# NETCODE: AN XOR-BASED WARNING DISSEMINATION SCHEME FOR VEHICULAR WIRELESS NETWORKS

NIAZ MORSHED CHOWDHURY

SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF
*Doctor of Philosophy*

SCHOOL OF COMPUTING SCIENCE

COLLEGE OF SCIENCE AND ENGINEERING
UNIVERSITY OF GLASGOW

JANUARY 2016

**Abstract**

The next generation of vehicles will be equipped with automated Accident Warning Systems (AWSs) capable of warning neighbouring vehicles about hazards that might lead to accidents. The key enabling technology for these systems is the Vehicular Ad-hoc Networks (VANET) but the dynamics of such networks make the crucial timely delivery of warning messages challenging. While most previously attempted implementations have used broadcast-based data dissemination schemes, these do not cope well as data traffic load or network density increases.

This problem of sending warning messages in a timely manner is addressed by employing a network coding technique in this thesis. The proposed NETwork COded DissEmination (NETCODE) is a VANET-based AWS responsible for generating and sending warnings to the vehicles on the road. NETCODE offers an XOR-based data dissemination scheme that sends multiple warning in a single transmission and therefore, reduces the total number of transmissions required to send the same number of warnings that broadcast schemes send. Hence, it reduces contention and collisions in the network improving the delivery time of the warnings.

The first part of this research (Chapters 3 and 4) asserts that in order to build a warning system, it is needful to ascertain the system requirements, information to be exchanged, and protocols best suited for communication between vehicles. Therefore, a study of these factors along with a review of existing proposals identifying their strength and weakness is carried out. Then an analysis of existing broadcast-based warning is conducted which concludes that although this is the most straightforward scheme, loading can result an effective collapse, resulting in unacceptably long transmission delays.

The second part of this research (Chapter 5) proposes the NETCODE design, including the main contribution of this thesis, a pair of encoding and decoding algorithms that makes the use of an XOR-based technique to reduce transmission overheads and thus allows warnings to get delivered in time.

The final part of this research (Chapters 6–8) evaluates the performance of the proposed scheme as to how it reduces the number of transmissions in the network in response to growing data traffic load and network density and investigates its capacity to detect potential accidents. The evaluations use a custom-built simulator to model real-world scenarios such as city areas, junctions, roundabouts, motorways and so on. The study shows that the reduction in the number of transmissions helps reduce competition in the network significantly and this allows vehicles to deliver warning messages more rapidly to their neighbours. It also examines the relative performance of NETCODE when handling both sudden event-driven and longer-term periodic messages in diverse scenarios under stress caused by increasing numbers of vehicles and transmissions per vehicle. This work confirms the thesis' primary contention that XOR-based network coding provides a potential solution on which a more efficient AWS data dissemination scheme can be built.

**Acknowledgements**

I would like to express my gratitude to Dr. Lewis Mackenzie, my principal supervisor, for his relentless guidance and encouragement throughout this doctoral research. I never had the opportunity to properly appraise him of how thankful I am; but today I like to take the opportunity to speak my heart out. To me, he has always been a mentor, guide and advisor since I first approached him showing my interest to pursue doctoral study under his supervision. We had spent hundreds of hours discussing the nature of the problem and its potential solutions, and on every occasion he was an excellent critic of my work and always directed me towards the right goal with his valuable comments and feedback. It has truly been a pleasure and privilege working with him, and I would like to continue this journey even after finishing my study.

I would also like to thank my co-supervisor Dr. Colin Perkins for all the interesting and challenging discussions we had over the past four years. It is, in fact, him who directed me towards the network coding approach and kept me motivated saying that the pair of encoding and decoding algorithm would be the key in my doctorate and I must demonstrate my rigour and passion in designing them. I am extremely grateful to him for bringing the best out of me by his critical comments and suggestions.

I am thankful to Scottish Government and Scottish Research Council for giving me the opportunity to pursue this PhD by awarding the Scottish Overseas Research Students Award (SORSA) Scholarship as well as the University of Glasgow for providing me with the College of Science and Engineering Scholarship.

My heartfelt thanks go to Dr. Md. Sadek Ferdous and Dr. Farida Chowdhury for being a family when my wife and I were in desperate need of it in a country where we just moved in. I would specially like to thank Dr. Soumyadeb Chowdhury and Dr. Ashkan Tousi for all the memorable days we worked together in the School of Computing Science and evenings we spent in the Gilchrist Postgraduate Club of the university. I am also very thankful to my sister in law Sarah Alam Shoilee, who herself is on the lookout for a doctorate in future, for proofreading the thesis with such a short notice.

I would like to offer my sincere gratitude to my parents Nurul Alam Chowdhury and Parveen Jahan Chowdhury who have always been my motivation and inspiration in life. I particularly would like to mention my mother who raised my sister and me in a difficult world after the sudden death of my father without giving us the slightest indication of how cruel and harsh the world could be at time. My special thanks also go to my sister Humayra Tasnuva Chowdhury and her husband Towhid Kibria, my father and mother in law Md. Shah Alam and Nurunnaher Begum, my brother in law Nafis Ibn Alam and other members of my family for their constant support throughout this doctoral study.

Last but not the least, I am blessed to have Abrunnaher Shifa, my beloved wife, as my life-partner. She had to move with me to Scotland soon after our marriage as I commenced my doctoral study in Glasgow and to my great surprise, she adapted with the new life very quickly. Despite being young in age and far from the family, she showed great courage and strength to take all the stress, anxiety and anxiousness off my shoulder. I must admit that this journey would not have been possible without the loving and caring support she provided me constantly. On this occasion, I would like to properly thank her for being with me regardless of all my insane, deranged and crazy behaviours I demonstrated in last four years.

This acknowledgement, however, would not be completed if I do not mention one last name. In the middle of freezing scottish nights when the whole world seemed to be finding happiness in sound sleep inside the soft duvet, I continued working on my doctoral research with my special companion who used to take the stress away from me with all her cuddling behaviours; she is our cat *April*.

*To my parents*
Nurul Alam Chowdhury, NDC
Parveen Jahan Chowdhury

# Table of Contents

# List of Tables

# List of Figures

# Chapter 1

# Introduction

> "We are just an advanced breed of monkeys on a minor planet of a very average star. But we can understand the Universe. That makes us something very special."
>
> ***Stephen Hawking***
> *(TED talk: Questioning the universe)*

The next generation vehicles will be equipped with many sophisticated functionalities. A working group[1] of the International Standards Organization (ISO) developing standards for those vehicles are standardising the functionalities vehicles must have in future [6, 7]. One of those functionalities will be automated collision avoidance system to warn neighbouring vehicles about potential accidents. These systems are commonly known as Accident Warning System (AWS) and Vehicular Ad-hoc Networks (VANETs) are considered to be one of the potential networks to host and run them on the vehicles [8].

Key to the success of any warning system is timely delivery of warning messages to the neighbouring vehicles. It is particularly important because these systems operate in real-time and any delay clearly makes them vulnerable. Previous warning systems were never evaluated against a delay representing the phrase *timely* and therefore a grey area remained unexplored. This thesis uses the two-second rule [9, 10, 11] that suggests a driver should ideally stay at least two seconds behind any moving vehicle as a reference and argues that AWSs should maintain a warning delivery queuing delay at least smaller than this threshold to be able to deliver warnings in a timely manner.

The timely delivery of warnings is, however, challenging due to the dynamics of the VANET. In order to cope with this challenge, most previous protocols attempting to build accident

[1] WG 14 Vehicle/Roadway Warning and Control Systems working group.

warning system have used broadcast-based data dissemination schemes for delivering warnings to vehicles. This is motivated by the fact that broadcast offers flexible network restructuring and operates based on local knowledge that are keys to design network protocol in VANETs. Nevertheless, in spite of being the first choice for warning delivery in AWS, broadcast demonstrates a serious vulnerability when data traffic load or network density significantly increases. This is due to the fact that wireless networks are inherently asynchronous so as to avoid potential collisions in concurrent transmissions. When any two nodes in these networks inadvertently try to transmit at the same time, a collision occurs with both nodes requiring to back-off. If the number of node increases or nodes try to transmit excessive data, stiff competition between nodes for accessing the medium becomes inevitable. Continuation of this conduct results in contention and excessive collisions in the network that generate broadcast storms and ultimately slow down data delivery.

AWS sends two different types of warning: standard warnings to warn vehicles about potential collisions and aftereffect cautions to avoid further collision. The former are sent periodically and have the ability to exhaust the network capacity. If that happens, it is likely to affect not only its own type but also the latter warning triggered after any specific event. It is therefore necessary to design a warning delivery scheme that follows the principle of broadcast to cope with VANET but also does not push the network to the point of suffering from a delay longer than the two-second threshold.

As the accident warning system is a new concept, many researchers have been trying to design their own systems without having any specific requirement analysis. This thesis, after examining existing warning systems along with possible scenarios and potential accident types, presents a detailed analysis of the requirements in Chapter 3. These requirements are later fulfilled while designing the new system proposed in the current thesis. Understanding the weakness of existing broadcast schemes and how and when those exhibit vulnerability is also important to know before attempting to solve the problem above. Therefore, an analysis of previously used warning systems from the three broad categories of broadcast schemes is conducted in Chapter 4. This chapter also includes development of a mobility model designed based on Glasgow City Centre and all warning systems are tested in a natural urban scenarios. This evaluation involves real vehicle rate, direction and traffic movement that can be found on roads in the Glasgow City Centre area.

The problem of sending warning messages in a timely manner is addressed by employing a network coding technique that disseminates multiple warnings together. This approach does not reduce the rate of periodically sent warnings but by making a reduced number of transmissions it effectively reduces collision and ultimately delivery time. Chapter 5 presents the design of a coding-based data dissemination scheme along with a prototype of an accident warning system. Later by performing simulated experiments, Chapter 6 demonstrates that how this scheme performs better than broadcast-based schemes in response to growing traffic

load and network density.

Finally, the main objective of sending the warning rapidly and timely is to prevent accident. Performance evaluation of the newly proposed warning dissemination scheme cannot be tested properly until real accident scenarios are involved in the investigation. Keeping this in mind, Chapter 7 and 8 present accident oriented evaluation to test proposed coding-based scheme alongside broadcast schemes in response to predetermined incidents.

## 1.1 Thesis Statement

The broadcast-based data dissemination in accident warning system is not suitable because this approach extends the warning delivery process as data traffic load or network density increases. It is shown in the earlier part of this thesis how broadcasting affects such systems by scrutinising the effect of network density and data traffic load on the network in the context of warning systems. Several performance evaluation studies argued that this problem can be solved with the help of full knowledge of the network or by reducing the traffic load. However, neither of these techniques are useful for accident warning system. The reason being, this cooperative system operates with the help of local knowledge and a regular flow of warning messages is necessary to keep neighbouring vehicles informed about the presence of the host vehicle and subsequently any potential incident that it might cause or be involved in.

Nevertheless, it is argued in this thesis that to overcome these limitations of the existing data dissemination schemes and make timely delivery of the warning message, network coding can play an important role. Therefore, this thesis asserts that:

**T1** The XOR-based network coding provides a potential solution on which a data dissemination scheme can be built, a solution that helps reduce the warning delivery time without restricting the regular flow of warning messages. This can be achieved by optimising the number of transmissions in the network. Being cooperative in nature, accident warning systems regularly disseminate warning messages that produce a warnings flow on the road. Intermediate vehicles in multi-hop VANET send these warnings to vehicles ahead or behind. While performing this operation, vehicles potentially can optimise the number of transmission by encoding a message coming from the behind with a message that arrived from the front and sending them together in one transmission.

**T2** Information about the two-hop neighbourhood can play a pivotal role in designing an encoding algorithm that picks packets in such an order so that receivers can decode them without requiring to wait for long. If a vehicle gets to know who are the neighbours

of its neighbours, it can easily identify those who are not connected directly, a finding that potentially helps the vehicle portioning the network into two subsets, one in front and another at the rear. Members of those subsets are aware of the transmissions made within their subset but unaware of any transmission in the other subset. Being the linking node of those two subsets, when a vehicle encodes packets taking one from each, receiver vehicles easily decode it using the packet available at their disposal.

**T3** The performance of the warning delivery can be improved further in regard to event-driven messages if a priority queue is maintained at the network layer of each vehicle. This queue would authorise any event-driven message to bypass the periodic messages in the packet queue for expedited delivery.

## 1.2 Research Objectives

The central goal of this thesis is to design a data dissemination scheme capable of making timely delivery of warning messages to detect potential accidents. In order to achieving this goal, the following six core research objectives are systematically formulated.

**RO1–Requirements Survey:** The objective is to identify and gather the requirements of an empirical warning system. An in-depth survey on the requirements along with a review of the existing proposals identifying their strength and weakness should be helpful for the future studies.

**RO2–Anatomising Existing Systems:** The objective is to anatomise the existing warning systems operate with broadcast-based data dissemination schemes with a view to explore their ability to comply with the two-second rule. Three warning systems from three broad categories of broadcasts will be picked to scrutinise their performances.

**RO3–XOR-based Warning Dissemination:** Having identified the shortcomings of the broadcast based data dissemination schemes in course of achieving the RO2, the objective at this phase is to derive with a proposal that seeks to improve the performance of the accident warning systems in VANET.

**RO4–Analysis of Warning Transmissions:** Having accomplished the RO3, the objective here is to evaluate the performance of this new scheme concerning transmissions related metrics.

**RO5–Analysis of Periodic Warning Message Dissemination:** The objective at this phase is to analyse the performance of the proposed scheme concerning periodic warning message as to how effectively they keep neighbouring vehicles informed about the presence of the host vehicle and how this information is later materialised to detect potential accidents.

**RO6–Analysis of Event Driven Message Dissemination:** The objective is to analyse the performance of event driven message dissemination by the proposed scheme. It also aims to establish the claim made in the thesis statement that priority-based warning dissemination can be effective, particularly in regard to event driven message.

## 1.3 Contributions

This thesis aims to solve the problem of delivering warning messages to neighbouring vehicles in a timely manner. The potential contributions of this thesis are in three folds:

- A comprehensive survey, first of its kind in the context of warning system, is presented that identifies the requirements of a practical and realistic system. In addition to the comparative study concerning existing systems, it also identifies supplementary devices, different scenarios, possible collisions and required messages to deal with those collisions.
- An in-depth longitudinal study of the performance of various existing warning systems operating with three broad categories of broadcast schemes is carried out with a view to observe the effects of network density and data traffic load on the network.
- A pair of encoding and decoding algorithm designed based on an original idea developed in course of this research that if two-hop neighbourhood information is used to create a partition amongst commuting vehicles and subsequently encode two warnings amongst the respective sides, the decoding process can be performed without having to wait for further warning arrival.
- NETCODE, a network coding based data dissemination scheme is proposed that makes timely delivery of warnings to the neighbouring vehicles by employing XOR-based network coding technique at network layer.

## 1.4 Thesis Outline

**Chapter 2:** It provides a comprehensive literature review on background and explains important topics such as vehicular ad hoc networks, medium access control algorithms, network coding and so on.

**Chapter 3:** It presents a requirements survey based on an in-depth study on the existing systems.

**Chapter 4:** It provides an analysis on the broadcast schemes and investigates their performance in relation to growing traffic load and network density.

**Chapter 5:** It presents the proposed warning dissemination scheme, encoding and decoding algorithms and its operation.

**Chapter 6:** It evaluates the performance of the newly proposed scheme concerning transmission related metrics.

**Chapter 7:** It evaluates the proposed scheme with a view to scrutinise its performance based on the periodic warning message.

**Chapter 8:** It evaluates the proposed scheme with a view to scrutinise its performance based on the event-driven message.

**Chapter 9:** It concludes the thesis showing that how the thesis statement is proven in course of the studies conducted throughout this thesis. It also discusses possible future directions could have been established based on the work accomplished in this thesis.

# Chapter 2

# Background

This chapter is written towards a twofold objective: to describe the context of the work carried out in this thesis, and to explain the background information required to understand the subsequent chapters. This thesis investigates a problem related to Accident Warning Systems (AWSs) as to how vehicles would be able to disseminate warning messages in a timely manner to detect potential collisions or prevent post-collision catastrophes. As AWSs use wireless networks to disseminate their warnings, it is relevant to provide with an ambiance of wireless technologies and how those networks are developed over time. This chapter, therefore, starts off with a brief history of wireless communications giving a chronological commentary on their development.

A type of ad hoc networks, or more specifically Vehicular Ad hoc Network (VANET), is used in this research to establish communications between vehicles. This network uses a MAC protocol commonly known by the name of its standard: *IEEE 802.11p*. The development of an AWS relies on these technologies as it operates alongside or over them; thus a rounded discussion on their characteristics and operational behaviour becomes imperative. This is presented with a focus on the recurrently changing topology of the network and how it controls the wireless medium for the purpose of data transmission.

Finally, this chapter provides with a review on the topic of *Network Coding*, the concept used in developing the proposed warning system in this thesis. Network Coding is a vast area developed over the period of last one and half decade. It is difficult to cover everything in a compact review; thus only relevant areas covering wireless networks are considered.

The rest of the chapter is organised as follows: Section 2.1 presents a brief history of wireless communication, Section 2.2 introduces different types of wireless ad hoc networks, Section 2.3 elaborately discusses the architecture, characteristics and applications of VANET, Section 2.4 unfolds the operation of IEEE 802.11 transmission and medium access control, Section 2.5 presents a comprehensive commentary on the network coding, encoding-decoding technique and its applications before the chapter concludes in Section 2.6 with a summary.

## 2.1 A Brief History of Wireless Communications

Wireless communication is one of the fastest growing industries in the modern world where explosive growth of devices with wireless capabilities introduces new scope for building futuristic applications every year. Cellular and satellite systems, wireless local area networks and sensor network based smart monitoring systems are some instances of wireless communication that can be frequently seen in our everyday life.

Although this technology looks like a modern invention but in reality wireless communication traces back its root to the late nineteenth century when scientists and researchers from different parts of the world investigated the problem of sending information from one point to another without having to use a physical medium. In 1891, the Croatian scientist Nikola Tesla used wireless power transmission to light several vacuum tubes from a distance [12]. One year later, Bengali scientist Jagdish Chandra Bose (photographed in figure 2.1[1]) used gunpowder to create an electromagnetic wave that remotely rang a bell [13]. The experiments of Tesla and Bose established the fact that communication over a wireless medium is not impossible.

Wireless communication finally became reality in 1895 when Italian scientist Guglielmo Marconi successfully transmitted the three-dot Morse code for the letter 'S' over a distance of three kilometres using electromagnetic wave [14]. This simple experiment holds huge significance in human history as it was the first occasion when individuals formally communicated with each other without using a tangible communication medium. In 1901, Marconi successfully demonstrated his *Wireless Telegraph* system to the world by transmitting radio signals across the Atlantic Ocean from Cornwall, England to St John's, Newfoundland (present day Canada), covering more than 1,700 miles [15]. Few months later, during the Anglo-Boer war in South Africa, Royal Navy first used wireless telegraphy to communicate amongst ships in Delagoa Bay. Shipping industry has been one of the major clients of wireless communication ever since and by the time the Titanic issued its radio distress calls in 1912, wireless became a standard for shipping [14]. Over the period of next few decades world experienced rapid enhancement in wireless technology. In 1920, first radio news program was broadcast from Detroit, Michigan. Five years later in 1925, Scottish inventor and one of the former students of the University of Glasgow John Logie Baird demonstrated the transmission of moving silhouette images in London. This invention later pioneered the development of modern Television. Few years later in 1931 US inventor Glenn Watson tested Radioteletype (RTTY) [16] and within a short span of time Short Wave (SW) and Frequency Modulation (FM) was also developed that added extra significance in radio communication by enhancing its capabilities.

[1] According to Imperial Copyright Act 1911 of the United Kingdom, this photograph is in the public domain.

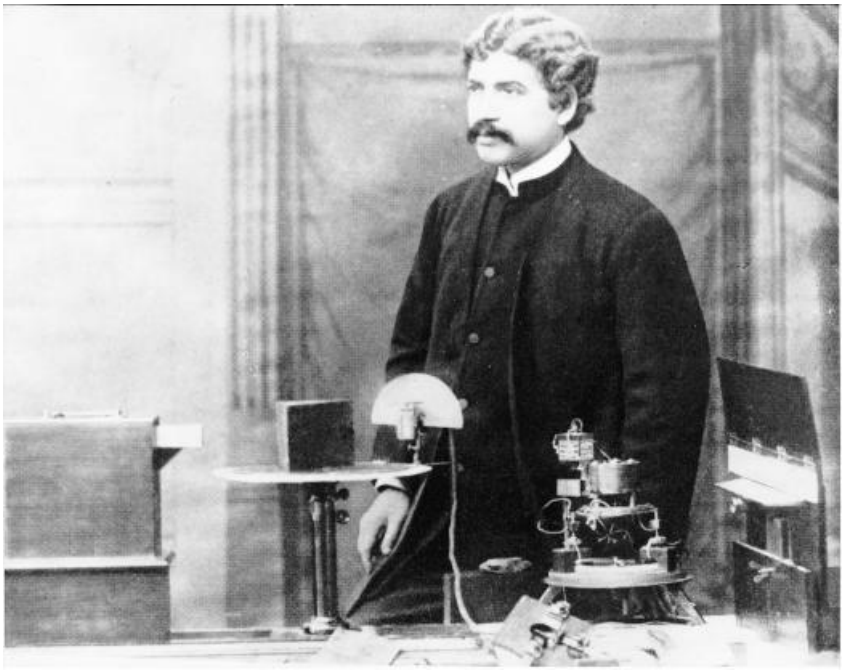


Figure 2.1: Famous Bengali scientists and one of the pioneering figures of wireless communication Sir Jagadish Chandra Bose at the Royal Institution in London, England in January 1897; two years after his demonstration of ringing bell in Calcutta, West Bengal.

Wireless communication entered into its modern era during 1970s when Norman Abramson and his fellow researchers at the University of Hawaii invented the ALOHAnet, a communication network to connect universities located on Hawaiian Islands. ALOHAnet utilised single-hop wireless packet switching and a multiple access solution for sharing a single channel. The success of ALOHAnet soon triggered widespread interest in different direction of computer communications including development of the Ethernet [17]. During the same period Defence Advanced Research Projects Agency (DARPA) launched a project called Packet Radio Network (PRNET) to develop a packet wireless network for military applications. PRNET had the capability of multi-hop wireless communication and could operate over a large geographical area. It incorporated Career Sense Multiple Access (CSMA) to access the shared radio channel. It was designed to self-organise, self-configure and detect radio connectivity for the dynamic operation of a routing protocol without any support from fixed infrastructure. Few years later in 1980s, a working group of the Internet Engineering Task Force (IEFT) was formed to standardise the protocols and functional specifications of wireless ad hoc networks. This group are called Mobile Ad hoc Network (MANET); who are still working with a vision to provide improved standardised routing functionalities to support self-organising mobile ad hoc networks.

The period between 1982 and 1992 was a golden era for wireless communication as world has experienced some magnificent inventions during this period. Although Ethernet was first introduced in 1972 to transfer data at a speed of 2.94 Mbps, it is in 1983 when a standard

for Ethernet was developed and IEEE 802.3 was proposed as the standard for this protocol. In 1990, L-band radio, underlying technology of Global Positioning System (GPS) was first demonstrated. The following year on 1 July, after a long ten-year research, first GSM call was made in Finland by the Finnish prime minister Harri Holkeri using Radiolinja Networks [18]. Same year precursor of Wi-Fi was developed by NCR Corporation in Netherlands up to a speed of 1-2 Mbps. In 1997 Wi-Fi became standard as IEEE 802.11 with a maximum bandwidth of 2 Mbps that was further enhanced as IEEE 802.11b in 1999 with a maximum bandwidth of 11 Mbps and IEEE 802.11g in 2003 with a maximum bandwidth of 54 Mbps. During this period Bluetooth was also developed and became a standard in 1999 when specification of Bluetooth 1.0 or IEEE 802.15.1 was released. In 2004 Wi-MAX came into being as IEEE 802.16 standard [19].

## 2.2 Wireless Ad hoc Networks

Wireless ad hoc networks are decentralised computer networks using radio frequency channel as their physical communication medium. Although this is a modern invention but multi-hop relaying, the underlying principle of ad hoc networking, can trace back its root to 500 B.C. when Darius I of Persia introduced an innovative communication system to send message from the capital to the remote provinces of his kingdom. According to this system, messengers used to sit on tall structures and shout to convey message to another messenger. This system was 25 times faster than regular messengers available at that time. Later this kind of ad hoc voice communication was frequently used in many ancient societies with a string of repeaters of drums, trumpets and horns [15].

