20 meters, an optimum range for the idea of collision suppression using confined neighborhood. At lower densities, the large radius of the smart neighborhood (almost half of the radius of the broadcast range for the three smart neighbor scenario) may cause the intended collision suppression using power control to appear less effective. However, the fact of the smaller density of nodes in such a scenario prevents the likelihood of excessive suppressions. This fact is substantiated in the subsequent figures.

In Figure 29, the performance of the proposed NSN-H algorithm is evaluated in terms of the reliability of reception. The average success percentage is presented against varying

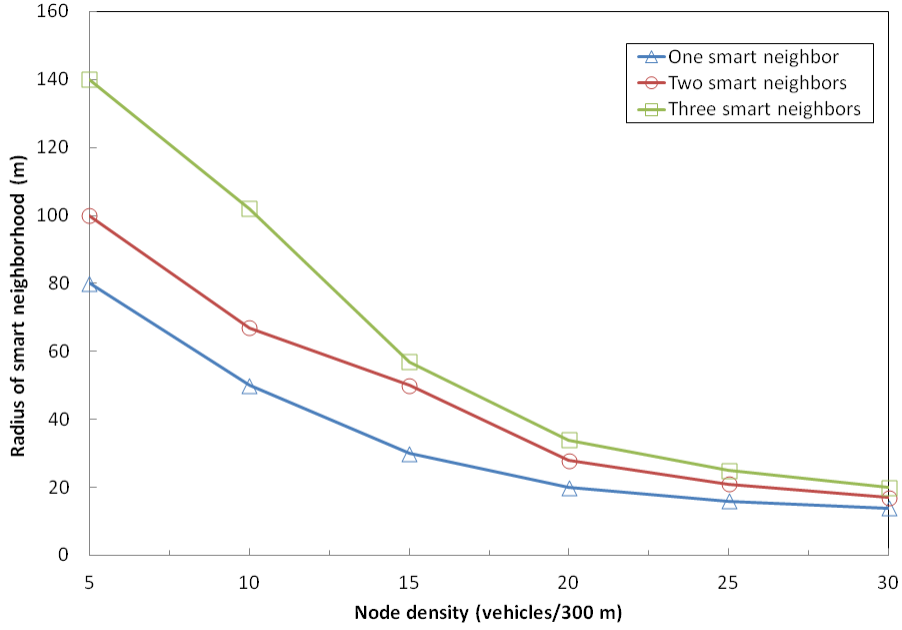


Figure 28: Radius of smart neighborhood with increasing node density.

node density. In the figure, the success percentage is the ratio of the safety packets received successfully and the packets lost. A packet loss is not counted for the node when the node eventually receives the message after a recovery rebroadcast or a forwarding rebroadcast. The packet-loss rate only counts the loss of a safety-message packet, and the overhead and control packets are not considered in the metric.

The reliability of the proposed algorithm is evaluated in comparison with the original NSN algorithm, the R-OB-VAN method, and the UMB method. The simulation considers the vehicles in the propagation path as obstacles and causing attenuation depending on the type of the vehicle. The NSN-H algorithm estimates the received signal strength in the smart neighborhood based on the knowledge exchanged in the periodic beacon messages. At lower node densities, since the propagation path is predominantly line of sight, therefore, the reliability of reception is almost equal for all the four methods under evaluation. As the node density increases, the UMB method falls short in terms of ensuring reliability as the method lacks any specific mechanism for message loss due to collisions or due to the

presence of node in a coverage hole. The R-OB-VAN algorithm offers better reliability due to its recovery method. However, in the density beyond 20 vehicles per 300 meters of road, the reliability decreases resulting from the probabilistic recovery response. Additionally, the R-OB-VAN method lacks a collision avoidance mechanism among multiple contenders of recovery-message broadcast. The lack of collision avoidance mechanism results in further collisions in the high-density traffic. Similarly, the original NSN method performs well until the density of 15 nodes per 300 meters of broadcast range, however, the method lacks support for covering oblivious vehicles located in coverage holes. Therefore, the reliability of the method falls short as the traffic increases, where many vehicles remain uncovered due to their existence in the coverage holes.

The proposed NSN-H method maintains high reliability in Figure 29 even in the high density scenario where coverage holes are highly common. The high reliability of the proposed algorithm is due to the specialized hole-recovery mechanism where every receiver verifies and ensures reception within its confined smart neighborhood. The reliability of the proposed algorithm slightly lowers beyond 25 nodes per 300 meters range. The decrease in the success percentage (although about 1%) is due to the excessive contention among neighbors for initiating a safety broadcast and also among rescuers within the smart neighborhood.

The reliability of the safety-message dissemination algorithms in terms of distance is presented in Figure 30. The figure shows the success percentage against increasing distance from the transmitter. The general trend of the performance is not different from Figure 30 where the success percentage was evaluated against increasing node density. Since the increasing node density and increasing distance from the transmitter have equal likelihood of the occurrence of coverage holes, therefore, the loss generally increases equally for both the parameters. With increasing distance, the number of obstructing vehicles along the propagation path increases causing higher attenuation and the consequent coverage holes. The UMB method falls short in terms of the success percentage with increasing distance

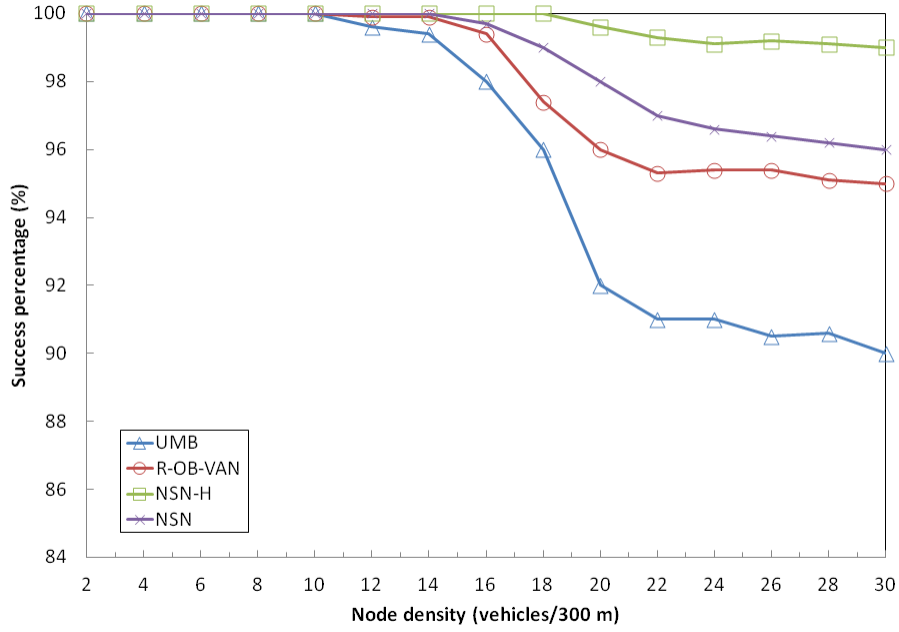


Figure 29: Average success percentage with increasing node density.

due to its lack of the recovery mechanism for a packet loss. The R-OB-VAN method and the NSN original method perform well until half of the broadcast range primarily due to their respective probabilistic recovery mechanism and the NACK feedback mechanism. However, towards the later half of the broadcast range the existence of coverage holes becomes high, and nodes located in the coverage holes remain unable to receive a given safety message. Therefore, the reliability of the two methods slightly drops in the later half of the broadcast range. The proposed NSN-H method, on the other hand, maintains high success percentage throughout the broadcast range with the exception of about a 1.4% drop in the worst scenario at the edge of the broadcast range. The slight decline, as mentioned earlier, is primarily due to the existence of the hidden terminal problem at the edge of the coverage radius.