Ad hoc networks, with the assistance of wireless technologies, mimic the above ancient conventions and produce one of the most popular wireless networking approaches of current time. In an ad hoc network, as shown in figure 2.2, participating nodes broadcast information which can be received by other nodes available within their transmission range. Due to the fact that nodes do not rely on an infrastructure, these networks can be formed quickly without having to spend much effort or money; hence the name ‘ad hoc network’ [15].

Figure 2.2 presents an example showing an ad hoc network with 5 nodes and its possible routing options. In this example, the purple node located at the very bottom is sending data to the green node located at the top of the image. A multi-hop path is shown using solid lines passing through the red and the orange nodes. There are other possible alternative paths available that connect the purple node with the green one. Those possible options are also shown using broken lines.

Ad hoc networks can be of different kinds and sizes. For example, Wireless Mesh Networks (WMNs) are a type of ad hoc network that are formed with a view to provide an alternative

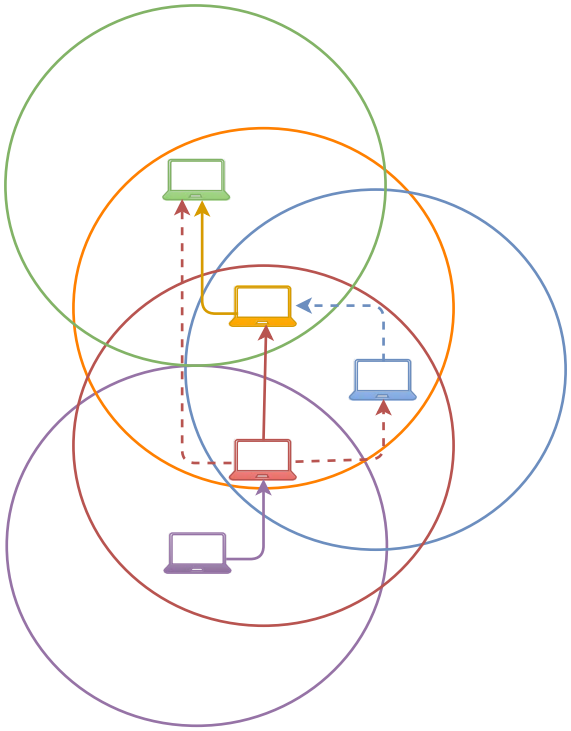


Figure 2.2: An ad hoc network with 5 nodes.

communication framework for mobile or fixed nodes without the spectrum reuse constraints. This network can employ full mesh topology by connecting nodes with every other nodes or partial mesh that connects nodes with a subset of nodes of the network. The Wireless Mesh Networks potentially provide highly economical data transfer capability coupled with freedom of mobility [20]. On the other hand, Wireless Sensor Networks (WSNs) are a special category of wireless network that provide a wireless communication platform amongst the sensors deployed in a specific application domain. Sensor nodes are tiny devises with ability of sensing physical parameters, processing the data and communicating over the network to the monitoring centre. A sensor network is basically a collection of a large number of such nodes deployed in a particular region [21, 22].

Mobile Ad hoc Networks (MANETs), another type of wireless ad hoc network, are self-organised autonomous network systems consisting of mobile nodes and capable of moving without the need of a wired infrastructure-based backbone [23, 24, 25]. A MANET node can be defined as a device with IEEE 802.11 physical and medium access control (MAC) interface. These nodes can roam around freely within a specific range because of their wireless functionalities. Nodes' ability to move in MANET brings new challenges as it influences network topology to change frequently and unpredictably. Unlike traditional wired network, each MANET node acts as a router; and discovers and maintains routes for themselves as well as for other members of the networks [15].

## 2.3 Vehicular Ad hoc Networks

The process of embedding communication technologies in vehicles started many years ago in the form of integrating satellite phone, cellular-based internet access point, in-car bluetooth adapter and so on. These technologies were always treated as add-on services for the on-board passengers and never intended to consider the vehicle as a participating member of a network service. A direct communication between vehicles or vehicle to infrastructure is a relatively new demand that stimulates the development of a new type of ad hoc network called Vehicular Ad hoc Network (VANET) [26].

### 2.3.1 Architecture

VANET is a subset of Mobile Ad Hoc Networks (MANETs) that holds the basic characteristics of the latter networks mentioned earlier. Nevertheless, it is also surprisingly different than MANETs in many aspects. This contradictory posture of VANET gives it a unique place amongst the ranks of wireless ad hoc networks.

VANETs are specially designed for the Intelligent Transportation System (ITS) that uses short-range wireless communication protocol IEEE 802.11p. The operating frequency of VANET is the 5.9 GHz band that the Federal Communication Commission (FCC) allocated for Licensed Dedicated Short Range (LDSR) communication in the United States and the European Telecommunications Standards Institute allocated for Intelligent Transportation System in Europe [27, 28]. The *p* version of the 802.11 MAC protocol is particularly designed with a view to reduce latency and enhance bandwidth of networks operating in a vehicular environment compared to other versions of the protocol. It is likely to be standardised in the next generation vehicles in coming years [29].

VANET can be classified into two broad categories. Vehicles communicating with other vehicles is called V2V communication. A pure V2V architecture does not rely on infrastructures and capable of operating standalone. However, inclusion of infrastructures in the network is beneficial as this can provide with complementary information such as traffic or weather condition; or create backbone for accessing the world wide web. Road Side Units (RSUs) are small fixed infrastructures located beside the roads and connect commuting vehicles with the backbones. RSUs are normally connected with themselves and other large infrastructures using wired networks with high data transfer capabilities. When VANETs incorporate infrastructures in its operation, it is called V2I communication. Some vehicular ad hoc networks make the use of V2V and V2I separately in the same network. Such architectures are often denoted as V2X. Moreover, large infrastructures such as communication towers, cloud data centre etc. communicate with themselves using both wired and wireless medium and sometime informally called I2I communication. Figure 2.3 demonstrates a

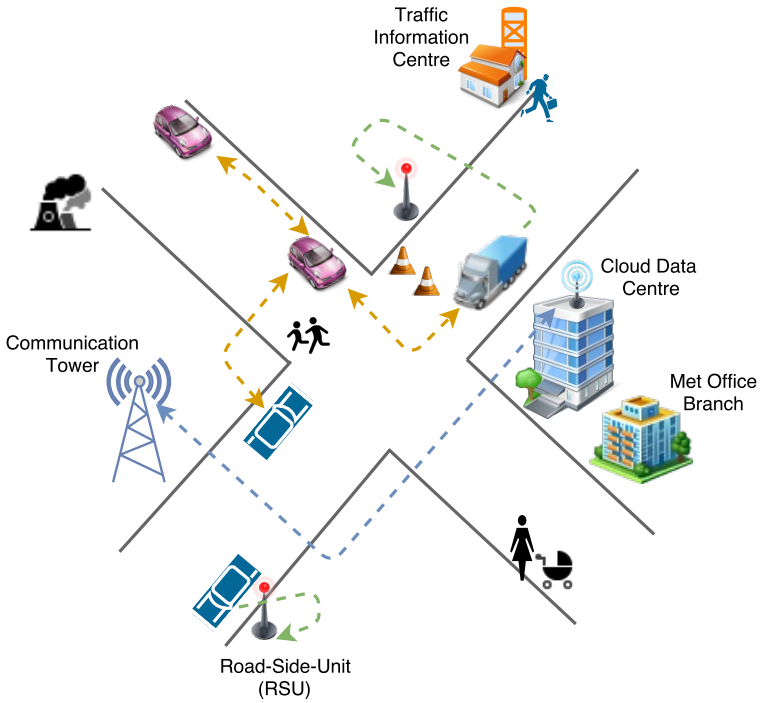



Figure 2.3: A VANET where Vehicles and Infrastructures are in operation. V2V communications are shown using orange lines, V2I using green lines and I2I using blue lines.

glimpse of VANET and its components in a single image.

### 2.3.2 Characteristics

The VANET exhibits some unique characteristics that are predominantly different than mobile ad hoc networks. For example, it covers potentially large scale regions such as city or motorways; and unlike MANETs, it does not have a power constraint. It also functions in a variable network density that changes depending on the roads [30].

It is, however, the topology that differentiates between MANET and VANET most. VANET's recurrently changing topology is affected by the high relative speeds of the vehicles and these rapid changes make it strenuous to govern nodes in the network [31, 32, 33]. The VANET also fragments very quickly and frequently despite having a high data rate deployment. [34, 35] showed that it happens because of VANET's connectivity that relies on the scenarios and vehicles move away from one scenario to another swiftly.

Another notable attribute that VANET holds is its small effective network diameter. The rapid changes in topology and connectivity cause many paths to get disconnected before they can be fairly utilised. [36] studied the effect of network diameter in vehicular environment and indicated that applications requiring to establish unicast and multicast path are mostly affected due to this property.

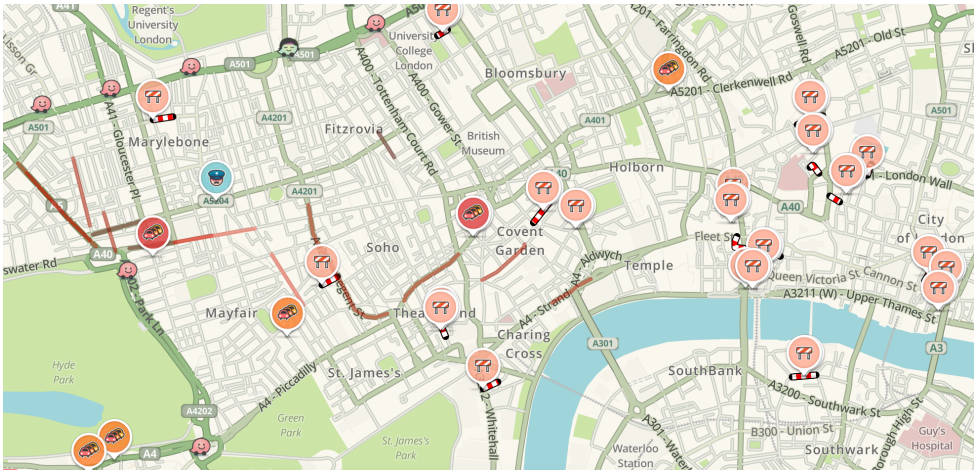



Figure 2.4: Live update with road closure, police check-post and commuter information of the City of London on the Boxing Day night 2015 at 22.00. This information is presented by *Waze*, a very popular traffic information application that received (as of 26 December 2015) 4.5 star ratting out of 5 from 4,264,564 voters on the android app store 'Google Play'.

### 2.3.3 Applications

There are demands for a number of interesting and desired VANET applications for both V2V and V2I. [37] arranged these applications into four broad categories: a) Safety applications, b) Commercial applications, c) Convenience applications; and d) Productive applications.

Amongst these four categories, safety applications produce potential accident and collision warnings as well as road safety notifications. These applications mostly rely on the cooperative nature of the network and sometime make the use of RSU to gather information of recent accidents or dangerous weather condition from police and weather office websites. Commercial applications, on the other hand, provide with entertainment services such as music and video contents, web access, digital map download etc.

Convenience applications in VANETs demonstrate futuristic ideas as this category includes cruise controlling, platooning, road works alert and traffic congestion information. Cruise control has already become a common feature in modern vehicles and platooning will follow this trend in upcoming next generation vehicles. There are also a number of innovative smart phone based applications that provide congestion and road works alert. For example, *Waze* is one of those applications that becomes very popular amongst the drivers because of its live presentation of traffic related information on an interactive map as shown in figure 2.4.

The last category is called 'productive' because these futuristic applications help commuters maintain a sustainable productivity. This category includes applications built for fuel and time utilisation as well as smart commuting to increase 'green footprints'. There are also some applications in this category that function with electric vehicles to assist with charging and improving 'green' energy contents in the battery.

## 2.4 IEEE 802.11: Medium Access Control

The Accident Warning System (AWS) proposed in this thesis uses IEEE 802.11p as its underlying physical and MAC layer protocol. The design choice of the proposed warning system requires knowledge on how the underlying protocol attempts to access medium and makes successful transmissions. It is, therefore, essential to have a review of the medium access control mechanism of the IEEE 802.11 that this section takes the opportunity to discuss. The following review is devised based on the revised standard published by IEEE in 2012 [38].

### 2.4.1 The Protocol

The IEEE 802.11 is an evolving family of specifications for wireless local area networks (WLANs). These specifications establish communications between computers and portable devises in the 2.4, 3.6 and 5 GHz frequency bands. All the 802.11 specifications use the Ethernet protocol and Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) algorithm for sharing wireless medium. The original modulation used in 802.11 was phase-shift keying (PSK) but alternative schemes, such as complementary code keying (CCK), are used in some of the newer specifications. The newer modulation methods aim to provide higher data rate and reduced vulnerability to interference.

The 802.x protocols are designed to embody both physical and MAC layers and 802.11 is no different. The latest standard of 802.11 defines a single MAC with three different physical layers namely Frequency Hopping (FH) Spread Spectrum in the 2.4 GHz band, Direct Sequence (DS) Spread Spectrum in the 2.4 GHz band and the InfraRed. It might sound irony that the protocol makes ad hoc networks function is designed based on a cellular architecture. In the design of IEEE 802.11, the system is subdivided into cells where they are called Basic Service Set (BSS) and controlled by a Base Station called Access Point (AP). Sometime two or more interconnected BSSs sharing the same network name form an Extended Service Set (ESS). It is possible to have a wireless LAN with just a single cell without an AP. However, generally installations are formed by multiple cells where APs are connected through backbones, such as wired networks.

### 2.4.2 Basic Access Method: CSMA

The 802.11 MAC defines two different access methods namely the Distributed Coordination Function (DCF) and the Point Coordination Function (PCF). Amongst these two, DCF is considered as the basic access mechanism. It is a Carrier Sense Multiple Access with Collision Avoidance mechanism (CSMA/CA). CSMA protocols are well-known in the in-

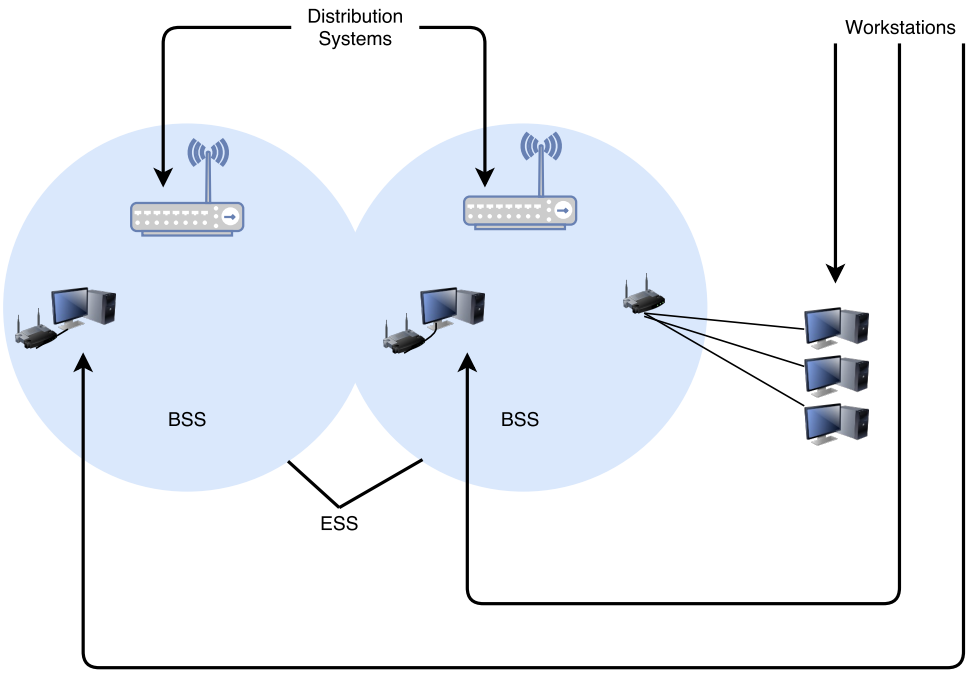



Figure 2.5: An example of IEEE 802.11 service set with two Basic Service Sets (BSSs) forming an Extending Service Set (ESS).

dustry and one of its most popular examples is the Ethernet (which is a CSMA protocol with collision detection mechanism).

The operational steps of a CSMA protocol are as follow: A station intending to transmit data senses the medium first. If the medium is found busy, it indicates that some other station is transmitting at that moment. This makes the intending station to defer its transmission to a later time. However, if the medium is sensed free, the station goes ahead with the transmission. CSMA protocols are effective when the medium is not heavily loaded as it allows stations to transmit with minimum delay. But there is always a chance that multiple station might simultaneously sense the medium and if found free, they could transmit at the same time causing a collision. In event of a collision, it is necessary that the MAC layer detects the collision to retransmit the data with a view to minimise the potential delay occurring due to retransmissions make by the upper layers. In the Ethernet, this collision is identified by the transmitting stations which go into a retransmission phase based on an exponential random backoff algorithm.

Despite the fact that the collision detection mechanism is very effective in wired networks, it does not seem to be very useful in wireless environment mainly because of two reasons. Firstly, implementing a collision detection mechanism would require implementation of a full duplex radio capable of transmitting and receiving at once. This is an approach that would increase the price significantly. Secondly, in a wireless environment we cannot assume that all stations are hearing each other, which is the basic assumption of the collision

detection scheme. Moreover, a station sensing the medium free does not necessarily mean that the medium is free around the receiver area [39].

In order to overcome these two problems, the 802.11 uses a Collision Avoidance (CA) mechanism together with a Positive Acknowledge scheme. According to this method, a station willing to transmit senses the medium first. If the medium is found busy then it defers. However, if the medium is found free for a specified time (called Distributed Inter Frame Space or simply DIFS), then the station is allowed to transmit. Upon receiving data, stations perform Cyclic Redundancy Check (CRC) on the received data and sends an acknowledgement. This acknowledgement informs the sender station about the fact that no collisions occurred. However, if the sender does not receive the acknowledgement then it retransmits the fragment until it receives an acknowledgement or the fragment is thrown away after a given number of retransmissions.

### 2.4.3 Virtual Carrier Sense

In order to reducing the probability of two stations colliding together because they cannot hear each other, the standard defines a Virtual Carrier Sense mechanism. It is noted that this mechanism is introduced by the standard explicitly for the wireless networks keeping the phenomenon in mind that such networks can have *hidden* stations.

According to this mechanism, a station willing to transmit data first transmits a short control packet. In the standard this packet is called 'Request To Send' or simply RTS, which includes the source, the destination and the duration of the round trip transaction. If the medium remains free, destination station responds with a response control Packet called 'Clear To Send' or simply CTS which includes the same duration information. All stations receiving either the RTS and/or the CTS, set their Virtual Carrier Sense indicator (called Network Allocation Vector or NAV) for the given duration, and use this information together with the Physical Carrier Sense when sensing the medium.

This mechanism reduces the probability of a collision on the receiver area by a station that is hidden from the transmitter to the short duration of the RTS transmission because the station hears the CTS and reserves the medium as busy until the end of the transaction. The duration information on the RTS also protects the transmitter area from collisions during the transmission of the acknowledgement. It is noted that as RTS and CTS are short frames, the mechanism also reduces the overhead of collisions.

### 2.4.4 Exponential Backoff Algorithm

The 'Backoff' is a well known method used to resolve contention between different stations willing to access the medium. This method is implemented with the help of four delays called Inter Frame Spaces (IFSs). These IFSs play pivotal role in granting access to the medium and a quick narration would help understanding the algorithm well. Therefore, before explaining the algorithm, a brief introduction to those four different IFSs are presented here.

The 802.11 standard defines 4 types of IFSs:

1. **SIFS:** 'Short IFS', is used to separate transmissions belonging to a single dialogue. The value is a fixed value for individual physical layer and calculated in such a way that the transmitting station will be able to switch back to receive mode and be capable of decoding the incoming data. On the 802.11 FH physical layer, this value is set to 28 microseconds.

2. **PIFS:** 'Point Coordination IFS', is used by the Access Point (or Point Coordinator, as called in this case), to gain access to the medium before any other station. This value is SIFS plus a *Slot Time*[2], i.e 78 microseconds.

3. **DIFS:** 'Distributed IFS', is the IFS used for a station willing to start a new transmission, which is calculated as PIFS plus one slot time, i.e. 128 microseconds.

4. **EIFS:** 'Extended IFS', is a longer IFS used by a station that has received data but could not understand it. This is essential to prevent the station from colliding with a future transmission belonging to the current dialogue.

The *Exponential Backoff*[3] algorithm requires each station to choose a random number $n$ between 0 and a given number and waits for this number of slots before accessing the medium, always checking if a different station has accessed the medium before. This method must be executed in the following cases: a) When the station senses the medium before the first transmission of a data frame and finds the medium busy, b) After each retransmission and c) After a successful transmission. The only case when this mechanism is not used is when the station decides to transmit a new data frame and the medium has been free for more than a DIFS.

[2]The *Slot Time* is defined in such a way that a station will always be capable of determining if another station has accessed the medium at the beginning of the previous slot. This reduces collision probability by half.

[3]The *Exponential Backoff* means each time the station chooses a slot and happens to collide; it will increase the maximum number for the random selection exponentially.

| A | B | A⊕B |
|---|---|---|
| False | False | False |
| False | True | True |
| True | False | True |
| True | True | False |

Figure 2.6: The binary XOR operation has the above truth table.

## 2.5 Network Coding

The Network Coding (NC)[4] is an evolving research area having the potential to build compelling applications in the networking systems [40]. This technique allows intermediate nodes to send packets as linear combinations of previously received data. There are two principal benefits that can be achieved using network coding approach. Firstly, it potentially improves the throughput of the network and secondly, it helps achieving high degree of robustness [2]. As network coding plays a very important role in the design the proposed Accident Warning System (AWS), this section makes an effort to present an instant primer on this technique. The following parts of this section focus on what network coding is, what it does and how it does that, particularly from the wireless network's perspective.

### 2.5.1 Network Coding Principle

The modern communication networks operate based on the fundamental principle that independent streams of data can share network resources but information enclosed inside the streams remain separate. The streams can be packets delivered over the Internet or mobile phone signals on a GSM network but they are treated similarly; just like vehicles on the roads being transported as if commuting over the highways. The way each vehicle remains separate entity on the highway and reaches its destination independently, data streams also find their ultimate terminus. All network functionalities including routing, error control and data storage are administrated based on this principle [1].

Network coding breaks this convention by proposing that instead of only forwarding data, intermediate nodes may recombine multiple incoming packets into one or more outgoing packets. The fundamental principle of network coding is straightforward: While sending

[4] 'Network Coding' was proposed by Ahlswede et al. in their seminal paper in the IEEE Transaction on Information Theory in July 2000.

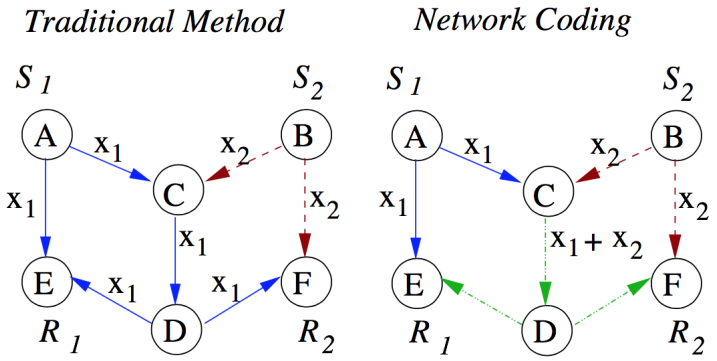



Figure 2.7: A classic example of the use of network coding to improve multicast flow in wired networks. This example was presented in many publications and books including [1, 2, 3].

packets, a node encodes multiple packets together using 'exclusive or' (XOR) operation and sends one or more combined packet(s).

This XOR operation follows the boolean principle presented in figure 2.6 which is zero for same binary representation (0-0 or 1-1) and 1 for other two combinations (0-1 and 1-0). This principle gives a useful outcome that is materialised in the network coding technique. If two elements are combined using XOR operation, one of them can be retrieved back by performing XOR operation on the resultant product and the remaining element. For example, $A = 10101$ and $B = 11000$ are two binary streams. $A \oplus B$ would give us $R = 01101$. Now, if we perform $R \oplus A$, we get B and vice versa. This principle can be further extended for $N$ number of streams such that an element can be retrieved from a resultant product provided that $N - 1$ elements are in hand.