In Figure 31, the comparison of the four safety-message dissemination algorithms is presented in terms of the delivery delay. Clearly, the UMB method performs best in terms of the average delivery delay. The reason for the higher performance of the UMB method

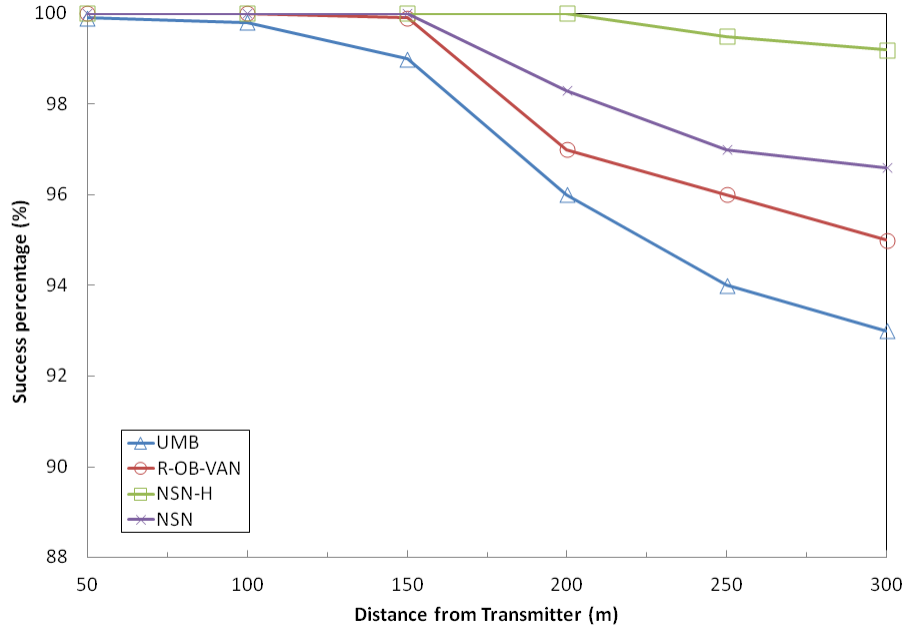


Figure 30: Average success percentage with increasing distance from the transmitter.

is that the algorithm mainly concerns the message propagation without employing any specific mechanism for reliability and collision avoidance. Therefore, the UMB algorithm, though lacking reliability, performs well in terms of message propagation delay with only about 11 milliseconds delay in the highest traffic density. The R-OB-VAN method incurs the highest delay among the three broadcast methods. The excess delay of the R-OB-VAN method is due to the unnecessary rebroadcasts of the probabilistic loss detection and the resultant collisions in the high node density. Moreover, the collisions caused by the recovery-broadcast contenders incurs additional delay due to the the lack of a contention resolution mechanism. The NSN original and the NSN-H methods provide almost an identical delay with about 16.3 milliseconds in the high traffic density. The reason for the identical performance of the two methods in terms of the delay is that the dominant overhead delay for both the methods is the wait time of one rebroadcast cycle before the recovery mechanism. The NSN original method incurs the overhead delay to for its recovery mechanism in case of message loss due to interference, while the NSN-H method

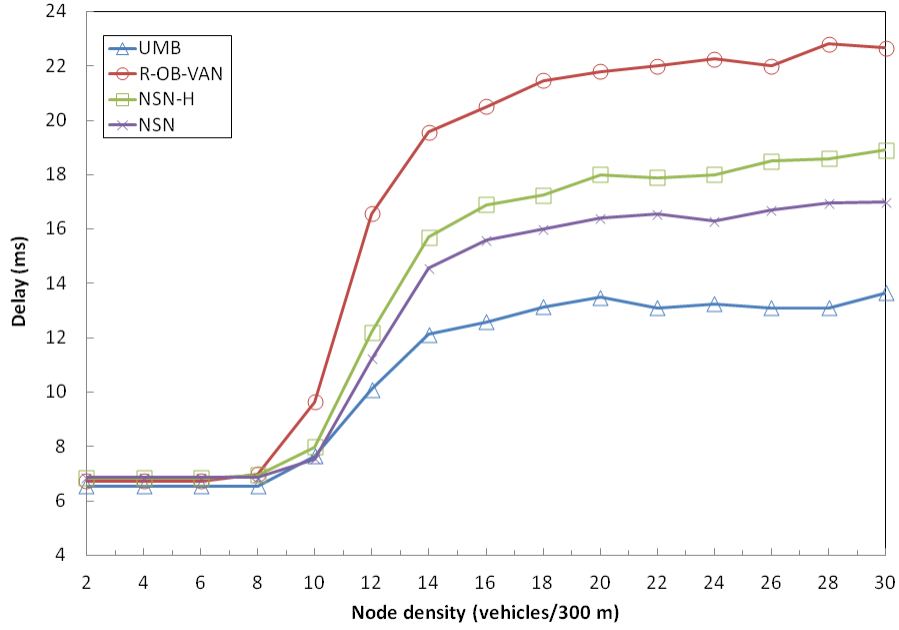


Figure 31: Mean one-hop delay with increasing node density.

being the extension the NSN method incurs the delay for its hole detection and recovery mechanism. The minor extra delay in the NSN-H over the NSN original is due to the detection of coverage holes (predominantly in the high density cases) and the consequent recovery mechanism, where the original NSN method evades the additional wait of one-rebroadcast cycle. Therefore, the NSN-H algorithm offers maximum reliability at the cost of a negligible additional overhead delay of five milliseconds over the delay efficient UMB method.

In this chapter, we have presented the NACK with Smart Neighborhood - Hole Recovery (NSN-H) to ensure reliability in safety-message dissemination in VANETs. We have reused our concept of smart neighborhood where we designate neighbors present in a confined immediate neighborhood to carry the responsibility of ensuring successful reception at each of their corresponding neighbors. The NSN-H technique aims to guarantee the reception of the safety message to all the related vehicles (endangered by an

event) on the road. The reception of a message is ensured through the use of the negative-acknowledgement (NACK) mechanism together with constant observation by the immediate neighbors in the confined smart neighborhood. To ensure the reception of the safety message at vehicles located in the coverage holes, the NSN-H technique employs constant observation of the immediate neighborhood by each vehicle. The given vehicle estimates the received signal strength (RSS) for each of its immediate neighbors and determines that a neighbor is located in a coverage hole if the estimated RSS for the neighbor is below the receiver sensitivity threshold. Upon detecting a node with message loss either due to interference (detected by NACK reception) or by being located in a hole (detected by RSS estimation), the immediate neighbors of the given node follow a sectoring-based elimination mechanism to decide a unique rescuer. Thus, the proposed technique follows message reception at the individual node level and ensures recovery in all potential cases of message loss. A very detailed implementation of the propagation scenario is performed in the ns-3 simulator, and the performance evaluation of the NSN-H algorithm is presented along with three other safety message dissemination algorithms. The simulation results suggest that the NSN-H provides guaranteed reliability at the cost of a negligible overhead delay of about five milliseconds even in the worst traffic-density scenario.

CHAPTER 6

CONCLUSIONS AND FUTURE WORK

In this dissertation, we have investigated the safety-message routing problem in vehicular ad hoc networks. We have contributed four novel techniques for the efficient and reliable routing of safety messages in the vehicular ad hoc network (VANET). The instant-broadcast technique has been proposed to improve the end-to-end dissemination delay. We have presented the lane-based sectoring mechanism for the collision mitigation in the dense-urban traffic scenario. The negative acknowledgment with smart neighborhood (NSN) technique has been presented to ensure the reliability of reception through recovering the packet loss caused by interference. Finally, the negative acknowledgment with smart neighborhood - hole recovery (NSN-H) technique has been presented to provide guaranteed reception of the safety message at each individual node in the VANET. The investigation of the safety message routing in VANET conducted in this research also revealed the significance of hitherto-neglected factors that influence the vehicular network. Significance of the small payload size of the VANET safety message, the effect of road width on the multi-hop relay, and the attenuation caused by vehicles in the propagation path are among some of the important revealed factors.

The instant-broadcast technique has been presented to improve the overall delay. In the instant-broadcast technique, the safety message is propagated without using the handshake mechanism and the related control packets. In case of a collision in the forwarding step, instead of restarting the broadcast, it is proposed that the next contending forwarder rebroadcasts the safety message, thus saving the overhead time of a complex collision-resolution mechanism. An analytical model based on Markov-chain modeling has also been developed for the message-propagation delay in the instant broadcast. Thorough evaluation and comparisons were performed in the ns-3 simulator, and the results demonstrate that the IB method improves the message-propagation speed by a factor of two over the existing

methods while maintaining equal reliability of reception.