Figure 2.7 shows a classic example of improving multicast network flow that had been presented in the literature by many publications and books while describing network coding technique [1, 2, 3]. This example demonstrates a butterfly network with two stations (typically, this example represents a wired network) S1 and S2 multicast to both R1 and R2. The links have capacity of unit 1. By implementing the network coding i.e. applying XOR operation on the data on link CD, the achievable rates become 2 for each source. This is equal to the rate each destination could achieve by using the network for its sole purposes. However, without the use of network coding, when both destinations jointly use the network, each could achieve a rate of maximum 1.5 unit.

### 2.5.2 Applications

The most well-known application of network coding is improving throughputs. This benefit is obtained using efficient packet transfers or in other words by sending more information in less transmissions. The butterfly example shown earlier in figure 2.7 is the most famous case

of demonstrating how throughput benefit is achieved in multicast network using network coding. This is, however, not the only case where this technique can play an important role. Ho et. al. showed that even in unicast network throughputs can be enhanced provided that at least two unicast streams are in operation [2]. Later other works also backed this claim by improving unicast flow using network coding [41, 42].

Wireless networks are one of the largest territories where network coding is utilised effectively such as for disseminating information, streaming live contents, sharing files etc. [43, 44, 45]. Nevertheless, its application is not limited to transmission of data only and one of the salient issues of wireless network, robustness to packet loss, can also be addressed and subsequently improved using network coding. Although the conventional way of ensuring successful delivery of a packet is to send acknowledgement followed by retransmission of the packed in event of loss. Arguably this approach is made famous by the Transmission Control Protocol (TCP) that later motivated many new protocols to adapt it. An alternative to this is channel coding applied by the source node that introduces a degree of redundancy in the packet in such a way that if a subset of it is received by the receiver node, full data can be recovered [46, 47, 48].

In addition to the robustness of random packet loss, network coding can be effectively used to quickly recover from path failure. This method uses a primary and a backup flow of transmissions simultaneously using coding principle. Because of having this alternative option, in event of link failure a new path can be very quickly recovered without going through rerouting process [2].

From a network security standpoint there are also attempts in recent years that use network coding for ensuring securities. For example, if an adversary obtains a subset of a message, it cannot read anything because of not being able to decode that subset with the information in hand. This provides an added layer of security on top of any regular mechanism [2].

It is, however, not just conventional networks that have materialised the potential of this technique. The peer-to-peer network is another area where researchers are building contents and file sharing frameworks using network coding [49, 50, 51].

### 2.5.3 Network Coding in Wireless Networks

Because of the fact that wireless network link layer operates using one-hop-broadcast and to avoid collision channel access is allocated one-by-one, NC works even better with IEEE802.11 MAC protocols. The following is a simple example involving a wireless network with a three node topology presented in [1]. As demonstrated in figure 2.8, node A and B want to exchange packet via an intermediate node S. A sends packet ‘a’ and B sends packet ‘b’ to node S. Instead of sending these ‘a’ and ‘b’ in sequence, if S broadcasts ‘a xor b’, the number

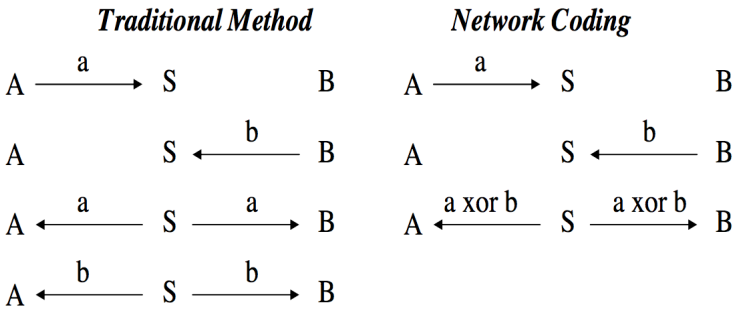



Figure 2.8: A Network Coding example with three node wireless topology presented in [1].

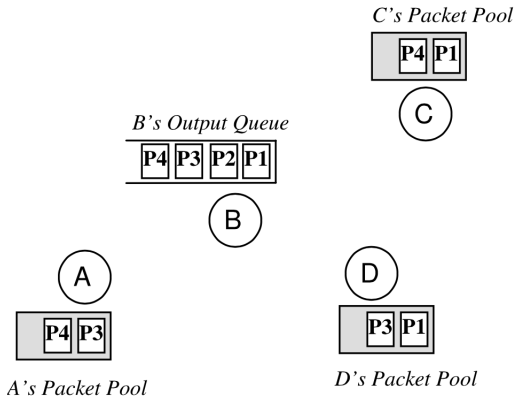
of transmissions will be reduced but both node A and B can recover the original packet by decoding the coded transmission with the available information at their disposal.

The network coding concept was theoretically materialised in a number of proposals showing the evidence it can be utilised in improving network performances [52, 53, 54, 55]. It is, however, only in recent years researches around the world implemented and evaluated NC-based protocols practically [56, 3, 57]. These implementations further boosted the confidence that NC can improve network performance significantly in futuristic applications.

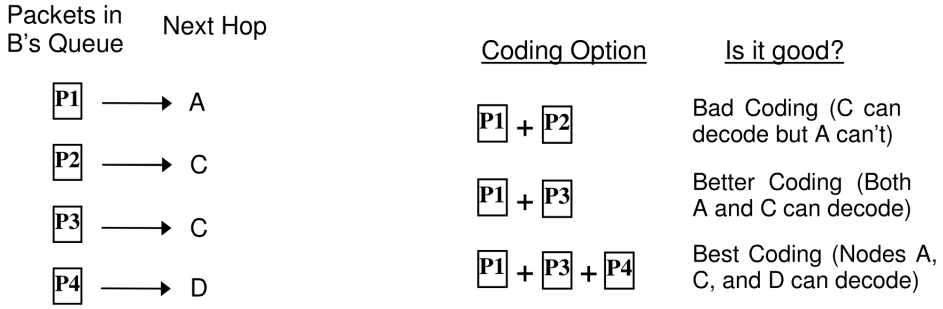
### 2.5.4 Encoding and Decoding

The encoding process is an operation that takes multiple incoming packets as input and 'xor' them together to form a single outgoing packet. The packet that had gone through the encoding process is called *encoded packet*. Information enclosed in an encoded packet is not readable until it gets decoded. A packet is said to be a *singleton* if it is not encoded and any information enclosed in it is readable without having to decode it. When two or more singleton packet is encoded together, it is called encoded packet of *degree d*. For example, if 3 packets are encoded together, it will be of degree 3 (a singleton holds degree 1). On the other side, the decoding is the reverse operation of the encoding. If the degree of an encoded packet is $d$, to decode this packet decoding node must have $d - 1$ packets available at its disposal. Naturally, the difficulty level of decoding increases with degree. An encoded packet of degree 3 will be more difficult to decode than an encoded packet of degree 2. Packet with more degree, however, transmits more information and therefore desirable.

Apparently the concept of network coding looks very simple but the main challenge lies in the encoding and decoding operations. From the previous example presented in figure 2.8, it is easy to understand that a node can easily 'xor' multiple packets and send through one-hop-broadcast to its neighbour. This, however, does not guarantee that the receiver can decode it and therefore, it is essential that the sender must encode in such a way that the receiver nodes can decode it with available 'information' at their disposal. Let's consider another example




**(a) B can code packets it wants to send**




**(b) Nexthops of packets in B's queue**

**(c) Possible coding options**

Figure 2.9: An example showing possible encoding combinations and their effectiveness in a wireless network; presented in [3].

presented in [3].

Figure 2.9 demonstrates a four node scenario with node A, B, C and D. P1, P2, P3 and P4 are four packets that those four nodes are exchanging with each other. This figure shows availability of packet at each node at an arbitrary moment. If B wants to send an encoded packet using one-hop-broadcast, it may 'xor' packets in different combinations such as P1+P2, P1+P3, P1+P3+P4 and so on. However, the first combination is not suitable because A cannot decode. The second combination is suitable for A and C though D will not receive anything new. The third combination is suitable for all as everyone receives something and will be able to decode it. This example tells us the importance of encoding and decoding packets appropriately.

When the network coding technique is used in information dissemination, encoding and decoding algorithms play the most vital role. These algorithms need to be designed in line with the objective of the application and the purpose it serves. For example, [56] proposes NC-based network layer broadcast protocol for ad hoc network, [55] proposes energy efficient

broadcast using network coding, [52] talks about minimum cost multicast and [3] discusses possible unicast communication for TCP in wireless mesh networks. Some of those protocols can tolerate delay (i.e. wait for more packets to arrive for decoding purposes) but need to be efficient whereas some try to establish one-to-one communication out of a broadcast-based MAC.

## 2.6 Summary

This chapter sets the context of this thesis and pulls off key discussions that are necessary to understand the subsequent chapters. It gives an intimation of what is forthcoming and possibly how the proposed warning system will be unfold. The description of the VANET and IEEE 802.11 protocol will be used as reference throughout this thesis and the Network Coding review will be used as the foundation of the Chapter 5 that describes the newly proposed warning system in this thesis.

# Chapter 3

# Requirements Survey for an Empirical System

Accident Warning Systems (AWSs) are used in Vehicular Ad-hoc Networks (VANETs) to avoid potential collisions and spread safety notifications amongst neighbouring vehicles [58]. The problem of designing efficient and effective warning systems has been widely studied. This involves design of warning systems that act proactively before an accident takes place, or spread post-crash messages for avoiding further collisions, or both [59]. Despite much previous research, however, there is still little agreement on the requirements for an empirical accident warning systems.

In order to build a warning system, it is needful to ascertain the system requirements, information to be exchanged, and protocols required for communication between vehicles. To achieve these goals, understanding the requirements for building the system and the existing research gaps in this area is of absolute necessity. An in-depth survey on the requirements along with a review of existing proposals identifying their strength and weakness should be helpful for the future studies. To the best of author's knowledge, no such initiative has been undertaken in relation to warning systems; thus the importance of having such a study remains high.

This chapter aims to accomplish the first research objective (RO1) set in Section 1.2 of Chapter 1 by presenting a practical model of a warning system based on a requirements survey and an assessment of previous proposals. First, Section 3.1 identifies the preliminaries required to build a warning system and Section 3.2 reviews existing warning systems described in the literature; second, Section 3.3 conducts the requirements survey and identifies gaps in existing research; and finally, Section 3.4 presents a practical model that an AWS should look like before Section 4.10 summarises the chapter.

## 3.1 Preliminaries

The problem of building automated Accident Warning Systems for next generation vehicles has been widely studied. Despite the fact that a number of proposals have been described in the literature, there are still many areas that require clarification. Many proposals assume that vehicles will exchange their location in real-time, but a scepticism remains with the Global Positioning System (GPS) as to how accurate this system is to provide location with sufficient precision. Other proposals talk about emergency braking, but do not give sufficient indication in regard to how a vehicle would detect another driver stopping abruptly. Some proposals require drivers to give input to the system but the human-vehicle interaction is not well ventilated in the literature. It would be inappropriate to move on without some answers to these issues. As this chapter intends to analyse requirements for an empirical and realistic warning system, it is imperative that it looks for clarification of these areas first. The following section presents a brief discussion concerning the background technologies underpinning accident warning systems.

### 3.1.1 The Network

Vehicular Ad-hoc Networks (VANETs) are considered suitable for AWS deployment mainly because of their infrastructure-less decentralised nature and dedicated vehicle-to-vehicle communication spectrum. A VANET is a type of wireless network that is specially designed for intelligent transportation systems. Most current implementations use short-range wireless communication protocol IEEE 802.11p and operate in the 5.9 GHz band that the Federal Communication Commission (FCC) allocated for *Licensed Dedicated Short Range (LDSR)* communication in the United States [27] and the European Telecommunications Standards Institute allocated for *Intelligent Transportation System* in Europe [28]. Compared to other versions of the protocol, the *p* version of the 802.11 MAC is particularly designed with a view to reducing latency and enhancing bandwidth of networks operating in a vehicular environment. Unlike infrastructure based networks, such as cellular networks, a VANET is very flexible and can be formed on-the-fly. It also does not require expensive equipment apart from the wireless connectivity that is likely to be standardised in next generation vehicles [29].

An Accident Warning System operating over a VANET is responsible for warning vehicles before collisions take place. AWSs and VANETs have a complex relationship that varies depending on the architecture of the system. Some AWSs operate at the application layer and remain completely independent of the network layer [60, 61]. Such systems see the VANET as the network that provides communication functionality. However, AWSs can also be found at the network [59, 62] and link layers [63, 64]. In the former, the system usually

acts as the main network protocol for a dedicated device whilst, in the latter, the AWS is integrated into the modified MAC protocol. Nevertheless, it is still a matter of debate at which layer warning system might be best fitted [65, 63].

### 3.1.2 Satellite Navigation System

The Satellite Navigation System (or in short *satnav*) is a space-based system that can provide with the geographic location of a suitable receiver anywhere on Earth [66, 67]. The Global Positioning System (GPS) is world's first operational satnav established in 1978 by the Government of the United States and considered a dual-purpose technology meaning that it serves both the military and the civilians [68].

A GPS-aware AWS obtains vehicle location through GPS and uses this information in its warnings. The accuracy of the GPS reading is particularly important because other vehicles act depending on this information [26]. Though military systems are more accurate, at the moment, the US Government is providing 7.8 meter accuracy at the worst with 95% confidence for public GPS. However, the actual accuracy that users attain depends on various other factors including atmospheric effects and receiver quality. The Federal Aviation Administration (FAA) of the United States government showed using real-life data that on average accuracy is usually 3 meter and can be further improved in combination with other augmentation systems [69].

The GPS modernisation program is an ongoing research that has high priority in the United States. The US government has policies to meet the growing demand for enhanced performance. The first next-generation GPS satellite was launched in 2005 and by 2016 GPS III will be in operation. This phase is expected to be fully functional within 2020 [70].

In addition to GPS, there are at least two other satellite navigation systems in development at the moment. GLObal NAvigation Satellite System (GLONASS) is operated by the Russian Aerospace Defence Forces and funded by the Russian government. This is the first alternative to GPS with a global coverage [71]. GLONASS-K and GLONASS-K2 are two versions of this system that are likely to match the performance of GPS in near future [72]. On the other hand, Galileo is operated by the European Space Agency and publicly funded by the European Union. This navigation system aims to provide with the same service that GPS does [73].

It is expected that by the time warning system becomes a standard in the next generation vehicles, these satellite navigation systems in combination with AWSs will help achieving safe and accident-free road transportation systems in future.

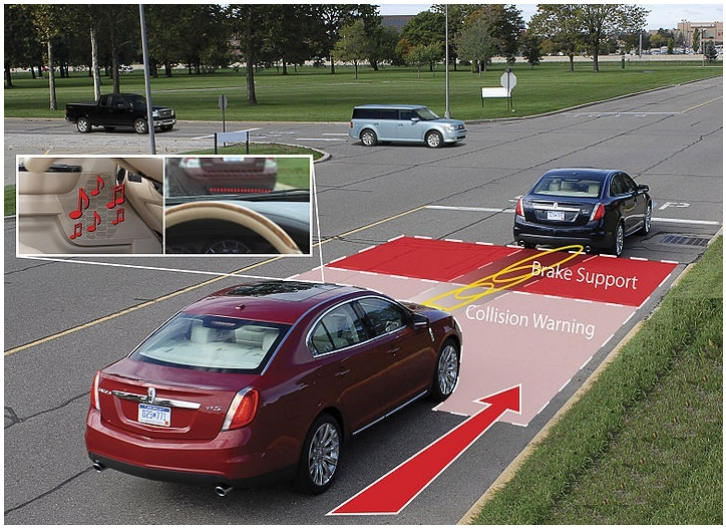



Figure 3.1: Collision Warning with Brake Support.

### 3.1.3 Supplementary Sensors

There are several sensors that detect problems and inform drivers accordingly [74]. For instance, *Lane Departure Warning System (LDWS)* are responsible for identifying unintentional lane changes. Mercedes has developed a LDWS called *Lane Keeping Assist* that detects unplanned lane changes and informs the driver accordingly [75]. An AWS can then transfer this warning to the vehicles who might be endangered because of this event. An *Emergency Braking System (EBS)* is a type of sensor that detects sudden braking and generates warnings. There is another type of sensor commonly known as *Frontal Collision Detection System (FCDS)* that detects obstacles in front of a car using infrared or radar. With the combination of these sensors, rapid warnings for a wide range of collisions can be produced.

### 3.1.4 On Board Unit (OBU)

An *On Board Unit (OBU)* is an in-vehicle smart device usually equipped with satnav and communication facilities [76, 77]. It facilitates the user to interact with the network to access a variety of applications such as Accident Warning Systems, Toll Payment Systems, Digital Maps etc. This device features push buttons to allow drivers giving input manually [78].

It is only until recently these devises become popular and commercial manufacturers start to come with combinations of innovative design and functionality. In near future, it will be straightforward to adapt OBU working with the AWSs. Given such a scenario, drivers would be able to generate warnings should they witness incidents.

| Year | Accident Warning Systems |
|---|---|
| 2005 | SAVN [62], IWS [60] |
| 2007 | VSPCA [59] |
| 2009 | RBSM [79], OppAWSt [80] |
| 2010 | AICC [63], CRCA [81], WMPIV [82], ESBR [83], ESMD [65], EABS [84] |
| 2011 | SBIRC [64], ODEM [85], RVSS [86], ICWS [61] |
| 2012 | Geo-Diss [87], OAWS [88], CarSpeak [89] |

Table 3.1: Available Accident Warning Systems in Literature.

## 3.2 A Systematic Review of Existing Warning Systems

Although researchers have been actively involved in designing accident warning systems for vehicles for several years, no initiative has ever been undertaken to accumulate system requirements for an empirical warning system. This chapter appraises 18 proposals in the literature that have been used to build warning systems between 2005 and 2012. Table 3.1 presents these proposals in order of their publication year. These proposals independently analysed the problem and came up with different solutions. However, as these solutions lack a proper analysis on the requirements, some important aspects have tended to be overlooked. In the following section, proposals are reviewed, and their advantages and disadvantages identified. Later these findings are used in the requirements survey.

### 3.2.1 Flooding-based Schemes

SAVN [62] is one of the earliest attempts at building accident warning system that covers a broad range of collision avoidance approaches. This system divides warning messages into different categories and assigns priorities. IWS [60] and ICWS [61] are two other simple systems that only address intersection hazards and trigger collision avoidance notifications when a vehicle approaches a junction. Nonetheless, VSPCA [59] is more sophisticated in terms of both coverage and data dissemination. It follows the footsteps of SAVN and generates warnings for a diverse range of scenarios that include periodically generated collision avoidance messages and event-driven warnings. One of the key contributions of this latter work is to separate messages based on creator and forwarder. A message created by a source vehicle holds the highest priority and any forwarder subsequently downgrades its priority to normal.

The main problem of the above four systems is their data dissemination schemes. As these schemes were proposed around a decade ago, those are designed based on less-effective

flooding technique. Flooding could have been a good solution to spread warning information for SAVN and VSPCA if vehicles on road always remain small in number. However, as in urban areas that is not the case, these schemes tend to distribute warnings without having to know the networks and flood them with bulk volume of redundant data. The other two schemes, IWS and ICWS, also flood the network but their major limitation is the operational jurisdiction which is limited to only intersections. All these schemes also risk generating broadcast storms in dense traffic scenarios.

### 3.2.2 Non-flooding Schemes

RBSM [79] is arguably the earliest proposal that shows much concern about *reachability*. It tries to bring a tradeoff between the importance of the reachability of a warning and the consequences the network suffers due to flooding. It introduces two key elements in the design of warning systems: firstly, it tries to control flooding by using a parameter that keeps track of the maximum number of time a message can be forwarded. Secondly, it makes use of beacon messages to allow any given vehicle to learn about its neighbourhood. The former approach is taken to allow senders to control the scope of a particular warning; in this thesis it will be called *limited-scoped broadcast*. The latter approach is particularly helpful because beacon messages can help sending data along with control information. OppCast [80] is another warning system that closely imitates the functionality available in RBSM except for the fact that its forwarding mechanism is based on an opportunistic algorithm, and to limit the coverage of the warning it uses specific length of roads. Nevertheless, it splits the responsibility for delivering potential collision avoidance messages and event-driven warnings between beacon messages and limited-scoped broadcasts respectively. ESBR [83] and Geo-Diss [87] also follow the principle followed by RBSM.

As mentioned earlier, a warning system can be found in the link layer too. The AICC protocol [63] is an example of this type of system. The key contribution of AICC is rate-based warning dissemination. Unlike the previously described systems, AICC does not send warnings at a constant rate, but rather tries to assess the nature of the situation and adjusts the rate of warning based on that assessment. In addition, it also increases or reduces transmission power to alter the coverage around the source vehicle. The former technique determines how frequently warnings should be disseminated and the latter how far a warning should travel in one transmission. SBIRC [64] is another link layer accident warning system. SBIRC makes the use of raptor codes for warning message dissemination. It also prioritises its warnings based on importance.

There are some event specific systems that trigger warnings if they encounter predefined events. For example, CRCA [81] is a limited-scoped broadcast-based warning system that only generates warnings in the event of emergency braking and potential intersection col-

lisions which it identifies in advance using a prediction-based algorithm. ODEM [85] is another road-safety system that gets activated when an accident takes place. It uses opportunistic propagation of accident information to hospitals, police stations and fire stations.

Although limited-scoped broadcast reduces the wastage of network capacity compared to flooding-based schemes, it does not stop the flooding of the immediate locale of the source. It has the basic properties of a stochastic broadcast scheme and is also capable of creating a broadcast storms. Therefore, above schemes naturally exhibit this problem while operating as a warning system associated with a vehicle. Besides, there are also other unique shortcomings laid inside each of those schemes that have been explained below.

The main limitation of OppCast is its opportunistic approach that is not suitable for disseminating periodic warning messages. The safest practice in building an warning system is to cover all neighbouring vehicles. The decision of making use of a particular warning message should be rested upon the recipient's discretion and the forwarding node may not take part in that process in any capacity apart from handing over the warning to the recipients. ESBR, on the other hand, takes this approach too literally and spreads the message within such a large region that the dissemination process could get out of control resulting in flooding again.

Geo-diss and RBSM demonstrate relatively better performance than those two former schemes and could only be less productive in event of large network density or data traffic load due to their repetitive rebroadcasting behavior. Amongst these two schemes, RBSM seems to be better off as it spreads warning based on number of hops as opposed to physical distance demonstrated by Geo-diss. It is because, when the number of nodes increases within a specific region, the covering jurisdiction of RBSM gets shrinked and it tends to send warnings to vehicles who are close to it. However, Geo-diss strictly maintains a physical radius and despite the fact that the number of nodes increases within that radius, it keeps sending warning to all the vehicles located within its predefined reach.

Both AICC and SBIRC have a very limited reachability as they only broadcasts warning from MAC layer that sends message only to its neighbours. Such approach could have been effective if further enhancement is enforced from the application layer of the system. For example, if an application analyses received warning and detects possible danger based on mathematical assumption and also keeps forwarding them to its neighbours with a view to give them the opportunity to make similar predictions, it could be very effective. However, as that is not the case here, these two schemes hardly looks better than buil-in IEEE 802.11 beacon message.

The event specific warning systems such as CRCA and ODEM are good for spreading post-crash information to the appropriate authorities but their operational limitation screens them out of the league of full-fledged warning systems.

### 3.2.3 Other Schemes

WMPIV [82] is a unique proposal that introduces *relay-based* forwarding. Its collision detection is limited to forward and lane-change collisions but significantly reduces number of transmissions while using limited-scoped broadcast. It selects suitable relay vehicles which carry warnings as those vehicles move on. EABS [84], RVSS [86] and OAWS [88] are other proposals that use the relay-vehicle and follow similar concept. One of the major limitations of a relay-based system is that it cannot ensure reachability and often covers only a narrow range of possible scenarios.

ESMD [65] is an attempt to bring in session-oriented data dissemination in the form of a tree-based multicasting. It transforms the multicast routing problem into a delay-constrained *Minimum Steiner Tree* problem with a view to connect all nodes together. It also uses beacon messages to communicate with one-hop neighbours and covers all possible collision scenarios. CarSpeak [89], a publish/subscription based content-centric warning systems introduces an approach that stores information in an *Octree* [90] and later distributes it on-demand. One of the major drawbacks that these schemes exhibit is poor latency. AWSs are extremely time-sensitive and provide little time to discover routing paths for fetching data from the network. As a result, the likelihood of timely success is slim.

## 3.3 Requirements Survey

This requirements survey aims to assess the possible requirements in a methodical way; thus it starts with possible scenarios followed by identification of potential collisions and different types of messages that AWSs typically exchange. It also discusses suitable data dissemination approaches that can make warning systems effective in those scenarios.

### 3.3.1 Possible Scenarios

It is difficult to identify scenarios because of the diversity in road types and speed limits in different countries. This thesis, therefore, focuses on the layouts available in the United Kingdom and Ireland only. There are many possible scenarios but, for simplicity, this survey groups them into five broad categories: i) Junction, ii) Roundabout, iii) Single carriageway iv) Dual carriageway, and v) Motorway.

It is also noteworthy that vehicles, while commuting through these scenarios, act differently in *urban* and *highway* layouts due to legal restrictions on maximum speed. In the urban layouts, speed limit is restricted to maximum 30 mph whereas in the highway layouts speed limit varies between 40 to 70 mph depending on the road types.


Figure 3.2: A roundabout is one of the most complex scenarios that warning systems need to deal with. This image shows a roundabout located in Swindon, England. It is widely regarded as one of the most complex roundabouts in the United Kingdom [4].

The following part of this section discusses these scenarios in details not only to prepare the basis of future discussions but also to give enough context for the simulation environments used in Chapter 4, 6, 7 and 8.

***Junctions:*** A junction is a place where multiple roads intersect. Generally busy junctions are controlled by traffic light where vehicles need to wait until the green light signals them to go. In the United Kingdom and Ireland, another type of junction can be found where traffic light is absent but *giveway* signs still control the movement of the vehicles. In these junctions, vehicles on the approaching road with giveway sign must allow incoming vehicles from other approaching roads and failing to do so could cause potential accidents. There are also small junctions available in these countries where no traffic light or giveway sign is available. In such junctions, drivers decide amongst themselves who to get the priority. It is noted that although junctions are frequently seen in urban layouts, they are not rare in highway layouts particularly when roads with 40 mph speed limit intersect.

Junctions are one of the most complex scenarios in terms of response time and participating entities. It is likely that an urban junction would include pedestrians and cyclists in addition to vehicles whilst only vehicles are usually present on highway layouts. The highway junctions are, however, more likely to involve a variety of vehicle types and speeds. A realistic warning system design must take these information into account.

***Roundabouts:*** A roundabout is a special type of circular junction as shown in figure 3.2 [91]. The continuous flow of vehicles makes it different from a regular junction. When a vehicle approaches on a roundabout, it must giveway to the vehicle coming from its right. In event of no vehicle coming from right, approaching vehicles are allowed to move on and commute through the roundabout following their designated lane. Both urban and highway layouts can have roundabout. Mini-roundabouts can be seen in the urban layouts where vehicles

Figure 3.3: Vehicles commuting on a typical dual carriageway in the United Kingdom and Ireland. This image shows the N11, a dual carriageway that connects the town of Wexford with the capital city Dublin in Ireland.

can even commute over the roundabout whilst on highway or busy urban layouts controlled roundabouts with traffic lights are common.

The possibility of the movement of vehicles from all sides makes roundabout one of the complex scenarios. Accident could take place at this scenario because of the slightest mistake of a driver and warning systems would not get enough response time if they are not fast enough.

***Single Carriageways:*** A single carriageway is a road where two or more lanes are arranged without the presence of a central-reservation. This is the most common road in the United Kingdom and Ireland that can be found both in urban and highway layouts. In the urban layouts, vehicles are allowed to speed up up to a limit of maximum 30 mph. In the highway layouts, vehicles can move at a speed of 40 to 60 mph. The national speed limit, however, is 60 mph for single carriageways.

Single carriageways could be potentially dangerous as vehicles moving at a high speed in opposite directions may collide with each other head on. Warning systems in such scenarios have little time to detect and warn drivers about possible collisions unless they are fast enough to communicate between themselves.

***Dual Carriageways:*** A dual carriageway is a road having multiple lanes divided by a central-reservation. It is possible to have dual carriageways with one lane on each side of the road but most of them have multiples lane on each side. This scenario is relatively rare in the urban and mostly seen in highway layouts. The national speed limit on a dual carriageway in highway scenario is 70 mph but in urban layout speed limit gets reduced to 30 mph. Because of the presence of the central reservation, dual carriageways, as shown in 3.3, do not have the


Figure 3.4: Vehicles commuting over multiple lanes on a typical motorway in the United Kingdom and Ireland. This image shows the west-flank of the M6, a motorway that connects England with Scotland.

same threat of head on collisions but have the possibility of vehicles getting into collisions from back due to high speed limit.

***Motorways:*** A motorway is a special dual carriageway with multiple lane on each side of the road and often features a hard-shoulder[1]. Motorways can not be found in the urban layouts and vehicle always commutes with a speed of 70 mph unless displayed otherwise. Exits on the motorways are created in such a way that flow of the vehicles does not get interrupted. These exits are generally located on the left-hand side with some very rare exceptions. It is notable that motorways do not have junctions but sometime roundabouts are used to connect two motorways or a motorway with another road.

Like dual carriageways, motorways do not have the threat of head on collisions. However, because of vehicles commuting at a high speed on multiple lanes as shown in figure 3.4, sudden lane change or braking manoeuvres can result in fatal collisions. In order to try to prevent these kind of accidents on single and dual carriageways as well as motorways, timely delivery of warning is of utmost necessity.

### 3.3.2 Potential Collisions

This requirements survey methodologically identifies the following categories of collisions covering the most real-world possibilities that warning systems should take into account.

***Follow-Up Collisions (FUC):*** FUCs are a type of collisions that can be seen frequently in the real-world. These occur when a vehicle slows or halts in the middle of a free-flow

[1]A hard-shoulder is a hardened strip alongside a motorway for stopping on in an emergency.

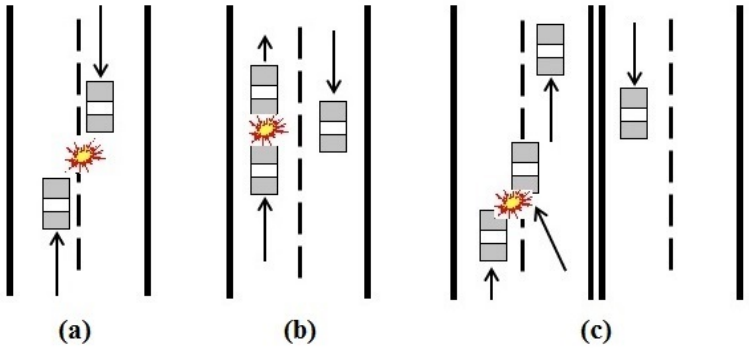



Figure 3.5: Possible collisions on a free-flow road: (a) Forward collision on a single carriageway. (b) Follow-up collision on a single carriageway. (c) Lane-change collision on a dual carriageway.

road, particularly on motorways or dual carriageways, because of a technical problem, loss of control on a slippery or damaged road surface, or a primary collision with an object or individual on the road. In such circumstances, successor vehicles following behind crash into the back of the vehicle affected.

***Pile-Up Collisions (PUC):*** Sometime referred to as a *Multiple Vehicle Collision*, PUC is a type of road accident that can develop out of a follow-up collision should following vehicles fail to stop in time. It particularly occurs on motorways and could be potentially devastating. Accident warning systems need to respond quickly and proficiently to stop or reduce the level of destruction caused by PUCs.

***Intersection Collisions (IntC):*** These collisions occur at junctions and roundabouts when drivers fail to notice a vehicle coming from another direction. Intersection collisions are especially common in busy urban layouts. Due to the fact that directions of vehicles are diverse at junctions and roundabouts, warning system needs to comply with the necessity of timely delivery of message to neighbouring vehicles.

***Forward Collisions (FC):*** This is a type of collisions that can be seen on the single carriageways in both urban and highway layouts. It occurs when two vehicles coming from opposite direction collide and crash into each other. This kind of collisions are generally extremely fatal and can potentially lead to pile-up collision on busy roads.

***Lane-change Collisions (LCC):*** These occur mostly on motorways and dual carriageways when drivers try to change lane but fail to notice vehicles coming from behind. Warning system can predict an LCC hazard based on the movement of nearby vehicles; however, in doing so they need to exchange information amongst themselves in a timely manner.

***Vehicle-to-Object Collisions (VOC):*** These occur when a vehicle hits stationary object. The object itself can be a part of the traffic infrastructure such as a barrier or some sort of obstacle accidentally or deliberately moved onto road. Such a collision can only be avoided

| AWS | FUC | PUC | IntC | FrdC | LCC | VOC | VBC |
|---|---|---|---|---|---|---|---|
| SAVN | ✓ | ✓ | ✓ | ✓ | ✓ | × | × |
| IWS | × | × | ✓ | × | ✓ | × | × |
| VSPCA | × | × | ✓ | ✓ | ✓ | × | × |
| RBSM | × | × | ✓ | ✓ | ✓ | × | × |
| OppAWSt | ✓ | ✓ | ✓ | ✓ | ✓ | × | × |
| AICC | ✓ | ✓ | ✓ | ✓ | ✓ | × | × |
| CRCA | ✓ | ✓ | ✓ | × | × | × | × |
| WMPIV | × | × | × | ✓ | ✓ | × | × |
| ESBR | ✓ | ✓ | ✓ | ✓ | ✓ | × | × |
| ESMD | ✓ | ✓ | ✓ | ✓ | ✓ | × | × |
| EABS | × | × | ✓ | ✓ | ✓ | × | × |
| SBIRC | ✓ | ✓ | ✓ | ✓ | ✓ | × | × |
| ODEM | × | ✓ | × | × | × | × | × |
| RVSS | × | ✓ | × | × | × | × | × |
| Geo-Diss | ✓ | ✓ | ✓ | ✓ | ✓ | × | × |
| OAWS | ✓ | ✓ | ✓ | ✓ | ✓ | × | × |
| ICWS | × | × | ✓ | ✓ | ✓ | × | × |
| CarSpeak | ✓ | ✓ | ✓ | ✓ | ✓ | × | × |

Table 3.2: Collisions that previous proposals addressed.

if the vehicle at risk is equipped with appropriate sensors; however, a warning system can effectively prevent follow-up and pile-up collisions that might occur as a consequence of a VOC by taking appropriate measures immediately.

***Vehicle-to-Body Collisions (VBC):*** This type of collision occurs when a vehicle impacts a human or animal who happens to be on the road for whatever reason. A VBC is somewhat different from a VOC because in this collision the non-vehicular party is mobile and may try to avoid the incident by moving randomly and abruptly. Avoiding this kind of collision also requires appropriate sensors and but, again a warning system can prevent follow-up and pile-up collisions developing out of the incident.

Table 3.2 shows that amongst the 18 proposals reviewed in this chapter, only 9 addressed the first five of those possible seven collisions. VOC and VBC are not covered at all by any of the previous proposals.

### 3.3.3 Warning Messages

Because collisions differ in nature, the warnings and safety notifications generated by accident warning systems also differ. When and how frequently these message are sent is an important concern. The following section briefly addresses the different message types and dissemination approaches used in the previous proposals.

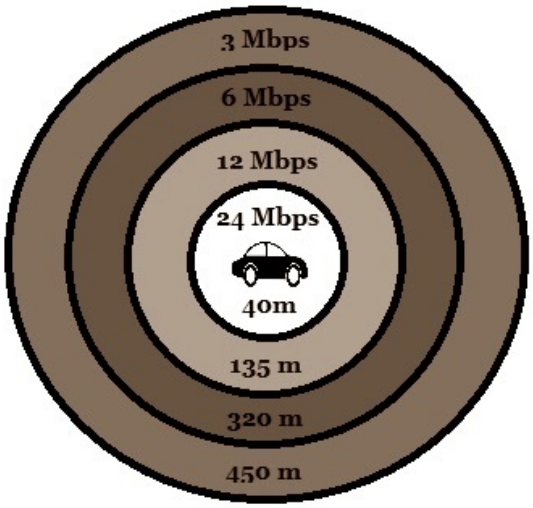



Figure 3.6: IEEE 802.11p Data Rate vs Coverage [5].

***Warning type:*** Event-driven Messages (EDMs) are found in most warning systems. Table 3.3 shows that amongst the 18 systems reviewed in this chapter, 11 use this type. Such warnings are reactive and sent in response to specific events. Incidents such as encountering an accident, emergency braking, careless driving, witnessing an incident and so on may result in such a warning being transmitted. A close observation in these warnings reveals that they can be classified into two types: Local and Forwarding. Local EDMs are generated by the vehicles involved in incidents whilst forwarding EDMs are passed by vehicles who either witness the incidents or receive the warnings from other vehicles. Local EDMs are more delay sensitive than passive EDMs as they aim to inform immediate neighbours about an incident. The design of an accident warning system will be beneficial if the classification discussed here is considered.

Periodic Warning Message (PWM), on the other hand, are present in almost every warning system.16 out of the 18 systems reviewed in this chapter use this type of warning. The primary objective of this warning is to warn nearby vehicles about a potential collision in advance. Dissemination of PWMs, however, needs to be conducted carefully as it may cause contention for channel access in the network.

There are two other types that can be found in some warning systems. These are Road Condition Notification (RCN) and Emergency Call-Up (ECU). RCN can be used to let other vehicles know about road congestion and weather conditions. However, rapid growth in smartphone apps development makes it possible to receive such information from alternative sources. ECU might be helpful for post-crash call-up to hospitals and police stations but, again that can be achieved by other means. Therefore, these types are not considered further in this thesis.

| AWS | EDM | PWM | RCN | ECU |
|---|---|---|---|---|
| SAVN | ✓ | ✓ | ✓ | ✓ |
| IWS | × | ✓ | × | × |
| VSPCA | × | ✓ | × | × |
| RBSM | × | ✓ | × | × |
| OppAWSt | ✓ | ✓ | × | × |
| AICC | ✓ | ✓ | × | × |
| CRCA | ✓ | ✓ | × | × |
| WMPIV | × | ✓ | × | × |
| ESBR | ✓ | ✓ | ✓ | ✓ |
| ESMD | ✓ | ✓ | × | × |
| EABS | × | ✓ | × | × |
| SBIRC | ✓ | ✓ | × | × |
| ODEM | × | × | × | ✓ |
| RVSS | ✓ | × | × | × |
| Geo-Diss | ✓ | ✓ | ✓ | × |
| OAWS | ✓ | ✓ | × | × |
| ICWS | × | ✓ | × | × |
| CarSpeak | ✓ | ✓ | ✓ | × |

Table 3.3: These are the warning messages that previous proposals addressed.

***Frequency:*** The number of warning sent per second is closely related to overall performance of the system. As PWMs are sent periodically, they can become the primary contributors to the frequency count. A dynamic counter-based frequency controller could play an important role in controlling the volume of such warnings [92].

***Priority:*** Prioritising warning messages is an approach towards establishing control over data dissemination although it has not been widely implemented. Only a few proposals have considered prioritisation of warnings. Nevertheless, this has the potential to partition overall bandwidth intelligently for different requirements [59].

***Coverage:*** Coverage is of obvious importance, yet has not been widely considered. Out of the 18 reviewed proposals, only one addressed altering coverage dynamically. Figure 3.6 shows how IEEE 802.11p coverage has a clear relation to data rate: an increase in coverage, decreases data rate and vice versa [5]. In network density with significantly higher number of vehicles, particularly in urban layouts, coverage can be reduced to improve the performance whilst in highway layouts with less vehicles, a warning system can increase coverage to reach vehicles at a greater distance.

### 3.3.4 Data Dissemination Schemes

An important challenge that has to be addressed in VANET-based AWSs is how to distribute warning messages amongst vehicles. So far this requirements survey has examined possible scenarios, potential collisions, required warning types to avoid those collisions and warning frequency to potential receivers. The next issue is to consider what type of dissemination scheme should be used for these warnings and why.

There are two different data dissemination models: pull and push [29]. The characteristics of the pull model can be very diverse as it can involve unicast, multicast, content-centric or other type of data dissemination scheme. The push model, on the other hand, is very much more straightforward and includes various broadcast-based schemes only. The following section discusses the suitability of those two models in the context of an AWS.

***Pull Model:*** Data dissemination schemes that are designed based on a pull model bring information from the sender on demand. It is completely at the receiver's discretion from where and when data will be fetched. As AWSs are based on VANETs, the pull model often suffers from long latency [34, 35, 36]. Previous investigation reveals that unicast paths in VANETs have very short lifetimes [32, 31] and vehicles frequently change trajectory [33]. As a result, it is difficult to keep tracking a sender for a continuous supply of data.

A recently popular pull approach is the publish/subscribe scheme where one or more nodes (publishers) act as the source of information while the rest are followers who subscribe to access the information [89]. This approach might work well even in a wireless network where movement of the nodes is relatively slow, but not in most VANET scenarios.

Core and cluster multicast are two examples of the pull model [93]. At first sight these schemes might fit into the problem under discussion. Since vehicles often move in a group on roads, formation of a core or cluster might provide the basis of group communication where a vehicle could talk to the core or cluster head and share its location while collecting neighbours information. However, this system breaks down when core node or cluster head leaves the network, as might happen at any junction or roundabout. Detection of the sudden disappearance of the core or cluster head followed by a compensatory election would potentially render the group inactive for a time and make it vulnerable.

***Push Model:*** In the push model, the source sends data to receivers whenever it wishes. It injects data into the network without necessarily knowing who the receivers will be and it therefore does not have to track them. Because of the unpredictable mobility behaviour of the nodes, many VANET routing protocols use the push model for data forwarding [94] and indeed it has been almost universally employed in previous proposals.

*Flooding* is the simplest push scheme in AWS operation. Vehicles send data to their neighbours and their neighbours resend received data to their neighbours and so on; so that a

| Data Dissemination Schemes | Accident Warning Systems |
|---|---|
| *Push Model* | |
| Flooding | SAVN, IWS, ICWS, VSPCA |
| LSB at Network Layer | RBSM, OppAWSt, ESBR, Geo-Dess, CRCA, ODEM |
| LSB at Link Layer | AICC, SBIRC |
| Relay | WMPIV, EABS, RVSS, OAWS |
| *Pull Model* | |
| Multicast | ESMD |
| Publish/Subscribe | CarSpeak |

Table 3.4: Data dissemination schemes in existing warning systems.

warning can be propagated quickly to every vehicle. In order to reduce network load, *opportunistic forwarding* is sometime employed [80]. This is a probabilistic data dissemination method that tries to send data at best effort; however, it does not guarantee successful delivery of all messages to its entire targeted audience. Although relay-based scheme has been one of the latest approaches being tried in accident warning systems, it is not a standalone method. It requires an auxiliary data dissemination scheme to keep it active in absence of sufficient vehicles to relay data [86, 88].

*Limited-scoped Broadcast (LSB)* is the most popular push model. Instead of flooding the whole network, this aims to limit data dissemination to a specific geographical scope. Though limited-scoped broadcast does not flood the entire network by sending packets, it does flood the locale of the sender. It typically uses a stochastic broadcast scheme and can generate a local broadcast storm.

Table 3.4 lists all surveyed warning systems along with the data dissemination schemes they employ. It is clear from the selection of schemes that the broadcast-based schemes from the push model are the most popular and limited-scoped broadcast tops the popularity list with 12 AWSs using it in total. In contrast, the pull model is not popular, because of its relative incompatibility with a highly mobile network like a VANET.

It seems clear therefore that the push model is the better data dissemination model for time-sensitive warning systems. It is, however, important to evaluate such broadcast-based dissemination schemes within a realistic mobility and simulation environment so that limitations can be identified and addressed.

## 3.4 An Empirical Warning System

Previously in this chapter, existing warning systems were reviewed and various advantages and disadvantages identified. A requirements survey has also been undertaken with a view to discerning where and how an AWS should operate. It is now time to summarise the outcomes of these deliberations as they impact the design of an empirical warning system.

**Auxiliary Components:** This thesis proposes that the AWS should be accompanied by at least three sensors: Lane Departure Warning Systems (LDWS), Emergency Braking System (EBS) and a Frontal Collision Detection System (FCDS). The vehicle should also be equipped with an On Board Unit (OBU) with satnav functionality. These components assist the warning system in covering possible collision scenarios discussed earlier.

**Data Dissemination:** In terms of data dissemination, the AWS should follow push model i.e. broadcast-based data dissemination scheme. Although limited-scoped broadcast is a good data dissemination scheme for reaching the maximum number of relevant receivers in the minimum time, some modification is necessary to optimise its transmission. A thorough investigation is required of various broadcast-based schemes to identify their potential limitations and impact on the data dissemination process. Otherwise, problem like broadcast storm may potentially render the system ineffective in certain situations. As mentioned earlier, a cross layer interaction between network and link layer is likely to enhance performance by allowing co-access to parameters from both layers such as hop count, transmit power etc.

**Warning Messages:** The warning system should be capable of sending two types of message: Event-driven Messages (EDMs) and Periodic Warning Messages (PWMs). Both message should be divided into two further categories: a) generated by a vehicle involved in an incident or sending its potential collision avoidance message, and b) generated by a vehicle witnessing an incident indirectly or receiving someone's event-driven or collision avoidance message. In order to give important warning access to medium, that warning should be prioritised. Warnings that are transmitted for the first time should have higher priority but when they start to propagate across multiple hops with a view to reaching a wider audience, their priority needs to be downgraded. The underlying argument behind this design choice is that a vehicle that sends a warning generated by itself is a greater threat to the vehicles immediately around it compared to those vehicles that later receive its warning message via third-party forwarding. It is also not recommended that road condition and traffic notification messages be sent alongside EDM and PWM as this might create more contention in the network. However, exceptional and potentially dangerous circumstance such as icy, slippery or damaged roads can be accommodated using EDMs with a special code.

The frequency of the PWM should be controlled by a dynamic counter. There should be another control parameter to adjust coverage area. With the help of these two parameters, the

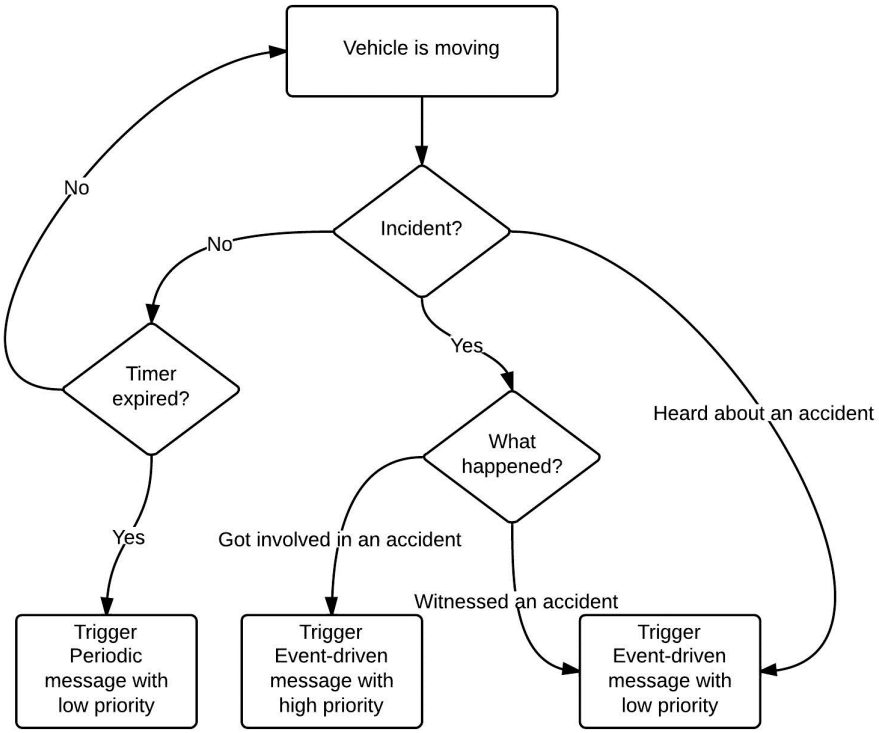



Figure 3.7: The warning dissemination process in an empirical warning system.

number of warnings can be controlled by sensing the environment around the native vehicle. Figure 3.7 summarises how the current analysis proposes the warnings to be handled and disseminated by an accident warning system.