We have presented the lane-based sectoring technique for the sectoring of the broadcast range for safety-message communication. The rush-hour-traffic scenario has been considered where most of the hitherto mechanisms are severely affected by collisions and the consequent high message-propagation delays. The hitherto neglected factor of road width is introduced as a second dimension (in addition to the road length) for sectoring the transmission range of the message sender. The collision gain of the proposed technique is evaluated using Markov chains. An extensive simulation evaluation is performed using the ns-3 simulator, and the results suggest that the lane-based sectoring technique reduces the rebroadcast collisions by two percent over the existing sectoring techniques even in the worst-traffic scenario. The results suggest that the lane-based sectoring significantly improves the message-propagation delay by as much as nine milliseconds for the message rebroadcast in each hop.

The negative acknowledgment with smart neighborhood (NSN) technique has been presented to ensure the reliable delivery of safety messages in VANETs. The concept of smart neighborhood is presented where we designated neighbors present in a confined immediate neighborhood to carry the responsibility of ensuring successful reception at their corresponding neighbors. The reception of the message is ensured through the use of negative acknowledgement (NACK) mechanism together with constant observation by the immediate neighbors. Immediate neighborhood is defined as the area around a given node with radius encompassing two (or more if there are more than two nodes present within the two node radius) other neighbors. NACK, unlike in conventional networks, is broadcasted only in the confined smart neighborhood to maintain effective channel utilization. Upon the reception of the NACK message, the immediate neighbors of the given node follow sectoring based elimination mechanism to decide a unique rescuer. The rescuer node rebroadcasts the safety message in the neighborhood and recovers the message loss at the given node. The NSN algorithm outperforms the existing routing methods by over two percent in terms

of the packet-loss rate in the high traffic-density scenario. The NSN technique ensures maximum reliability of reception in the cases where a given node encounters message loss due to interference; however, the technique lacks the support for the cases where a node is located in a coverage hole.

The negative acknowledgment with smart neighborhood - hole recovery (NSN-H) technique has been presented to ensure guaranteed reception of the safety-message among all the vehicles in the desired broadcast range. To ensure the reception of the safety message at vehicles located in the coverage holes, the NSN-H technique employs a constant observation of the smart neighborhood by each vehicle. The given vehicle estimates the received signal strength (RSS) for each of its immediate neighbors and determines that a neighbor is located in a coverage hole if the estimated RSS for the neighbor is below the receiver sensitivity threshold. Upon detecting a node with message loss either due to interference (detected by NACK reception) or by being located in a hole (detected by RSS estimation), the immediate neighbors of the given node follow a sectoring-based elimination mechanism to decide a unique rescuer. Thus, the proposed technique follows message reception at the individual node level and ensures recovery in all potential cases of message loss. A very detailed implementation of the propagation scenario is performed in the ns-3 simulator. The simulation results suggest that the NSN-H provides guaranteed reliability at the cost of a negligible overhead delay of about five milliseconds even in the worst traffic-density scenario.

The potential future work pertaining to this research include the real life testing of the proposed safety-message routing techniques and the investigation of the application of the proposed ideas in the service channels in VANETs. The real life evaluation of the vehicular scenario is a resource intensive campaign that involves a large number of vehicles equipped with 802.11p transceivers travelling in real traffic within the required multi-hop broadcast range of each other. In addition, while simulating a VANET scenario in the existing network simulators and topology generators, a thorough consideration of the vehicular

environment is required for accurate evaluation in scenarios such as in the presence of parallel (service) roads, ramps, interchanges and overhead bridges. Finally, the proposed techniques can be extended for the non-safety traffic in VANETs. As a future work, the extension of the techniques would require further evaluation of the techniques in the service channels for video, voice and Internet traffic that also involves road-side unit as an imperative entity.