## 3.5 Summary

This chapter fulfils the first objective of this thesis. In doing so, it presents a detailed requirements survey for building warning systems for next generation vehicles and proposes a realistic model for future development. The main contribution of this chapter can be summarised as: identifying preliminaries and key requirements that is necessary to build a warning system and having reviewed existing proposals, presenting an empirical model that fits with the requirements. Later in Chapter 5, this empirical model will be used as a blueprint for the design of the proposed warning system; and identified collisions and scenarios will be used in creating realistic simulation environment in Chapter 4, 6, 7 and 8.

# Chapter 4

# Analysis of Broadcast-based AWS in VANETs

Broadcast is one of the most popular data dissemination schemes amongst the researchers who build Accident Warning Systems (AWSs) over Vehicular Ad hoc Networks (VANETs). AWS aims to avoid potential collision by sending warning messages to neighbour vehicles. The use of broadcast scheme in existing warning systems is motivated by the highly dynamic nature of VANETs where nodes move very fast and topology changes frequently. In such an environment broadcast performs better than multicast or unicast protocols. On the other hand, the two-second rule which is a widely accepted approach of defensive driving in many countries including the United Kingdom, Ireland and the United States. This rule states that a driver should maintain two-second distance between his car and the car in front to avoid possible incidents. This two-second window potentially gives warning systems the time to communicate with each other and make decisions about cautioning the drivers.

In spite the fact that broadcast seems to be an ideal data dissemination scheme for AWS, it has some drawbacks that can lead to a collapse of the communication system. It sometime propels the network to the verge of breaking down by generating broadcast storms. In the event of such a storm, a node fails to communicate with its neighbour for the duration of some period. If this period is longer than two seconds, warning systems cannot tolerate such isolation and it could potentially make them vulnerable.

Existing warning systems described in the literature have typically taken a generalised approach and their performance evaluation has often been based on unrealistic simulation and mobility models that do not represent the movement of vehicles on roads well. As a result, those systems never got tested on handling broadcast storm and a grey area remains unexplored.

This chapter aims to accomplish the second research objective set in Chapter 1. In doing so, it presents a performance analysis of broadcast schemes as to how they comply with

the two-second rule stated above. A realistic simulation environment is built along with a city mobility model with a flow of vehicles which mimics that of a real city to evaluate the schemes. Three warning systems are simulated representing three broad categories of broadcast namely *limited-scope*, *flooding* and *single-hop*; their behaviour is then analysed to understand the effect of broadcast storm on their performance.

Section 4.1 provides a brief introduction to broadcast and broadcast storm problem followed by a prelude on the two-second rule and the maximum tolerable queuing delay in Section 4.2. Section 4.3 presents the investigated warning systems and section 4.4 describes in detail the simulation environment, mobility model and the simulator used in this thesis. Section 4.5 outlines the assumptions, Section 4.6 introduces the metrics used in the evaluation and Section 4.7 describes the method of study. Finally, Section 4.8 and 4.9 present four rigorous evaluations followed by a summary in Section 4.10.

## 4.1 Background

While disseminating data, vehicles sometime suffer from delays due to excessive transmissions or high network density. As AWSs are cooperative systems, these delays can be very crucial at bends, junctions or even on the straight roads. Therefore, to make AWS work effectively these scenarios need to be addressed.

One of the key reasons that causes these delays is data dissemination approach. Depending on the type of schemes used, delays can vary. Nevertheless, the process of data dissemination in VANETs is challenging because of their dynamics [95, 96, 97] and an added layer of difficulty is introduced when the VANET is the basis of a real-time AWS. The review presented in section 3.2 of Chapter 3 shows that existing proposals for warning systems that address problem related to collision and accident avoidance mostly rely on broadcasting for data dissemination scheme to cope with this highly dynamic nature of VANETs.

It is also notable that broadcast schemes used in various warning systems are not identical. Those schemes can be divided into three broad categories namely *flooding*, *limited-scoped* and *single-hop* broadcast. Amongst these three categories, limited-scoped can be defined as a dissemination technique that sends data to all nodes within a defined boundary such as certain number of hops or a small geographical region. Definition of flooding can be as simple as the technique of sending data to all connected nodes. The last category, called single-hop broadcast, only disseminates data to the neighbours located within one hop distance.

Performance varies depending on the type of their categories. For example, flooding provides the best coverage but injects a large amount of redundant data into the network while single-hop provides least coverage but shows less redundancy in terms of data overhead. It is no surprise that large number of existing protocols use limited-scoped because it provides a

trade-off between coverage and redundancy. Despite showing different characters, all three categories follow the basic principles of stochastic broadcasting.

Broadcast, however, is infamous for creating *storms* in the network that can isolate a node from its neighbours for some period. A broadcast storm can be explained in brief as follows: in ad hoc network when a node broadcasts a packet to its one-hop neighbours, they usually receive that packet almost at the same time. An imperative to rebroadcast that packet instantly results in all receiver nodes trying to get channel access that incurs collision. In order to avoid such a situation, stochastic broadcast protocols in ad hoc network may deliberately insert a small but random delay called Random Assessment Delay (RAD) in the scheduling of data delivery from network layer to link layer so that neighbouring nodes rebroadcast data at different times [98, 99]. However, when the number of rebroadcasts significantly increases, contention to get channel access becomes fierce and the RAD alone cannot prevent nodes from getting involved in collisions. If network continues to experience such behaviour, it results in a broadcast storm [100, 101, 102].

A number of previous studies showed how this phenomenon affects various networks and applications while operating with broadcast schemes. [103], through numerical analysis, shows how a broadcast storm is generated in IEEE 802.11 multi-hop wireless networks and argues that as the number of neighbour node increases, throughput performance falls. [104, 105] investigate the problem from ad hoc network's perspective and identify that rebroadcast is the key factor in creating broadcast storms that lead to redundancy, contention and collision in the network. [106, 107] reinvestigate the issue from VANET's perspective and conclude that i) high link load causes high contention in the network resulting packet loss and ii) low packet penetration causes long delay. Previous work, however, has not investigated the behaviour of broadcast schemes with a real-time system like an AWS, a gap this chapter aims to fill.

## 4.2 Maximum Tolerable Queuing Delay (MTQD)

The two-second rule is considered a rule of thumb by which a driver can maintain a safe distance with a following car. The rule suggests that a driver should ideally stay at least two seconds behind any moving vehicle that it follows. The government of the United Kingdom, Ireland and the United States promote this rule via driving and road safety authorities of the respective countries [9, 10, 11].

The reference to this two-second rule is used in this thesis to determine a benchmark delay that defines the maximum period a warning system can potentially be isolated. In reality, this isolation occurs when warnings await in the delivery queue but underlying MAC layer does

not get access to the medium due to competitions. Therefore, this period is named *maximum tolerable queuing delay* and will be denoted as $MTQD$ throughout this thesis.

A delay greater than $MTQD$ will be unacceptable as it risks the warning system failing to identify any potential accident before that takes place. It is, however, noted that this does not mean a warning system can always identify accidents if its queuing delay at network layer remains below $MTQD$. This threshold acts as an acceptable reference and warning systems in this chapter will be evaluated as to how they comply with it.

## 4.3 Investigated Warning Systems

Upon reviewing all available accident warning systems and having categorised those into the previously mentioned three broad categories, three warning systems have been picked up from each. It was the aim to pick the best performing system from each category except single-hop where only one choice was left. Brief descriptions of those three investigated AWSs are presented below.

***VANET Solution to Prevent Car Accident (VSPCA):*** VSPCA typifies the use of flooding. This warning system is more sophisticated compared to other members of its category in terms of both coverage and data dissemination. It generates warnings for a diverse range of scenarios that include collision avoidance messages and event-driven post-incident warnings [59].

***Reliable Broadcasting of Safety Messages in VANET (RBSM):*** RBSM represents limited-scoped broadcast category. This pioneering warning system shows much concern about reachability. It tries to bring a tradeoff between the importance of the reachability of a warning and the consequences the network suffers due to flooding. It introduces two key elements into its design: firstly, it tries to control flooding by using a parameter that keeps track of the maximum number of times a message can be forwarded. Secondly, it makes use of beacon messages to allow any given vehicle to learn about its neighbourhood. The former approach is taken to allow senders to control the scope of a particular warning and therefore turns flooding into a limited-scoped broadcast [79].

***IEEE 802.11p:*** IEEE 802.11p is a single-hop broadcast protocol. There is no other system at the moment that uses single-hop message delivery other than the built-in beacon frame embedded here. Although the general beaconing rate is twice a second, it is altered in this study to explore its performance further by placing a simple network layer on top of it.

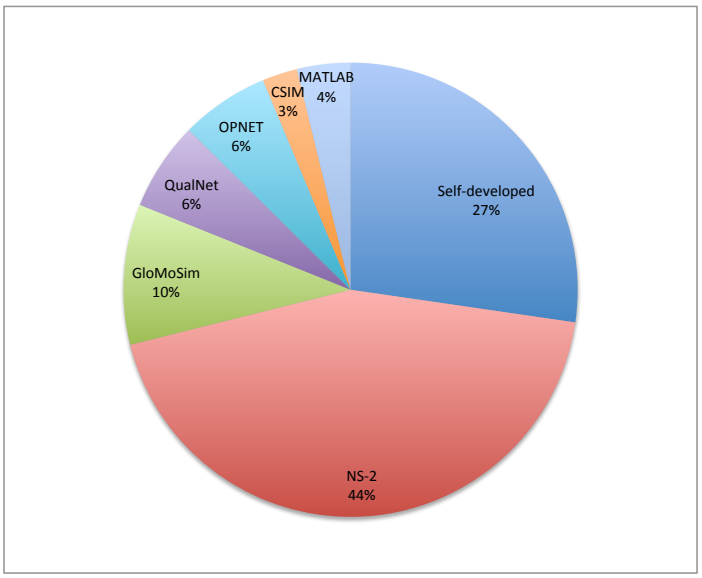



Figure 4.1: Simulator usage from the MobiHoc survey.

## 4.4 Simulation Environment

In this thesis a custom-built simulator is used to run and simulate experimental studies. Detailed descriptions of the simulation environment are presented in this section and will be used throughout this thesis unless explicitly stated otherwise.

### 4.4.1 Simulator

Simulators have been considered a valuable tool for research domains where real-life trials are not possible prior to the physical design of the systems or a simulated study has the potential to evaluate more functionalities than a real trial. Nevertheless, finding a realistic simulation environment is difficult because mainstream simulators [108, 109, 110] such as NS2, NS3, OMNET++, OPNET etc. often come with predefined mobility models, obstacle models, protocols and parameters that require strenuous effort to customise. Yet it is not always possible to calibrate these features in line with specific requirements of a particular experiment. For example, mobility model for nodes with assorted velocity is a customary feature in most available simulators. But this is typically implemented as some pattern-based or randomly generated movements that are unrealistic and unsuitable for a vehicular environment [111]. There are also some open source simulators developed recently (such as Veins [112]) which provide custom-built mobility models but development without sufficient technical support and community contribution often limits the usefulness.

There is a third option where researchers develop their own custom-built and self-deployed simulator. A study reveals that between 2000 and 2005 in MobiHoc, one of the most prestigious mobile network conferences, 27% authors used self-developed simulators [113]. Al-

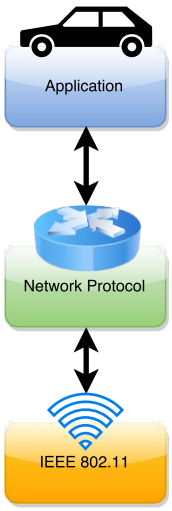



Figure 4.2: The stack-view of the protocols in the custom-built simulator used in this thesis.

though NS2 was the most popular simulator at the time of this study, self-developed simulator was still second most popular choice by a large margin as shown in figure 4.1.

These are highly customisable and very specific functionalities can be included in the experiments. Taking these options into consideration, for the current work it was decided that only the medium access control layer will be borrowed from an existing simulator and a network and application layer along with a realistic mobility model will be built on top of it.

An open source simulator called *Pamvotis* is chosen for providing the support of the MAC layer. It provides various IEEE 802.11 protocols and this thesis uses its *p* variant. Pamvotis is a lightweight and highly customisable Java-based simulator that has provision to connect any mobility and radio model from outside without the developer having to touch its internal functionalities [114]. While building on top of Pamvotis, this provision ensures that the performance of the MAC layer will remain unaltered.

The two network layer protocols and warning systems, VSPCA and RBSM, are implemented using Java based on the description provided in the respective publications. An application layer protocol is also developed using the same language that generates periodic warnings at a defined rate. For the single-hop broadcast protocol, a simple network protocol is developed to act as an interface between application and MAC layer. Its operation is limited to passing warnings between its top and bottom layers. Figure 4.2 shows how the simulator looks like with protocols at their appropriate layers. In addition, after considering several radio models that attempt to create vehicular environments such as [115, 116, 117], [118] is developed and integrated with the simulator.

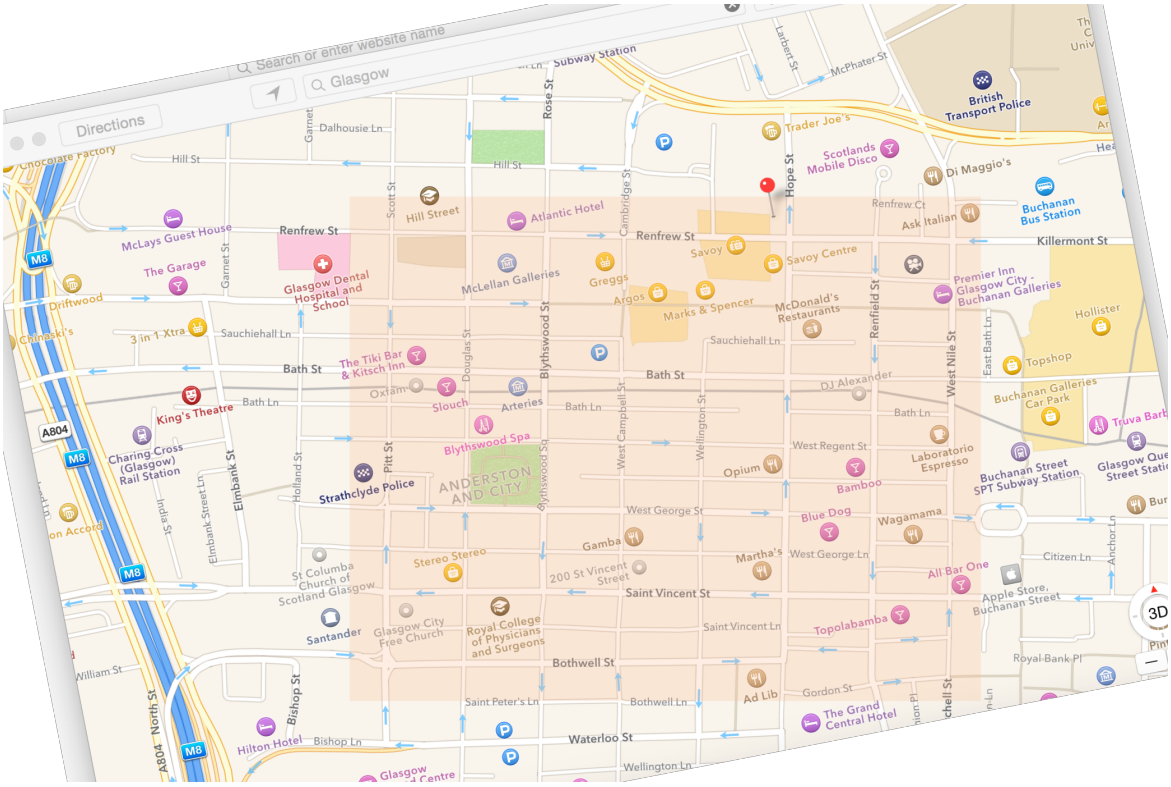



Figure 4.3: The area covered by Glasgow Mobility Model (GMM).

### 4.4.2 Mobility Model

Mobility models are used to evaluate performance of wireless protocols and algorithms by simulating them in an environment where the nodes are in motion. There are two possible types of mobility model found in the literature, namely trace and synthetic models [119]. Trace is based on the measured movement of real nodes whilst synthetic models follow a mathematical formula that artificially approximates such movement. In the context of AWS, trace is not a good choice, since it cannot be expected to generate possible accident scenarios. Although synthetic models are often considered unrealistic, in the current experiment, they can produce approximately realistic movement if some auxiliary information is fed in the real environment. [120] named such hybrid schemes, "synthetic model starting from real traces". This thesis develops a model of this type called the *Glasgow Mobility Model*.

The model uses a real location, Glasgow City Centre, as the simulation arena in the designed environment. This location is an excellent example of a grid-road scenario where roads run from East to West and North to South setting up an ideal urban environment for testing warning systems. Figure 4.3 shows Glasgow City Centre on an online map. The highlighted area is the busiest part of the centre and also the active experimental region in this simulation. A noticeable feature is direction of the movement of the vehicles. All roads in the centre area are unidirectional as shown on the map via light-blue arrows. While developing the mobility model, these directions are strictly followed.

| *Density* | *Name* |
|---|---|
| *(vehicle)* | *(Streets in Glasgow City Centre)* |
| 10 | Douglast St. / West Campbell St. / Welington St. |
| 20 | Bothwell St. / Pit Street / Blythswood St. |
| 30 | Bath St. / West Regent St. / West George St. / West Nile St. |
| 40 | Sauchiehall/Renfrew St. / Saint Vincent St. |
| 50 | Hope St. / Renfield St. |

Table 4.1: The network densities of the Glasgow City Centre.
These are used as the vehicle generation rates in the simulation.

In addition, the model uses realistic vehicle density on the roads. To achieve this goal, the author measured peak hour vehicle movement by visiting the location on five consecutive working days of a typical week. Table 4.1 shows streets and their average density where data is rounded to the nearest whole number.

Finally, each road is assigned a *source* and a *sink*. Sources generate vehicles at the appropriate rate which start to move from an initial trace but follow a formula that leads them towards the sink. When a sink absorbs a vehicle, it immediately passes it to the corresponding sink so that the vehicle can be sent back on the street. During this exchange, all the communication parameters of the vehicles kept unchanged.

While moving, each vehicle is assigned one of the following velocities: 10 mph, 30 mph and 50 mph. It is noted that in the United Kingdom, 30 mph is the maximum legitimate speed a driver can maintain in a city area. The speed domain includes a slower speed than the maximum allowed as well as a faster speed that is illegal but sometimes drivers reach that limit. In this study vehicles cannot vary their speed over time.

## 4.5 Definition and Assumption

This chapter and the subsequent chapters will use the following definitions and make the succeeding assumptions while conducting studies unless stated otherwise. If any additional definition or assumption is needed for a particular study later, it will be explicitly stated in the description of that chapter.

- The term *traffic load* will always be used in this thesis to represent data traffic load. The term *network density* or *vehicle generation rate* will be used to mention the density of vehicles on the streets. Similarly, the term *collision* will only imply transmission collisions. The situation involving vehicles colliding with each other will be expressed as *accident*. This thesis will also exchangeably use the terms *node* and *vehicle* and therefore, these are going to indicate the same entity.

- Throughout this thesis, *blind movement* will be the situation when a vehicle passes a junction with a transmission queuing delay larger than the previously defined (in Section 4.2) maximum tolerable queuing delay. If a vehicle, either while moving straight or at a junction, collide with another vehicle in such a situation that at least one of them failed to receive a warning prior to the collision, then that situation will be called a *potential accident*. However, if both vehicles receive a warning before colliding, that incident will be considered as *safe movement*. It is because in real-life after receiving warning drivers of the involved vehicles either stop or avoid the collision. As in the simulation it is kept running until the end, vehicles are allowed to move even if a potential accident is detected.
- Figure 3.6 on page 38 shows that for 24 Mbps data rate, coverage radius is 40m whilst for 12 Mbps rate, it is as large as 135m. In this thesis the average of these two coverage is taken and nodes are configured with transmit power in such a way that they cover a radius of 88m.
- This thesis assumes that in all studies nodes will have constant power supply at all time and their transceiver will remain active always. All nodes also operate with same transmission range unless stated otherwise.

## 4.6 Performance Metrics

Performance metrics are used to measure the efficiency of the network. They are also an indicator of how good or bad the protocol being examined actually is. In this chapter, studies use performance metrics from both network and application layer. Detailed descriptions of each of those performance metrics are presented below.

### 4.6.1 Network Layer Metrics

At the network layer, two metrics are evaluated: i) *Rate of Collision*, a metric that expresses number of transmission collisions encountered by a node (i.e. vehicle) every second during the simulation time; and ii) *Queuing Delay*, a metric that expresses on an average how long a warning needs to wait at the respective transmission queue from the time of its generation in millisecond.

### 4.6.2 Application Layer Metrics

At the application layer, five metrics are evaluated. The first three metrics are evaluated at junctions and do not count how many times they occur; rather at how many junctions they

occur in. These are as follows: i) *Accident-at-junction*: a metric that expresses a potential accident occurred at a particular junction; ii) *Blind-move*: a metric that shows a particular junction has blind movement; and iii) *Safe-move*: a metric that indicates a particular junction has safe movement. If a junction encounters a potential accident, it will be counted towards accident-at-junction. However, if a junction encounters no potential accident but at least one blind movement, it will be counted towards blind-move. All other junctions will be counted towards safe-move. Two other metrics are evaluated that give total number of *Potential Accident Undetected* and *Potential Accident Detected* during the simulation.

## 4.7 Method of Study

This chapter aims to analyse performance of warning systems focusing on the effect of broadcast storm on different types of broadcast schemes that force vehicles to run with transmission queuing delay more than the previously defined *MTQD*. To achieve this goal, the custom-built simulator described earlier in Section 4.4.1 is used and a closely imitated real-life motor traffic setting of Glasgow city centre representing the single carriage way scenario in urban layout described in Section 3.3.1 of Chapter 3 is constructed. This environment assists simulating and observing behaviour of the experimental protocols with a wider range of freedom. First, it allows to populate vehicles from the source in a very specific order with a view to measure certain aspects in relation to incidents. Second, it helps monitoring each street and junction separately to have a wider understanding. And third, it allows to generate and disseminate warnings as per the need of the study.

Two studies have been conducted in this chapter with each having two versions – *moderate* and *heavy*. The moderate version examines the network with a moderate probe of either data traffic load or network density whilst the heavy version shakes the network with a probing that could well be considered “not normal” in general.

The first study investigates the effect of data traffic load on the performance metrics. These studies varied data traffic load between 1 to 25 warning/sec to inspect how performance metrics react in response to this variation. Based on the reciprocation received from the performance metrics, this study finds a suitable warning generation rate for what queuing delay stays below *MTQD*. This rate will be later used in the second set of studies as the moderate data traffic load. No application layer performance metrics are evaluated in this study and initial assignment of vehicles on the streets does not have a specific order.

The second study investigates the effect of network density on the performance metrics of the experimental warning systems at different network densities. This study has two objectives as it evaluates both network and application layer metrics. The network layer component


Figure 4.4: Junctions used in the studies to evaluate *accident-at-junction*, *blind-move* and *safe-move* in this current chapter and in Chapter 7.

examines warning's transmission collisions in the network and subsequently inspects prolonged queuing delays. Collision indicates how stiff the competition is to get access to the medium whilst delay reveals the consequences of that competition. In this study, protocols suffering from more than two second delay are considered inadequate and later application layer counterpart reconfirms that by showing their vulnerability in preventing accidents.

At the application layer, it has been determined how many junctions in figure 4.4 have blind-move and accident-at-junction. In addition, the number of potential accident undetected both at junction and on straight streets during the simulation is also evaluated. To have a better understanding over the results of this segment of the study, vehicles are generated in a particular order at the sources. It is mentioned earlier in section 4.4.2 that streets in Glasgow city centre are one-way (unidirectional) and the developed mobility model strictly mimicked that characteristics. It is assumed for simplicity that there are two lanes on each street and three fixed velocities available for vehicles. Instead of randomly assigning lane and velocity, this is intentionally conducted in such a way that a vehicle with higher velocity cannot follow a vehicle with lower velocity in the same lane as to avoid any collision. This rule, however, is only broken for two highest velocity vehicles who are placed at the very back of the street. These two vehicles pass through slower vehicles in front of them as simulation progresses. With the help of this setup, potential accidents are deliberately created to evaluate how many of such accidents go undetected when vehicles operate with various warning systems.