REFERENCES

- [1] Y. Toor, P. Muhlethaler, and A. Laouiti, “Vehicle ad hoc networks: applications and related technical issues,” *IEEE Communications Surveys Tutorials*, vol. 10, pp. 74–88, quarter 2008.
- [2] “Intelligent vehicle initiative technology—advanced controls and navigation systems,” in *Proceedings of Society of Automotive Engineers, SAE World Congress*, 2005.
- [3] “Vehicle infrastructure integration 2009,” in *Proof of Concept Report No. FHWA-JPO-09-003* www.intelligdriveusa.org/documents/052009-POC-vehicle-final-report.pdf, 2009.
- [4] “Car 2 car communication consortium,” in <http://www.car-to-car.org/>.
- [5] “Network on wheels project,” in <http://www.network-on-wheels.de/>.
- [6] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, “Vehicular ad hoc networks (vanets): status, results, and challenges,” *Telecommunication Systems*, pp. 1–25. 10.1007/s11235-010-9400-5.
- [7] H. Guo and N. Balon, “Vehicular ad hoc networks and dedicated short range communication,” in *IEEE Global Telecommunications Conference (GLOBECOM)*, 2006.
- [8] M. Bauer, D. Harwood, and K. Richard, “Safety effects of using narrow lanes and shoulder-use lanes to increase the capacity of urban freeways,” in *Transportation Research Board’s Transportation Research Record: Journal of the Transportation Research Board No. 1897*, 2004.

- [9] “Standard specification for telecommunications and information exchange between roadside and vehicle systems 5 ghz band dedicated short range communications (dsrc) medium access control (mac) specifications,” in *ASTM E221303*, 2003.
- [10] “Notice of proposed rulemaking and order fcc 02-302,” in *Federal Communication Commission*, 2002.
- [11] Y. Kudoh, “Dsrc standards for multiple applications,” in *Proceedings of the 11th World Congress on ITS*, 2006.
- [12] D. Jiang and L. Delgrossi, “Global standardization of network and transport protocols for its with 5 ghz radio technologies,” in *Proceedings of the ETSI TC ITS Workshop*, 2009.
- [13] F. Li and Y. Wang, “Routing in vehicular ad hoc networks: A survey,” *IEEE Vehicular Technology Magazine*, vol. 2, pp. 12 –22, June 2007.
- [14] J. Xie, A. Das, S. Nandi, and A. Gupta, “Improving the reliability of ieee 802.11 broadcast scheme for multicasting in mobile ad hoc networks,” *IEE Communications*, vol. 153, pp. 207 – 212, Apr. 2006.
- [15] E. Giordano, R. Frank, G. Pau, and M. Gerla, “Corner: A radio propagation model for vanets in urban scenarios,” *Proceedings of the IEEE*, vol. 99, pp. 1280 –1294, July 2011.
- [16] J. Sobrinho, R. de Haan, and J. Brazio, “Why rts-cts is not your ideal wireless lan multiple access protocol,” in *Wireless Communications and Networking Conference*, vol. 1, pp. 81 – 87 Vol. 1, March 2005.
- [17] J. Otto, F. Bustamante, and R. Berry, “Down the block and around the corner the impact of radio propagation on inter-vehicle wireless communication,” in *29th IEEE International Conference on Distributed Computing Systems*, pp. 605 –614, June 2009.

- [18] L. Cheng, B. Henty, D. Stancil, F. Bai, and P. Mudalige, “Mobile vehicle-to-vehicle narrow-band channel measurement and characterization of the 5.9 ghz dedicated short range communication (dsrc) frequency band,” *IEEE Journal on Selected Areas in Communications*, vol. 25, pp. 1501 –1516, Oct. 2007.
- [19] R. Meireles, M. Boban, P. Steenkiste, O. Tonguz, and J. Barros, “Experimental study on the impact of vehicular obstructions in vanets,” in *IEEE Vehicular Networking Conference (VNC)*, pp. 338 –345, Dec. 2010.
- [20] M. Boban, T. Vinhoza, M. Ferreira, J. Barros, and O. Tonguz, “Impact of vehicles as obstacles in vehicular ad hoc networks,” *IEEE Journal on Selected Areas in Communications*, vol. 29, pp. 15 –28, January 2011.
- [21] B. Blaszczyszyn, P. Muhlethaler, and Y. Toor, “Performance of mac protocols in linear vanets under different attenuation and fading conditions,” in *12th International IEEE Conference on Intelligent Transportation Systems*, pp. 1 –6, Oct. 2009.
- [22] X. Yang, L. Liu, N. Vaidya, and F. Zhao, “A vehicle-to-vehicle communication protocol for cooperative collision warning,” in *First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services*, pp. 114 – 123, Aug. 2004.
- [23] R. Santos, R. Edwards, A. Edwards, and D. Belis, “A novel cluster-based location routing algorithm for inter-vehicular communication,” in *15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, vol. 2, pp. 1032 – 1036 Vol.2, Sept. 2004.
- [24] R. Santos, A. Edwards, and O. Alvarez, “Towards an inter-vehicle communication algorithm,” in *3rd International Conference on Electrical and Electronics Engineering*, pp. 1 –4, Sept. 2006.