In this study, streets are grouped based on their network density. For example, all streets having 50 vehicle/min density are grouped together by averaging their performance metrics and so on. It could have been possible that the graphs are being prepared by street names but that would not clearly demonstrate the context of the results which is network density in this case.

## 4.8 The Effect of Data Traffic Load

The study of the effect of data traffic load is conducted by varying warning generation rate of the vehicles while keeping other parameters fixed. This study will be in two folds with two different network density. The first network density is named *moderate* because it runs the simulation with 5 vehicle/min network density whilst the second density is called *heavy* and it uses 15 vehicle/min network density. There are two performance metrics that will be evaluated in this study. These are *rate of collision* and *queuing delay*. Simulation will run for 60 sec and the simulator collects data throughout to prepare the graphs.

### 4.8.1 Network Density: *Moderate*

The study of the effect of data traffic load in moderate network density varies data traffic load from 1 to 25 in order of 1, 5, 10, 15, 20 and 25 warning/sec. An average of 20 trials is finally taken to prepare the graphs.

#### 4.8.1.1 Rate of Collision

It has been previously noted that contention for medium access occurs in wireless networks due to excessive rebroadcast [104, 105]. This study further investigates the issue in the context of accident warning systems. Figure 4.5 demonstrates the effect of traffic load on collision rate in moderate network density. This study finds a relationship between the rate of data traffic load and rate of collision in the network. It shows that collisions occur more frequently as data traffic load increases in the network and follows a sharp increase with the growth of the load generation rate. It is notable that RBSM that uses limited-scoped broadcast, and VSPCA that uses flooding, experience this sharp increase at an early stage and later 802.11p follows the same pattern.

The number of collision, however, is not similar for all three warning systems. 802.11p encounters fewer collisions compare to the other two when data traffic load stays below 15 warning/sec. RBSM and VSPCA performs relatively similar throughout the study and become stable at 80 collision/sec when data traffic load is 15 warnings/sec or more. The

most notable attribute observed in this study is how 802.11p responds when data traffic load surpasses 20 warning/sec. This system in such situation encounters more collisions than RBSM and VSPCA in spite of forwarding warnings no more than a single hop distance.

This study also finds that network does not suffer from contention when data traffic load is 5 warning/sec or less. With data traffic load increasing further, protocols are more likely to encounter excessive collisions that result in creation of broadcast storm in the network.

#### 4.8.1.2 Queuing Delay

Figure 4.6 shows that there exists a relationship between data traffic load and the queuing delay of warnings and that the latter increases rapidly as data traffic load grows. This is when warnings in the transmission queue fails to obtain medium access due to excessive contention. As the wireless networks transfer data sequentially, when a node attempts to deliver data via the wireless medium, other nodes within its transmission range must back-off to avoid potential interference, as described in Section 2.4.4 of Chapter 2. Because of this phenomenon warnings waiting in the queue must stay there until the sender receives access to the medium.

From the figure mentioned above, it is evident that the performance of RBSM and VSPCA are almost identical. This is because at a network density of 5 vehicle/min, these two systems perform in a similar fashion. As data traffic load grows, both face a sharp rise in their queuing delay and at the peak of 25 warning/sec this delay hits nearly 4 sec, a delay almost twice of the $MTQD$, for each warning system. 802.11p, however, performs better because of not rebroadcasting warnings. It remains unaffected and maintains a consistent and very small queuing delay throughout.

This study finds that 5 warning/sec is a suitable warning generation rate as queuing delay of all three protocols for that rate is minimal. However, RBSM and VSPCA stays within the border line of the $MTQD$ when this rate is 15 warning/sec.

### 4.8.2 Network Density: *Heavy*

The study of the effect of data traffic load in heavy network density, like its *moderate* counterpart, is conducted by varying the warning generation rate between 1 to 25 warning/sec. However, the network density in this study will be 15 vehicle/min. Three performance metrics evaluated in previous section will be used again in this study.

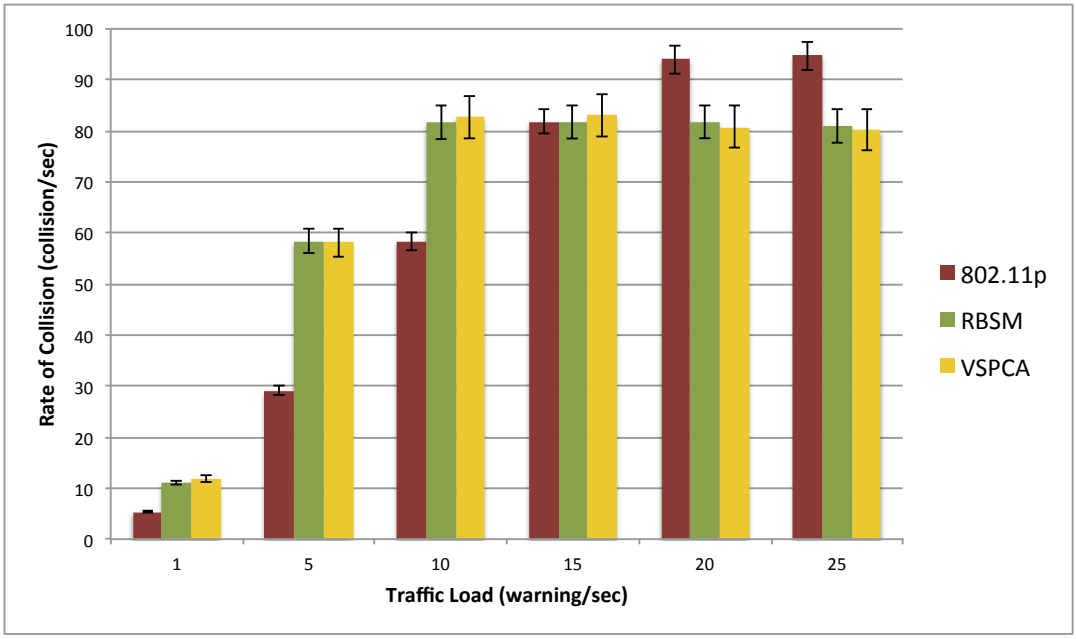



Figure 4.5: The effect of data traffic load on rate of collision in moderate network density.

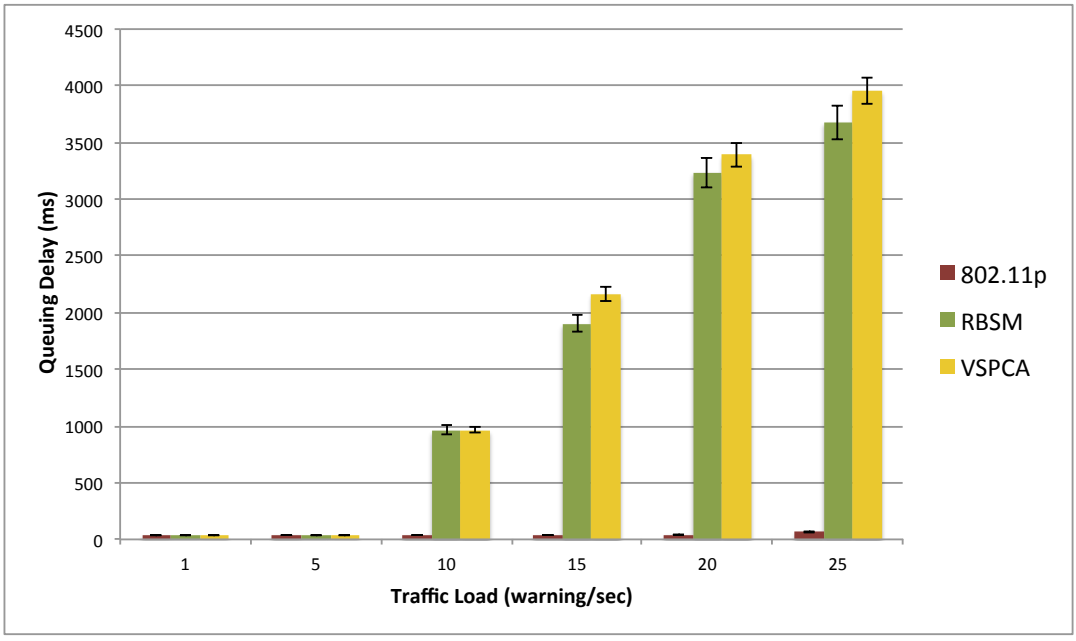



Figure 4.6: The effect of data traffic load on queuing delay in moderate network density.

#### 4.8.2.1 Rate of Collision

Figure 4.7 demonstrates the effect of data traffic load on collisions at heavy network density. It shows that all three systems exhibit sharp increase as in the case of moderate network density but now starts earlier. Like the previous study, 802.11p initially maintains a slower growth but later surpasses the others. It is, however, notable that despite having network density of three times to the previous study, the rate of collision does not change. This is an indication that although the growth of the network density plays an important part in creating contention in the network, but contention does not follow the growth strictly by getting increased proportionally.

#### 4.8.2.2 Queuing Delay

Figure 4.8 further demonstrates that there exists a relationship between data traffic load and the queuing delay of warnings. As explained earlier, this happens because nodes fail to obtain medium access due to excessive contention. This figure also shows that queuing delay in heavy network density is sharply higher in comparison to the previous experiment where more than 5 warning/sec rate was required to have such growth.

It is also evident from this study that performance of limited-scoped based RBSM and flooding based VSPCA are almost identical and at the peak of the data traffic load of 25 warning/sec, this delay exceeds 3 sec for each system. 802.11p, however, performs better and exhibits identical behaviour to the case of moderate network density. It is also evident from this experiment that performance of limited-scoped based RBSM and flooding based VSPCA are almost identical and at the peak of the traffic load with 25 warning/sec, this delay hits above 3 sec for each system. 802.11p, however, performs better and exhibits identical behaviour that it demonstrated earlier in moderate network density.

This study reconfirms that 5 warning/sec is a suitable warning generation rate. Despite the fact that the network density is 15 vehicle/min, both RBSM and VSCPA stays within the $MTQD$.

### 4.8.3 Summary of the Study

The study of the effect of data traffic load is one of the two studies performed in this chapter to accomplish the second research objective, i.e. whether the existing broadcast-based warning systems can comply with the two-second rule and maintain a queuing delay below the $MTQD$ threshold.

The current study diagnoses how warning systems perform in response to data load and shows that collisions occur more frequently as data traffic load increases in the network and

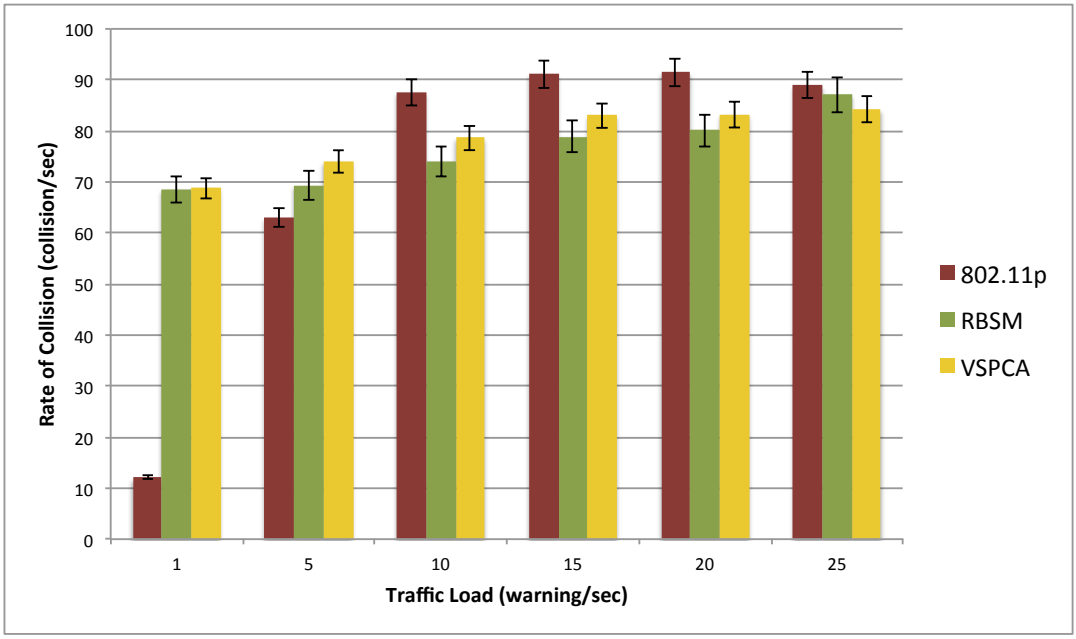



Figure 4.7: The effect of data traffic load on rate of collision in heavy network density.

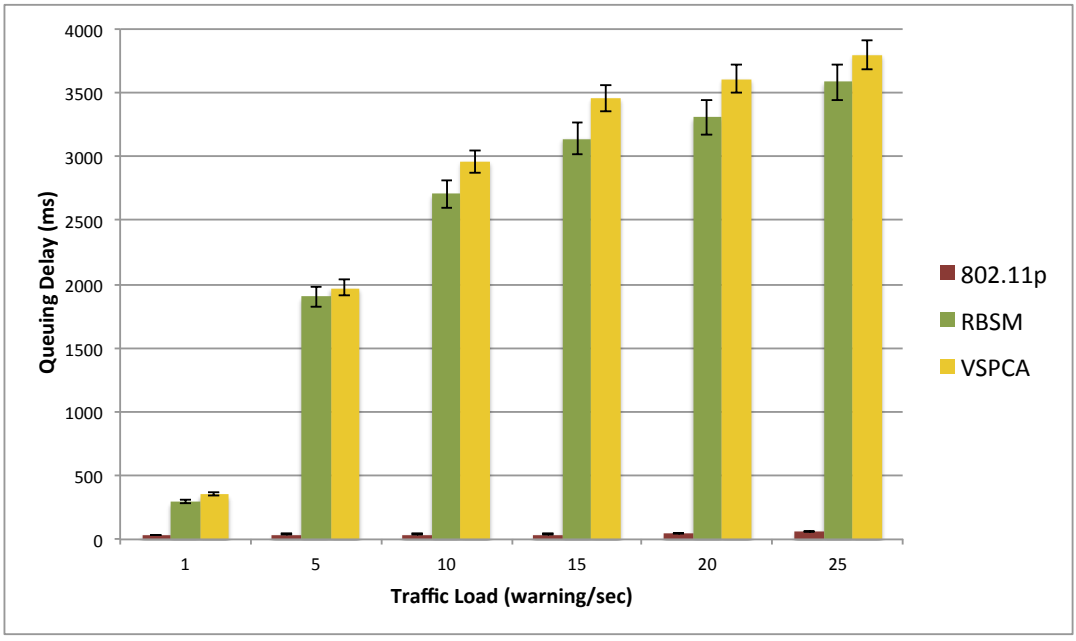



Figure 4.8: The effect of data traffic load on queuing delay in heavy network density.

follows a sharp rise with the growth of the warning generation rate. It also identifies that network does not suffer from contention when data traffic load is 5 warning/sec or below with network density 5 vehicles/min. However, as data traffic load increases further, warning systems are more likely to encounter excessive collisions that result in creation of broadcast storm in the network. This study finally relates collision with the queuing delay and identifies that as the likelihood of having a broadcast storm increases, the queuing delay increases too. It strengthens this discovery by showing a queuing delay in 15 vehicle/min network density (three times larger than the previous load) that sharply grows in comparison to the low network density.

Based on the above summary, this study partially fulfils the second research objective of the thesis and confirms that existing warning systems can not comply with the $MTQD$ threshold with growing data traffic load in the network. Nevertheless, it finds that 5 warning/sec is a suitable warning generation rate as in both 5 and 15 vehicles/min network densities, warning systems maintain a queuing delay below $MTQD$ while operating with this rate. Thus, from the findings of this study it is recommended that warning systems should use this rate to generate PWMs to warning neighbouring vehicles around the host.

## 4.9 The Effect of Network Density

The study of the effect of network density is performed by varying density of vehicle while keeping other parameters fixed. This study will be in two folds with two different data traffic load. The first data traffic load is named *moderate* because it uses a suitable probe of 5 warning/sec recommended in the previous study. The second is called *heavy* and it uses 15 warning/sec data traffic load. This study will be conducted to evaluate all five performance metrics mentioned in section 4.6 and the simulation runs for 60 sec.

### 4.9.1 Data Traffic Load: *Moderate*

In this phase of the study, the network density is determined by the rate of vehicle on streets shown in table 4.1. Five values of network density, 10, 20, 30, 40 and 50 vehicles/min, are used in this study. An average of 20 trials are taken for each metrics for preparing the graphs.

#### 4.9.1.1 Rate of Collision

Figure 4.9 shows the number of collisions (transmission collisions) in the network. It is evident from the results that when more vehicles enter into the same enclosed area, competition

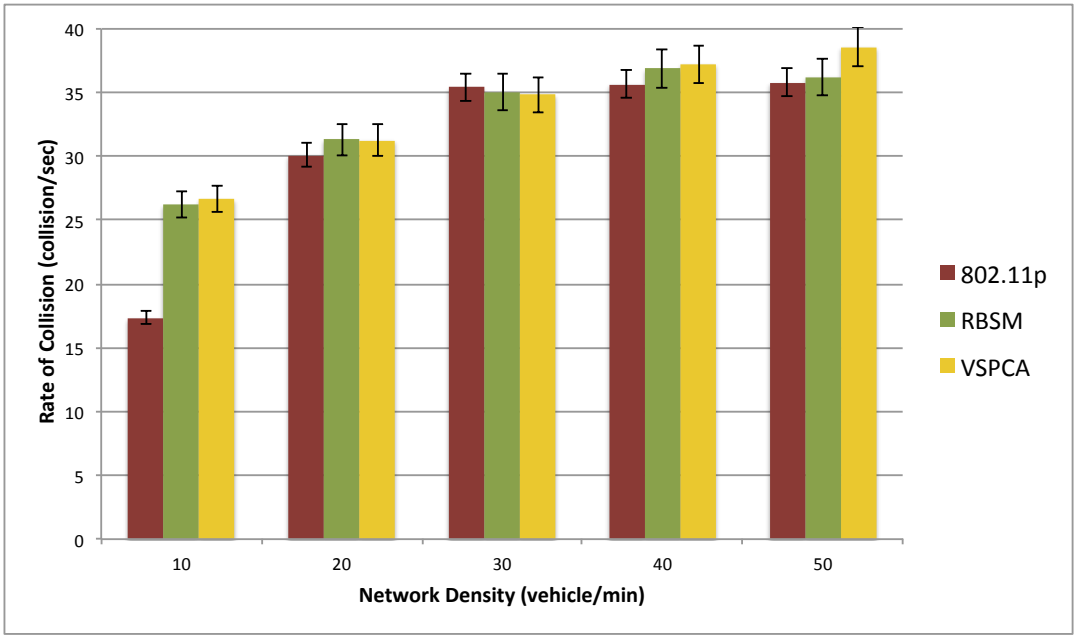



Figure 4.9: The effect of network density on collision in moderate data traffic load.

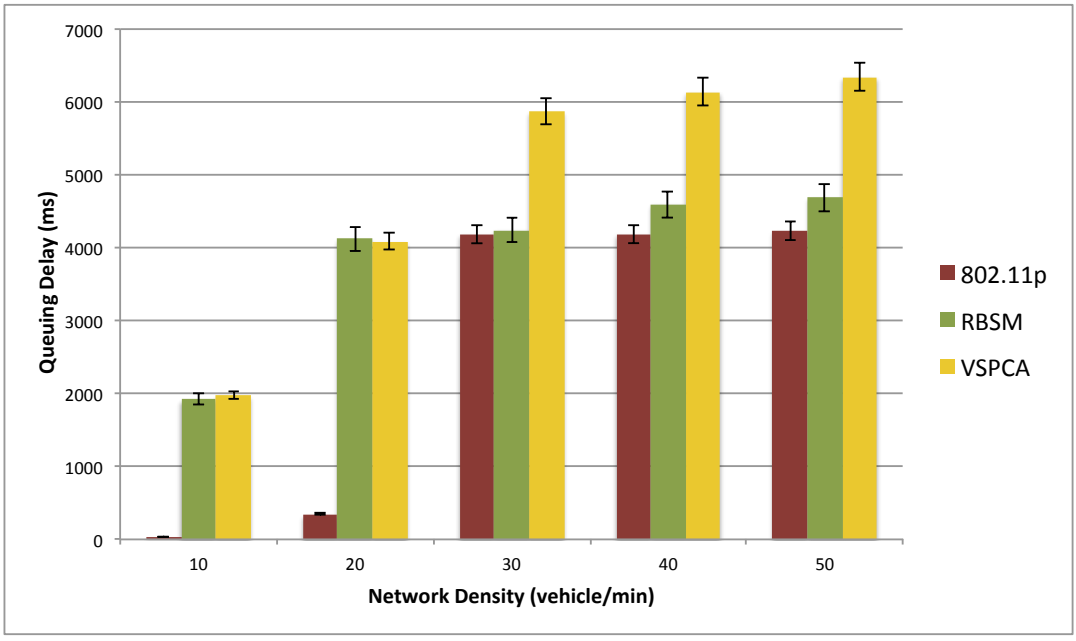



Figure 4.10: The effect of network density on queuing delay in moderate data traffic load.

for accessing the medium gets stiffer and streets with more vehicles tend to have more collisions. This behaviour suggests that as network density increases, number of rebroadcasts of warning message significantly increases in the network that ultimately results in broadcast storm.

The results show that both RBSM and VSPCA that have limited-scoped and flooding technique respectively encounter more than 25 collisions when network density is 10 vehicle/min. The IEEE 802.11p beacon, however, encounters less collisions because it does not rebroadcast warning message. However, as network density increases, broadcast storm looks severe and all three system see more than 40% rise in collisions.

#### 4.9.1.2 Queuing Delay

The results in figure 4.10 demonstrate the effect of network density on the queuing delay of warnings while operating with moderate data traffic load. It clearly shows that like the previous results, there exists a relation between queuing delay and network density; and with more vehicles entering on a street, competition for accessing the medium gets stiffer. It also demonstrates that collision is a cause generated by broadcast storm and queuing delay is its consequences.

VSPCA exhibits a sharp rise that begins with a delay just below 2 sec initially but becomes double as the network density doubles. Subsequently this delay touches 6 sec, three times than $MTQD$, when network densities are between 30 and 50 vehicle/min. This behaviour can be explained by realising that as the number of vehicles increases in the network, number of rebroadcasts also increases that result in broadcast storm and subsequently long queuing delay. As RBSM only forwards warning up to five hop distance and therefore generates less rebroadcast than flooding. Thus it exhibits less queuing delay compared to VSPCA. When network density is not high, both of these systems perform almost identically. This is due to the fact that during this phase distance between any two vehicles could have been rarely more than five hops. However, when number of vehicle increases, possibility of obtaining path longer than five hops becomes prominent and performance of limited-scoped based RBSM deviates from its flooding counterpart. It is also noted that IEEE 802.11p exhibits small queuing delay for network density of 20 vehicle/min or less. Nevertheless, it shows a very sharp rise afterwards and continues with a queuing delay similar to RBSM.

#### 4.9.1.3 Junctions

There are total 44 junctions in the simulation as shown in figure 4.11. When vehicles moved through these junctions, three situations can occur: i) Accident-at-junction; ii) Blind-move; and iii) Safe-move.