- [25] G. Korkmaz, E. Ekici, F. Özgüner, and U. Özgüner, “Urban multi-hop broadcast protocol for inter-vehicle communication systems,” in *Proceedings of the 1st ACM International Workshop on Vehicular Ad hoc Networks, VANET '04*, (New York, NY, USA), pp. 76–85, ACM, 2004.
- [26] E. Fasolo, A. Zanella, and M. Zorzi, “An effective broadcast scheme for alert message propagation in vehicular ad hoc networks,” in *IEEE International Conference on Communications*, vol. 9, pp. 3960 –3965, June 2006.
- [27] M. Li, W. Lou, and K. Zeng, “Oppcast: Opportunistic broadcast of warning messages in vanets with unreliable links,” in *IEEE 6th International Conference on Mobile Adhoc and Sensor Systems*, pp. 534 –543, Oct. 2009.
- [28] J. Thriveni, B. Ashwini, A. Latha, K. Sandhyashree, G. Prakash, A. Alice, K. Venugopal, and L. Patnaik, “Dual covered broadcast with negative acknowledgements for enhanced reliability in mobile ad hoc networks,” in *IEEE Region 10 Conference (TENCON)*, pp. 1 –6, Nov. 2008.
- [29] N. Wisitpongphan, O. Tonguz, J. Parikh, P. Mudalige, F. Bai, and V. Sadekar, “Broadcast storm mitigation techniques in vehicular ad hoc networks,” *IEEE Wireless Communications*, vol. 14, pp. 84 –94, Dec. 2007.
- [30] K. Ibrahim, M. Weigle, and M. Abuelela, “p-ivg: Probabilistic inter-vehicle geocast for dense vehicular networks,” in *69th IEEE Vehicular Technology Conference (VTC)*, pp. 1 –5, Apr. 2009.
- [31] A. Laouiti, P. Muhlethaler, and Y. Toor, “Reliable opportunistic broadcast in vanets (rob-van),” in *9th International Conference on Intelligent Transport Systems Telecommunications, (ITST)*, pp. 382 –387, Oct. 2009.

- [32] F. J. Ros, P. M. Ruiz, and I. Stojmenovic, "Acknowledgment-based broadcast protocol for reliable and efficient data dissemination in vehicular ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 11, pp. 33–46, Jan. 2012.
- [33] Q. Xu, T. Mak, J. Ko, and R. Sengupta, "Vehicle-to-vehicle safety messaging in dsrc," in *Proceedings of the 1st ACM International Workshop on Vehicular Ad hoc Networks*, VANET '04, (New York, NY, USA), pp. 19–28, ACM, 2004.
- [34] G. Bianchi, "Performance analysis of the ieee 802.11 distributed coordination function," *IEEE Journal on Selected Areas in Communications*, vol. 18, pp. 535–547, mar 2000.
- [35] P. Chatzimisios, A. Boucouvalas, and V. Vitsas, "Packet delay analysis of ieee 802.11 mac protocol," *Electronics Letters*, vol. 39, pp. 1358 – 1359, Sept. 2003.
- [36] "The ns-3 network simulator (ns-3.9)." <http://www.nsnam.org/>, 2011.
- [37] Haerri., Fiore., Fethi., and Bonnet, "VanetMobiSim: generating realistic mobility patterns for VANETs." <http://vanet.eurecom.fr/>, 2006.
- [38] F. Khan, Y. Chang, S. Park, and J. Copeland, "Handshaking vs. instant broadcast in vanet safety message routing," in *Proceedings of IEEE PIMRC'11*, pp. 709–714, 2011.
- [39] K. F. Turnbull, "Houston managed lanes case study: The evolution of the houston hov system," *US Department of Transportation, Federal Highway Administration*, Sept. 2003.
- [40] D. Krajzewicz and C. Rossel, "Simulation of Urban MObility (SUMO)." <http://sumo.sourceforge.net/index.shtml>, 2007.
- [41] "Traffic and Network Simulation Environment (TraNS)." <http://lca.epfl.ch/projects/trans>, 2011.

- [42] M. Torrent-Moreno, D. Jiang, and H. 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, VANET '04*, (New York, NY, USA), pp. 10–18, ACM, 2004.
- [43] X. Ma and X. Chen, “Delay and broadcast reception rates of highway safety applications in vehicular ad hoc networks,” in *2007 Mobile Networking for Vehicular Environments*, pp. 85 –90, May 2007.
- [44] X. Ma, X. Chen, and H. Refai, “On the broadcast packet reception rates in one-dimensional manets,” in *IEEE Global Telecommunications Conference (GLOBECOM)*, pp. 1 –5, 30 2008-Dec. 4 2008.
- [45] X. Ma, J. Zhang, and T. Wu, “Reliability analysis of one-hop safety-critical broadcast services in vanets,” *IEEE Transactions on Vehicular Technology*, vol. 60, pp. 3933 –3946, Oct. 2011.
- [46] Piorkowski., Raya., Lugo., Papadimitratos., Grossglauser., and Hubaux., “Propagation by diffraction).” Recommendation ITU-R P.526-12, 2012.
- [47] U. technology corporation, “802.11p dsrc communication unit by unex corporation - data sheet.” OBE-102 data sheet, 2012.
- [48] G. Yan, W. Yang, M. Weigle, S. Olariu, and D. Rawat, “Cooperative collision warning through mobility and probability prediction,” in *IEEE Intelligent Vehicles Symposium (IVS)*, pp. 1172 –1177, June 2010.
- [49] M. Rudack, M. Meincke, K. Jobmann, and M. Lott, “On traffic dynamical aspects of inter vehicle communications (ivc),” in *IEEE 58th Vehicular Technology Conference*, vol. 5, pp. 3368 – 3372 Vol.5, Oct. 2003.

- [50] M. Durresi, A. Durresi, and L. Barolli, "Emergency broadcast protocol for inter-vehicle communications," in *Proceedings of 11th International Conference on Parallel and Distributed Systems*, vol. 2, pp. 402–406, July 2005.
- [51] K. Xu, M. Gerla, and S. Bae, "How effective is the ieee 802.11 rts/cts handshake in ad hoc networks," in *IEEE Global Telecommunications Conference*, vol. 1, pp. 72–76 vol.1, Nov. 2002.
- [52] Y.-T. Yang and L.-D. Chou, "Position-based adaptive broadcast for inter-vehicle communications," in *IEEE International Conference on Communications Workshops*, pp. 410–414, May 2008.
- [53] O. Tonguz, N. Wisitpongphan, F. Bai, P. Mudalige, and V. Sadekar, "Broadcasting in vanet," in *Mobile Networking for Vehicular Environments*, pp. 7–12, May 2007.
- [54] M. Booyesen, S. Zeadally, and G.-J. van Rooyen, "Survey of media access control protocols for vehicular ad hoc networks," *IET Communications*, vol. 5, pp. 1619–1631, 22 2011.
- [55] M. Hallenbeck and M. Rice, "Vehicle volume distribution by classification," in *69th IEEE Vehicular Technology Conference (VTC)*, Apr. 2009.
- [56] F. Khan, Y. Chang, S. J. Park, and J. Copeland, "Introducing lane based sectoring for routing in vanets," in *Wireless Communications and Networking Conference (WCNC), 2012 IEEE*, pp. 3040–3044, april 2012.
- [57] F. Khan, Y. Chang, S. Park, and J. Copeland, "Towards guaranteed safety message delivery in vehicular ad hoc networks," in *Proceedings of IEEE Globecom'12*, pp. –, 2012.