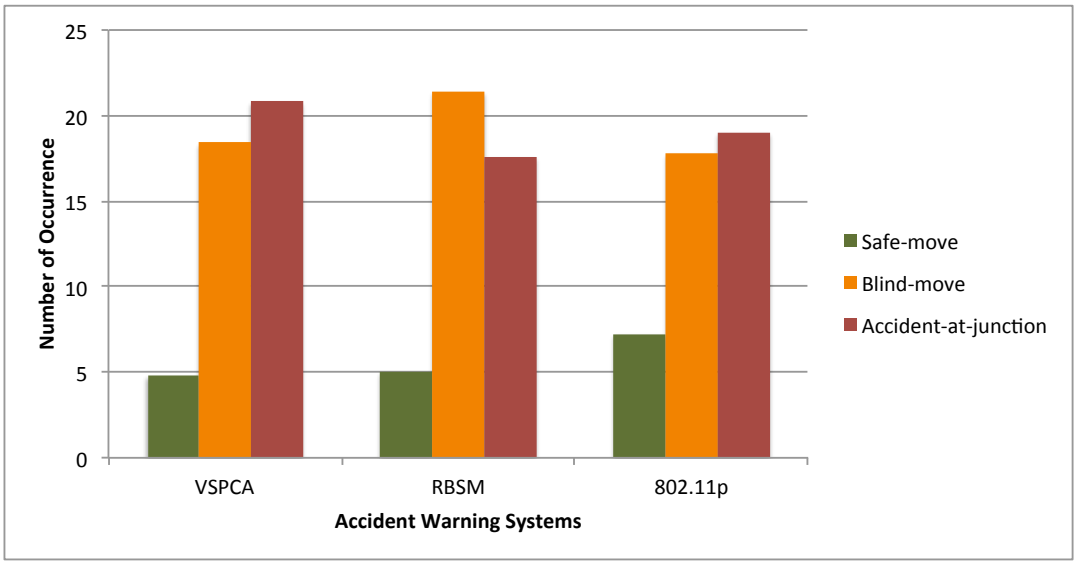



Figure 4.11: Movements at the junctions in moderate data traffic load

Figure 4.11 demonstrates that flooding-based VSPCA encountered more accidents than any other protocol whilst RBSM encountered more blind-moves. Results showed in section 4.9.2.1 and 4.9.1.2 explain this behaviour. As these two warning systems experienced long delays in high network densities, they either encountered more potential accidents or had numerous blind-movement at junctions. It is, however, notable that despite showing better performance than the other two systems in terms of delay, the IEEE 802.11p beacon also encountered significant number of accidents at junctions. It is because with its more limited coverage vehicles often fail to propagate warnings to the appropriate recipients.

#### 4.9.1.4 Potential Accident Undetected

The streets are grouped based on their densities in this simulation and the number of potential accident undetected in those groups are recorded during the simulation. In section 4.7, it is mentioned earlier how vehicles are placed on the street at the beginning of the simulation. Two vehicles with 50 mph velocity from the very back hit slower vehicles while moving forward. These deliberate actions make sure that accidents occur in the simulation and therefore pave the way for testing the effectiveness of the warning systems.

Figure 4.12 shows VSPCA has more potential accidents undetected than any other warning systems whilst RBSM and 802.11p performs almost identically except for the highest network density. The performance observed here is quite simple to understand: when vehicles experience long queuing delay, they fail to disseminate warning messages on time that ultimately makes their warning systems vulnerable. It is important to realise that in spite of having a better queuing delay than RBSM for the network density 20 vehicle/min or less, 802.11p did not perform better because while quicker delivery of the warning messages is

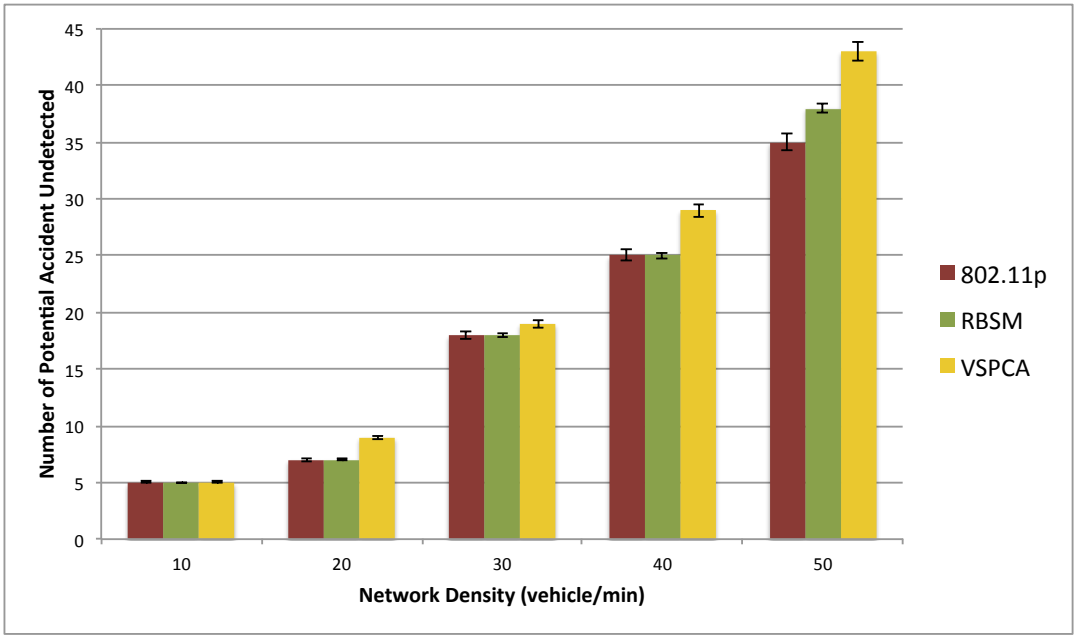



Figure 4.12: The number of potential accident undetected in moderate data traffic load.

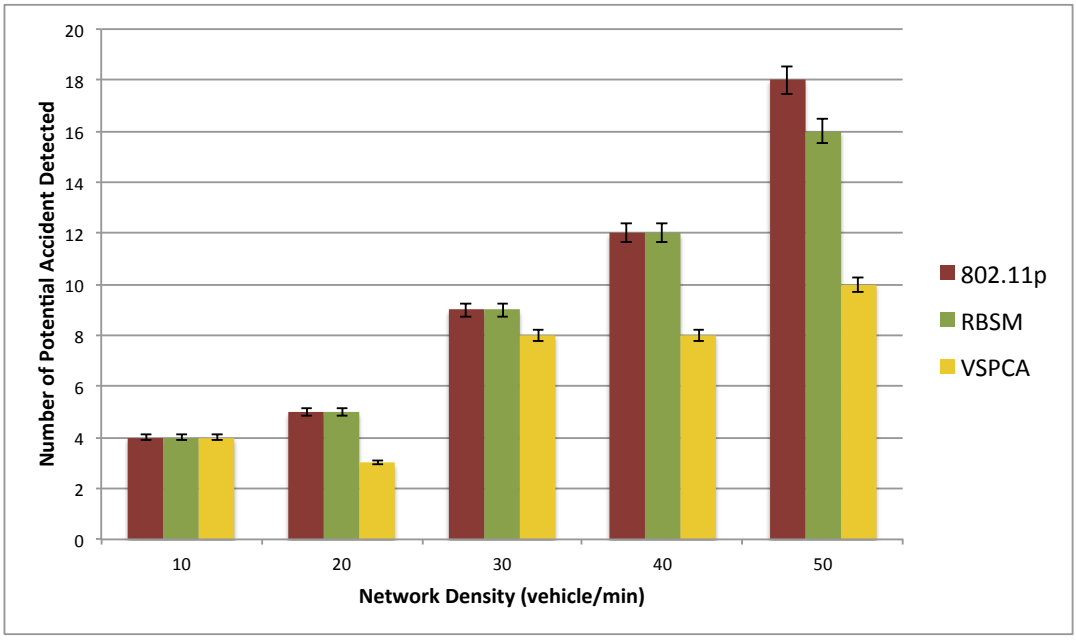



Figure 4.13: The number of potential accident detected in moderate data traffic load.

important, spreading the message to the right audience cannot be overlooked either. Having covered only one hop distance neighbours, 802.11p fails to spread the warnings to all required vehicles.

It is also notable that in high network densities the number of potential accident undetected remains between 35 and 45 whilst in the low network densities it is just around 5. This is reasonable to understand that broadcast storm influences this performance in an unfavourable way by pushing the queuing delay towards or more than $MTQD$. To improve performance of the warning systems, a countermeasure is, therefore, required that should prevent broadcast storm being generated in the network; hence keeps the queuing delay below $MTQD$.

#### 4.9.1.5 Potential Accident Detected

The number of potential accident undetected gives a picture of how badly the systems perform. However, it does not give the account of how many accidents being detected and a complete picture cannot be observed without exploring both metrics. Figure 4.13 demonstrates the number of potential accident detected during the simulation. While VSPCA encounters nearly 45 accidents in the high densities, it only detects around 10 potential accidents. So roughly, for every five potential accidents, VSPCA is capable of detecting only one. The other two warning systems perform relatively better as they are capable of detecting one out of three accidents.

### 4.9.2 Data Traffic Load: *Heavy*

In this phase of the study, a traffic load of 15 warning/sec is used to observe how performance metrics respond to such a heavy data traffic load. Like the previous study, the network density is determined by the rate of vehicles on streets shown in table 4.1. Five values of network density, 10, 20, 30, 40 and 50 vehicles/min, are used. An average of 20 trials are taken for each metrics.

#### 4.9.2.1 Rate of Collision

Figure 4.14 shows the number of collisions in the network in the presence of heavy data traffic load. If this result is compared with the previous results described in , a slight increase of collision can be observed for similar network densities. This behaviour, however, is expected because with more warning entering in the network, collision is likely to increase.

This study demonstrates that both RBSM and VSPCA encounter just over 25 collisions at the beginning but later settles between 35 and 40 collisions. The IEEE 802.11p beacon

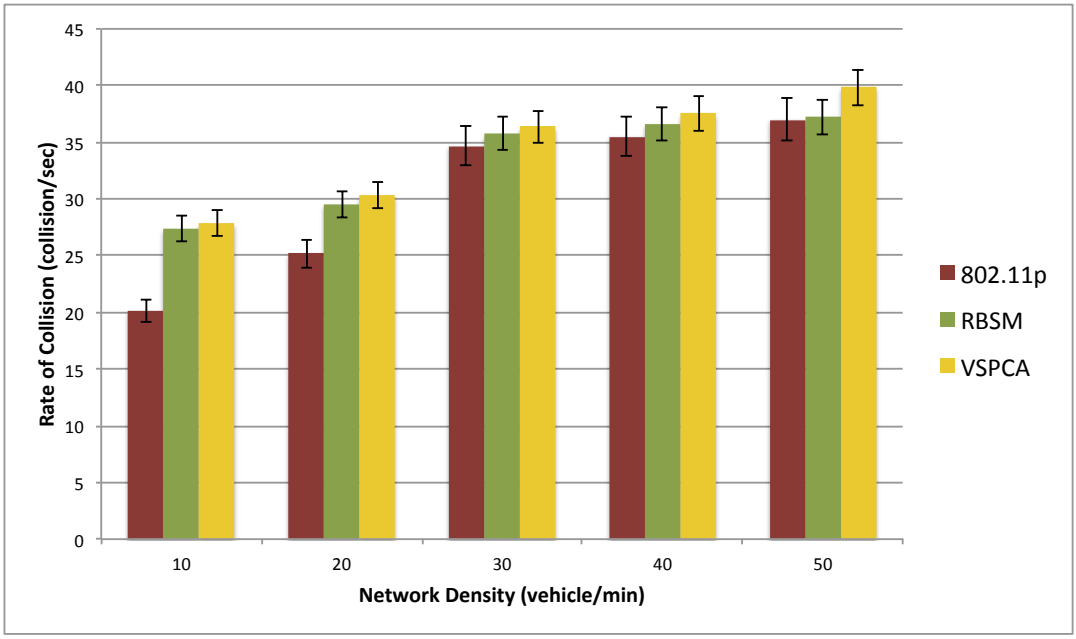



Figure 4.14: The effect of network density on rate of collision in heavy data traffic load.

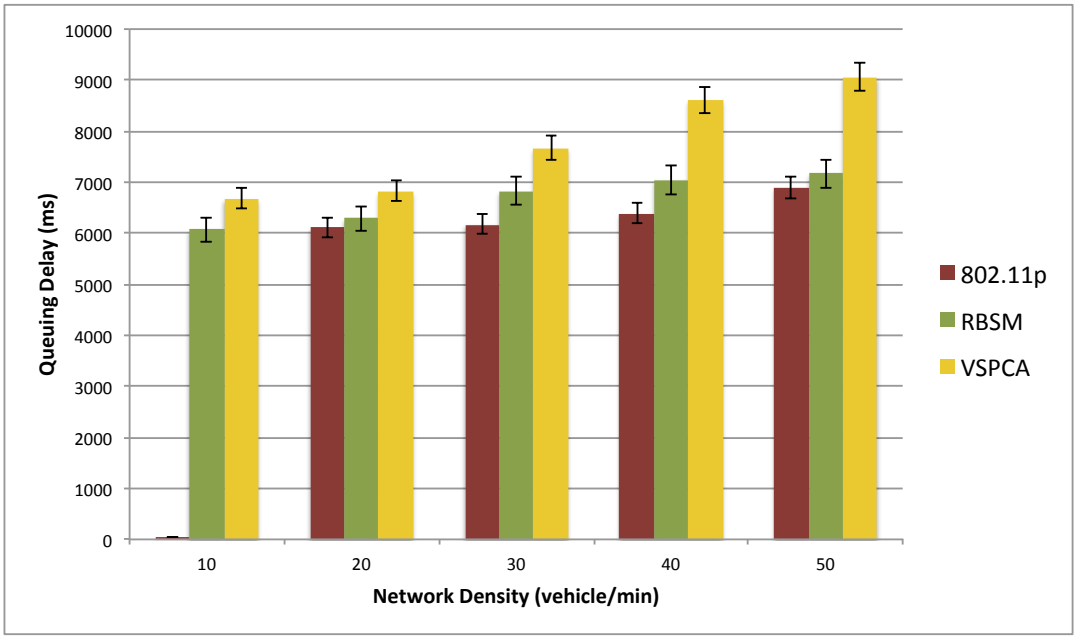



Figure 4.15: The effect of network density on queuing delay in heavy data traffic load.

encounters less collisions because it does not rebroadcast warning message. However, as network density increases, all three systems exhibit a rise in the number of collisions.

#### 4.9.2.2 Queuing Delay

The results in figure 4.15 demonstrate the effect of network density on the queuing delay of warnings while operating with heavy data traffic load. Previous section shows the large number of collisions in the network that is also an indicator of fierce competition for medium access. This figure confirms that having experienced heavy collisions (transmission collisions) by the vehicles, large delays are outcomes of the broadcast storms. It is noteworthy that due to the additional warnings in the network this delay prolonged compared to its moderate counterpart performance presented in 4.10.

This figure is evident that all three systems exhibit long delay well above the $MTQD$ from the beginning. Although RBSM and IEEE 802.11p show stable performance but VSPCA demonstrates a growth throughout the simulation period. This behaviour can be explained by realising that when number of vehicles and number of data traffic load, both increases in the network, fierce competition occurs in the network to get access to the medium. It clearly results in very long queuing delay for sender vehicles.

#### 4.9.2.3 Junctions

It is previously mentioned that there are total 44 junctions in the simulation and vehicle may experience *blind-movement* or *safe-movement* while passing through these junctions or encounter a *potential accident*. In presence of heavy data traffic load, the queuing delay sharply rises from the very beginning deviating from the performance demonstrated for a moderate data traffic load. This change in queuing delay significantly affects the statistics measured for the circumstances recorded at junctions.

Figure 7.13 demonstrates that all warning systems encounter almost same number of accidents as they do for moderate traffic load. However, the safe-move drastically reduces whilst blind-move increases for each of them. This change in behaviour is influenced by the long queuing delays that these warning systems experience even in low network densities.

#### 4.9.2.4 Potential Accident Undected

It is mentioned earlier that the streets are grouped based on their densities and the number of accidents undetected in those groups are recorded during the simulation. Section 4.7 describes the placement of the vehicles and how they are released at the beginning of the simulation on the streets.

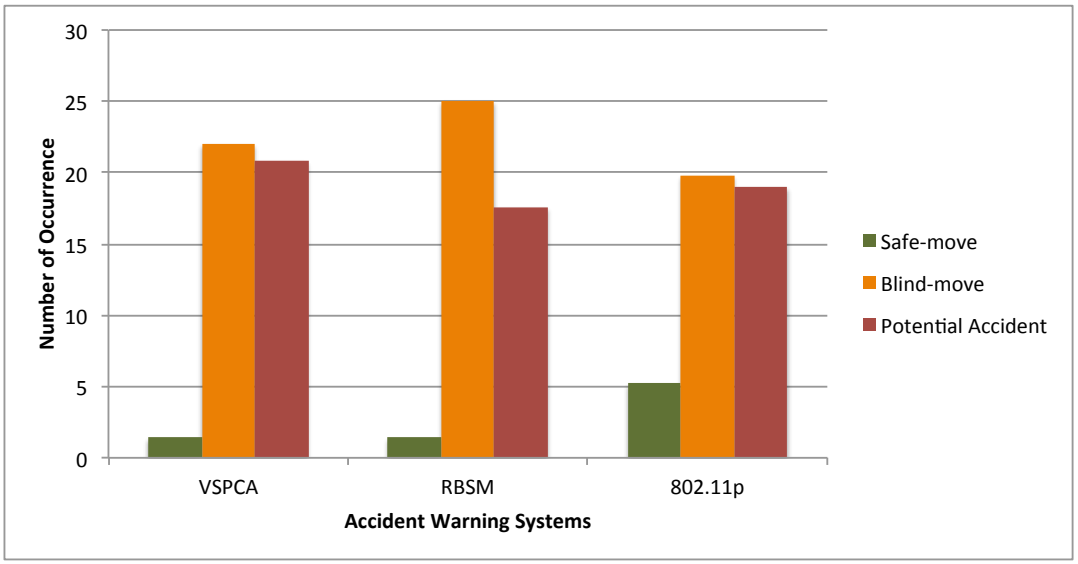



Figure 4.16: The movements at the junctions in heavy data traffic load.

Figure 4.17 shows all warning systems have more potential accidents undetected than they have in moderate data traffic load. Amongst them, however, VSPCA has more undetected potential accidents than any other system. On the other side, RBSM and 802.11p perform almost identically expect for the lowest network density. The performance observed here further confirms the fact that when vehicles experience long queuing delay (longer than $MTQD$), they fail to disseminate warning messages on time, which ultimately makes their warning systems vulnerable.

#### 4.9.2.5 Potential Accident Detected

Figure 4.18 demonstrates the number of potential accident detected during the simulation. While VSPCA has nearly 50 undetected potential accidents in the high network densities, it only has around 4 of these. This gives us roughly for every 12 potential accidents, VSPCA is capable of detecting only one when warning dissemination rate (i.e. data traffic rate) is very high, in this case 15 warning/sec. The other two systems also fail to demonstrate a convincing performance and detects only about 10% of the potential accidents.

### 4.9.3 Summary of the Study

The study of the effect of network density is performed in this chapter with a view to accomplish the second research objective. In Section 4.8.3, a summary of the effect of data traffic load is presented to partially fulfil this objective and with this summing-up, it will be completed.

This study finds that when more vehicles enter into the same enclosed area, competition for

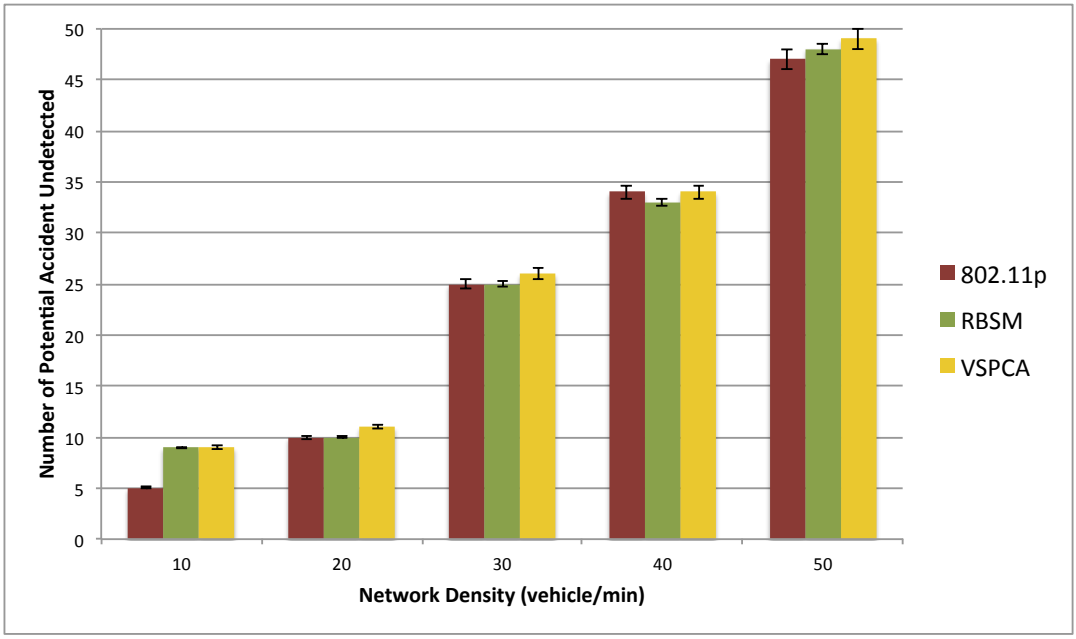



Figure 4.17: The number of potential accident undetected in heavy data traffic load.

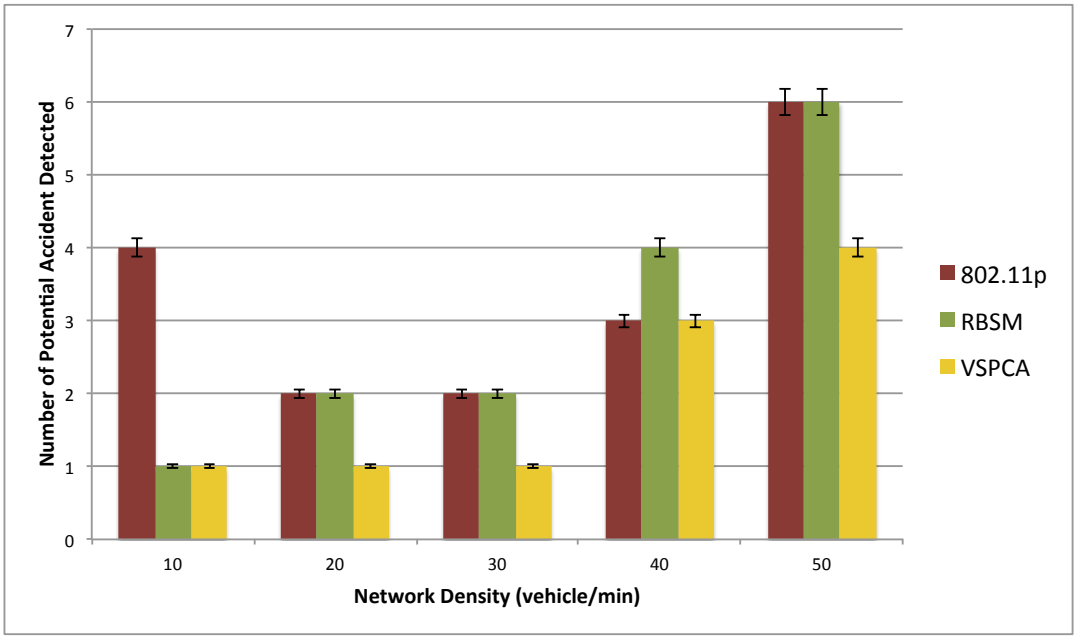



Figure 4.18: The number of potential accident detected in heavy data traffic load.

accessing the medium gets stiffer and streets with more vehicles tend to have more collisions. This behaviour suggests that as network density increases, number of rebroadcasts of warning message significantly increases in the network that ultimately results in broadcast storm. These findings then relate collision with queuing delay and shows that collision is a cause generated by broadcast storm and queuing delay is its consequences.

Based on the network layer observation, therefore, this study confirms that collisions occur more frequently as network density increases and this behaviour subsequently results in large queuing delay in the network. It further summarises that when the warning systems operate with 5 warning/sec data traffic load, they fail to comply with the $MTQD$ in high network densities. The systems are also evaluated with a heavy load of 15 warning/sec to observe their ability to perform under stressed environment and the outcome shows in such situation they fail to comply with the above threshold even in low network densities.

The observation made in the application layer finally sums-up the whole chapter by showing that failing to comply with the $MTQD$ has serious consequences as warning systems can not successfully detect potential accidents in the simulation. If the broadcast storm cannot be controlled, it remains a risk for the systems that pushes the queuing delay towards or more than $MTQD$ and subsequently makes the systems vulnerable. Therefore, it is important that an improvement in the broadcast scheme is introduced to help warning systems maintaining transmission queuing delay below $MTQD$.

## 4.10 Summary

Broadcast is the most obvious data dissemination method for accident warning systems but has the tendency to generate broadcast storms in the network that can isolate nodes for some period. As the degree of this threat was unknown, it was important to investigate how badly it might affect warning systems. This chapter has accomplished the second objective set in Chapter 1 by showing through the studies that although broadcast seems to be the most straightforward scheme for AWSs, existing systems cannot handle excessive transmissions and while going through broadcast storms, often exhibit long transmission queuing delay. This behaviour leads to the collapse of the system for more than the critical threshold of $MTQD$ in a number of situations and during these phases vehicles can move along road segments and pass through junctions with little or no ability to communicate with their neighbours. The findings of this chapter demonstrate that broadcast schemes are not reliable enough to disseminate warnings in AWSs consistently and an enhancement on top of broadcast schemes is a necessity.

# Chapter 5

# NETCODE: A new XOR-based Data Dissemination Scheme

Chapter 4 explored the inadequate behaviour of accident warning systems that operate over broadcast schemes while delivering periodic warning message to neighbouring vehicles. This chapter aims to accomplish the third research objective of the thesis by describing a warning system that aims to overcome the shortcomings demonstrated earlier by offering a solution using the generic architecture presented in section 3.4 followed by a data dissemination scheme powered by network coding technique.

This thesis proposes NETwork COded DissEmination (NETCODE), a VANET-based accident warning system, responsible for generating and sending warnings to vehicles on the road. It generates warning in both urban and highway layouts based on first-hand and shared information in a cooperative environment. Similar to the previously discussed warning systems, it uses IEEE 802.11p as its wireless communication Medium Access Control (MAC) and physical layer protocol. It also provides a set of higher layer functionalities that include warning generation, warning administration, queuing and distribution.

The NETCODE offers an XOR-based data dissemination scheme that sends multiple warning in a single transmission and therefore, reduces the total number of transmissions required to send the same number of warnings that broadcast schemes send. Hence, it reduces contention and collisions in the network that improves the delivery time of the warnings.

This chapter provides a comprehensive description on the proposed warning system. The functional building-block of the system is described in Section 5.1 followed by descriptions of addressing, types of message and packet format in Section 5.2. Section 5.3 presents the encoding and the decoding algorithms along with an example showing how they work. A state transition diagram with description of states and their transitions are given in Section 5.4. Finally, the chapter concludes in Section 5.5.

## 5.1 Functional Building-block

The NETCODE is an XOR-based coding technique that encodes multiple warnings together using *exclusive-or* operation. It generates warnings that alert neighbouring vehicles about the presence of a potential threat such as another vehicle. Although the principal contribution of this system is its data dissemination scheme, to make it functional and perform effectively, a complete system is developed from the ground up.

This system is built on top of the IEEE 802.11p protocol. For reasons of simplicity, it is designed in two separate layers namely application and network layers. Figure 5.1 shows a functional building-block of NETCODE. The only component in the figure that is not developed as a part of this system is IEEE 802.11p MAC protocol. The rest of the components altogether form NETCODE.

### 5.1.1 Application Layer

In this system, the Warning Generator (WG) and the Warning Receiver (WR) are two key components that jointly form the application layer. Of those, WG is the busiest, continuously generating periodic warning messages and occasionally event driven messages as required. The WG is also responsible for submitting these messages to the network layer for delivering to the appropriate recipients. The WR, on the other hand, is less active compared to the WG and receives messages from the network layer when it is appropriate for the host vehicle. Having received a warning, it shows the alert on the On-Board-Unit (OBU).

### 5.1.2 Network Layer

The Network layer in NETCODE is divided into two subsystems: the Processing Unit (PU) and the Delivery Unit (DU). The PU is the heart of this system as it is responsible for encoding and decoding of warnings. It also decides if a warning needs to be discarded or forwarded to neighbouring vehicles as well as be passed to the application layer.

The DU plays the role of “deliveryman” in this system. It hands over decoded received warnings to and accepts encoded new warnings from the PU. It uses broadcast to deliver warnings to one-hop neighbours. It also inserts neighbourhood information in its own warnings and with the help of the PU sends instruction for the MAC layer to include that information into the IEEE 802.11p beacon frame [121].

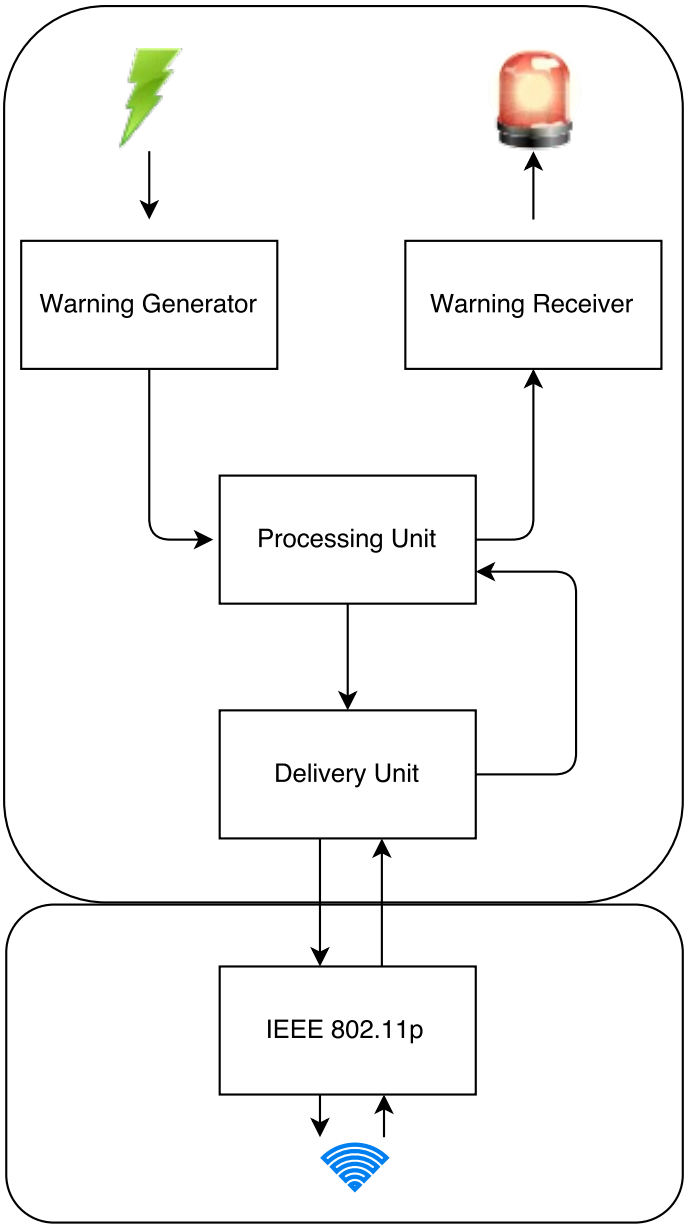



Figure 5.1: Functional Building-block of NETCODE.

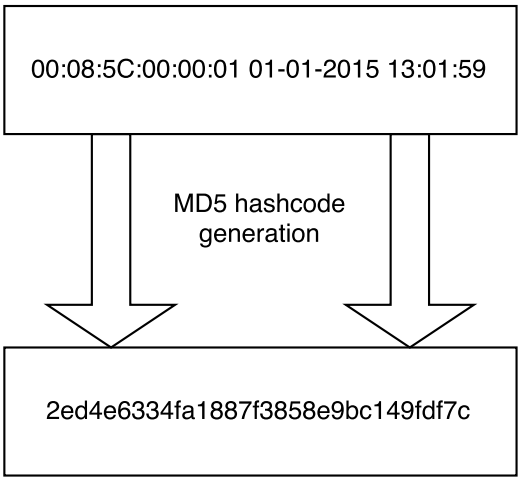



Figure 5.2: Generation of *Warning ID* in NETCODE.

## 5.2 Warning Administration

Warnings play an important role in AWSs. Vehicles not only make decisions based on warnings, but also generate and spread warnings as they sense the environment. NETCODE changes the conventional way of delivering warning to other vehicles and proposes an aggregated delivery method. This section describes how NETCODE exchanges warnings amongst neighbouring vehicles.

### 5.2.1 Addressing

The design choice of NETCODE requires unique identification of warnings at each node because of the encoding and decoding process. Keeping this in mind, warnings are given a unique identifier called a *Warning ID* and kept separate from the *packet*. In NETCODE, the term packet has a special definition and will be described elaborately later.

The Warning Generator assigns a Warning ID at the time of generation. Each warning receives an MD5 hashcode as its ID. MD5 hashcode is a 128-bit hash value presented as a 32 digit hexadecimal number [122]. The hash value (i.e. Warning ID) is generated by passing two elements: i) A string containing the host vehicle's MAC address and ii) A Warning Generation timestamp. Figure 5.2 shows how Warning ID is generated in NETCODE.

Packets are, however, identified differently. It is not required to distinguish packets uniquely in NETCODE, the reason is explained later in Section 5.2.3. The PU uses the MAC address of the respective senders to keep track of the nodes (i.e. vehicles) that send packets.

| *State* | *Contents* | *Contents* |
|---|---|---|
| *(L or F)* | *(Event-driven)* | *(Periodic Warning)* |
| Local | EDM (L) | PWM (L) |
| Forwarding | EDM (F) | PWM (F) |

Table 5.1: Classification of Warning Messages in NETCODE.

### 5.2.2 Classifications and Priority

In Chapter 3, a classification of warning message is presented. It is also mentioned that prioritising warnings can help in sending important warnings quickly. This section takes that idea into account and assigns priority based on the classification of warnings in NETCODE.

#### Classification

NETCODE warnings can be classified in two independent ways. The first classification identifies the state of the warning based on where it is generated. If a warning is generated at the host vehicle, then it is called a *local warning* whereas if it is generated by another vehicle and sent for forwarding purposes, it is identified as a *forwarding warning*.

The second classification identifies the type of the warning based on its contents. NETCODE sends two types of warnings namely *Event Driven Messages (EDM)* and *Periodic Warning Message (PWM)*. EDMs are reactive warnings sent in response to specific events such as encountering an accident, emergency braking, careless driving, and so on. PWMs are a type of warnings that are sent periodically. The primary objective of this latter type of message is to warn nearby vehicles about a potential collision in advance. Table 5.1 presents warning messages in combination of types and states.

#### Priority

The warning messages represented in table 5.1 have different priorities. From the description above, it is notable that EDMs are more time sensitive because they are generated in response to specific incidents whereas PWMs are less time sensitive as they are generated as a precaution. An “EDM (L)” has special importance because this combination implies that the host vehicle has encountered an incident and as a result of that event, this warning is generated. A PWM with local warning state i.e. “PWM (L)” embedded in the packet header is also important for the receiver because it indicates the presence of a vehicle within radio transmission range. Instead of maintaining a simple warning message queue at the network layer, NETCODE maintains a priority queue with four degree of priorities so that it

| *Priorities* | *Warnings* |
|---|---|
| | *(from Table 5.1)* |
| P1 | EDM (L) |
| P2 | EDM (F) |
| P3 | PWM (L) |
| P4 | PWM (F) |

Table 5.2: Priorities of Warning Messages in NETCODE.

can deliver sensitive warnings quickly. Table 5.2 shows the warning combinations and their priorities.

### 5.2.3 Packet

The term *packet* in NETCODE has special definition. It is a message that contains and carries one or more warnings. A packet can have coded or uncoded warnings. Coded warnings can have degree $1$ to $d$ which implies how many warnings are encoded together. As defined in Chapter 2, a warning is said to be singleton if it is not encoded i.e. its degree is 1. Such a warning implies that it is left uncoded for reasons that will become apparent shortly when encoding and decoding algorithms are explained.

A packet has two important fields namely *local warning* and *forwarding warning*. Each packet, along with packet header, contains these two fields. Local warning contains either EDM (L) or PWM (L). These warnings are generated by the host vehicle and always sent as singleton. Forwarding warning contains warnings that host vehicle receives from its neighbours and forwards for other vehicles in the network. While sending a packet, priority is determined based on the list presented in table 5.2.

EDMs are generated in response to specific event and therefore there is no fixed rate of generation for this type of warnings. However, PWMs are generated periodically. As no previous work ever mentioned at what rate warnings of this type should be generated, this thesis by conducting studies in Chapter 4 (section 4.8.3) suggests that 5 warnings per second should be appropriate to let neighbouring vehicles know about the presence of a potential hazard. Therefore, 5 PWMs are generated every second. If no forwarding warning is available at the time of sending a packet, NETCODE makes *isEmpty* field of the forwarding message true. In this way the other end of NETCODE can easily identify that the packet only contains a local warning from the sender.

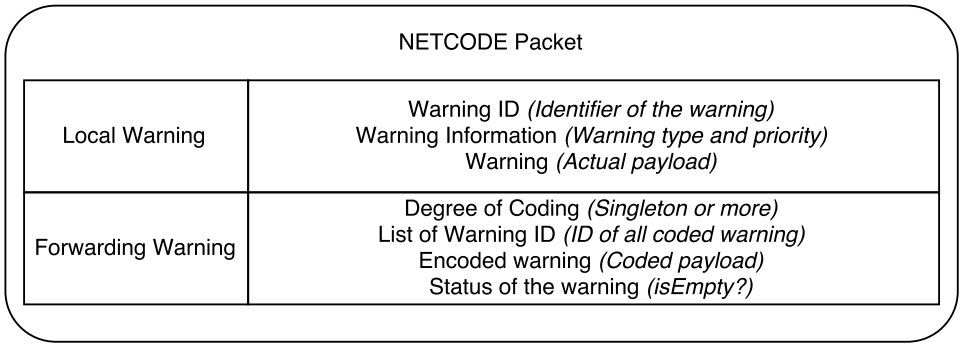



Figure 5.3: Overview of a NETCODE packet.

## 5.3 Data Dissemination

NETCODE follows the basic principles of a broadcast scheme but also conflates network coding technique with it to improve data dissemination performance. It applies an XOR-based encoding and decoding method on warnings to reduce the number of transmissions that in turn keeps the medium free for disseminating more warnings.

As shown earlier in figure 5.3, a NETCODE packet has two fields namely Local Warning and Forwarding Warning. The first field contains a single local warning whilst the second field includes forwarding warnings received from other vehicles. NETCODE only encodes the latter warnings depending on the availability of appropriate warning messages at the sender's end.

The proposed data dissemination scheme sends packet through one-hop broadcast to surrounding neighbours. However, unlike other broadcast schemes, neighbours do not rebroadcast the packet. Instead, every time a vehicles receives a packet from its neighbours, it extracts the content, stores local warnings, attempts to decode encoded forwarding warnings and if successful, keeps the warnings in a message pool that later acts as the source of warnings for the encoding algorithm.

The following subsections describe this data dissemination method along with the encoding and decoding algorithms in detail. It also sets up the basis of a series of rigorous evaluations presented in Chapters 6, 7 and 8.

### 5.3.1 Motivation

As reviewed in Chapter 2, one of the main challenges in using network coding in a routing protocol is how quickly message can be decoded. In the context of accident warning systems, this challenge becomes the biggest challenge. Even if we transmit a warning very quickly but cannot decode it to read the contents, it is not going to help detecting a potential

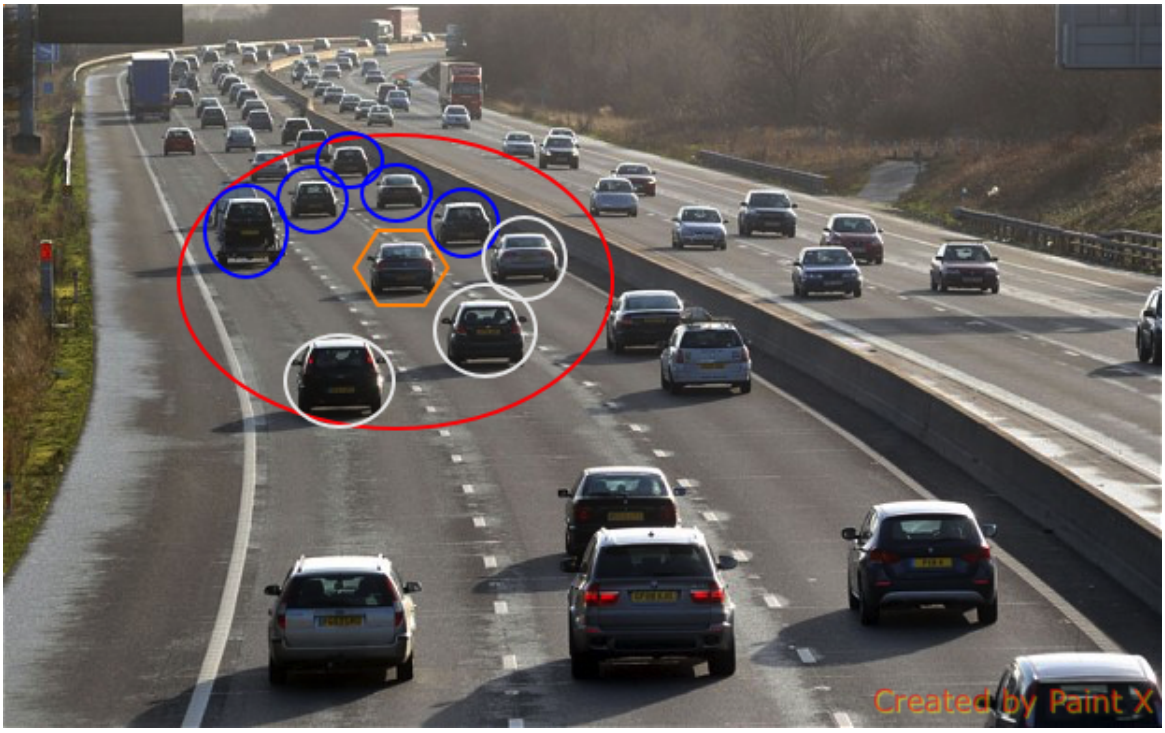



Figure 5.4: The movement of vehicles on road.

collision. Therefore, it is very important that warning systems not only transmit the warning quickly but also decode it at the shortest possible time. Keeping this objective in mind, this thesis proposes a pair of efficient encoding and decoding algorithms that work together. The encoding algorithm finds the order of encoded packet in such a way that the decoding algorithm can decode it without having to wait for further warnings to come in.

The motivation for the design choice of this pair of encoding and decoding algorithm came from the movement of the vehicles on road. If we carefully look at the movement, we notice that roads can be treated as a one-dimensional structures of negligible width. Therefore, we can assume that warnings arrive from only two directions – front or rear, except in the scenario of a junction or roundabout. This observation led to designing an algorithm that groups vehicles into two subsets in such a way that host vehicle can act as an intermediate node between two subsets. It is noted that this condition does not necessarily mean that host vehicle acts as an articulation point between those subsets or the formation of the subsets accurately divides vehicles in front and rear of the host vehicle. Rather, the objective of forming two subsets in this way is to maximise the likelihood that vehicles from each subset unable to communicate with each other directly and the host vehicle connects them by acting as an intermediate node.

For example, the vehicle in the orange hexagonal box in figure 5.4 establishes two subsets of vehicles around it. It is noted that a similar grouping can be imagined for any vehicle in this figure. Once this group formation is established, the host vehicle that forms the groups

encodes one warning from each group together and inserts in the forwarding warning field of the packet. Let us consider two vehicles A and B; A from the blue set and B from the white set such that A and B are not within the transmission range of each other but can communicate via C, vehicle in the orange hexagonal box. When A sends a warning X to its neighbour, C receives it and when B sends a warning Y to its neighbour, C receives that too. Now, instead of sending X and Y in two transmissions, C can encode $(X \oplus Y)$ and send it in one. As A and its neighbours who are within the transmission range of C already have X, they can easily decode Y by performing the following operation and vice versa:

$$Y \leftarrow (X \oplus Y) \oplus X$$

Section 2.5 in Chapter 2 presents further insights on network coding, its operational principle and applications.

### 5.3.2 Two-hop Neighbourhood

Although finding two subsets is very critical to this data dissemination method, developing and making this method work, there are other bones of contention that need to be taken care off. Knowing the two-hop neighbourhood is one of such concerns.

NETCODE enforces each vehicle ($host$) to maintain two sets called $R$ and $N$. $R$ contains all one-hop neighbours of the $host$ and is defined as:

$$R = \{\ x \mid x \text{ is adjacent to } host\}$$

On the other hand, $N$ contains $R$ of all vehicles present in the $R$ of the $host$ (but not the $host$ itself) and is defined as:

$$N = \{R_1, R_2, R_3, ...R_n\} \text{ where } R_i = \{\ y \mid y \text{ is adjacent to } x \text{ except } host\}$$

This information is spread with the use of beacon frame in combination with packets that carry warnings. It effectively allows each vehicle to know its two-hop neighbourhood. This information is kept regularly updated by every vehicle to keep track of its neighbours and neighbours of neighbours.

### 5.3.3 Time To Live (TTL)

Network coding requires $n-1$ packet to decode a coded packet that is encoded with $n$ packets as shown in Section 2.5 in Chapter 2. Hence, it is important to know who the providers of the packets are (here *warnings*) and for how long they are going to be within communication range. A period called Time To Live (TTL) is proposed and used in this thesis that tells us about the suitability of a vehicle for coding. It is defined as:

$$TTL = \frac{r}{|v_{host} - v_x|} \tag{5.1}$$

where, $v_{host}$ and $v_x$ are the velocities in $ms^{-1}$ of the host vehicle and the vehicle's $TTL$ is calculated for respectively. *r* denotes the radius of the radio transmission coverage of the host in meter. It gives a time period in sec.

There is also a minimum threshold $TTL$ called *minimum time to live* or $TTL_{min}$. It is determined by the time period that a vehicle requires to pass $88\ meter$ distance at $70\ mph$ speed. Generally radio coverage varies depending on the data rate. As we have seen earlier, in figure 3.6, that for $24\ Mbps$ data speed, coverage radius is $40m$ whilst for $12\ Mbps$ range, it is as large as $135m$. To set a minimum threshold value of time, the average of these two coverage ($88m$) is taken and the maximum legal speed in the United Kingdom which is $70$ $mph$ ($31.2928\ ms^{-1}$) is used. It gives us:

$$TTL_{min} = \frac{r_{average}}{v_{max}} = \frac{88m}{31.29ms^{-1}} = 2.89sec \tag{5.2}$$

Equation 5.2 suggests that a vehicle having a TTL value less than $2.89sec$ has the likelihood of going out of reach before decoding an encoded warning and therefore needs to be avoided during coding process. Warnings from such vehicles should be passed on to the neighbours as singleton so that the contents can be read without having to going through the decoding process.

### 5.3.4 Encoding Algorithm

The proposed data dissemination scheme only encodes two warnings together; therefore, the degree of a coded warning can be maximum 2. The encoding algorithm of NETCODE attempts to find a pair of warnings that match with each other in such a way that they can

**Ensure:** $|Pool_{RX}| \geq 2$
1: **for all** $i$ such that $1 \leq i \leq |R|$ **do**
2: **if** $TTL_{n_i} \geq TTL_{min}$ **then**
3: $R^{active} \leftarrow R_i$
4: **end if**
5: **end for**
6:
7: **if** $n_{first} \notin R^{active}$ **then**
8: **return** $warning_{first}$
9: **else**
10: $n_{best} \leftarrow \emptyset$
11: $distance_{max} \leftarrow 0$
12: $M \leftarrow N^{R^{active}} - R_{n_{first}}$
13: **for all** $i$ such that $1 \leq i \leq |M|$ **do**
14: **if** $R_{n_{first}} \bigcap M_i = \emptyset$ **and** warning from $n_i \in Pool_{RX}$ **then**
15: $distance \leftarrow getDistance(n_{first}, n_{i^{th}})$
16: **if** $distance > distance_{max}$ **then**
17: $distance_{max} \leftarrow distance$
18: $n_{best} \leftarrow n_{i^{th}}$
19: **end if**
20: **end if**
21: **end for**
22:
23: **if** $n_{best} \neq \emptyset$ **then**
24: **return** XOR($warning_{first}$, $warning_{best}$)
25: **else**
26: **return** $warning_{first}$
27: **end if**
28: **end if**

Algorithm 1: Encoding algorithm

**Ensure:** $degree = 2$
1: $warning_{decoded} \leftarrow \emptyset$
2: **for all** warning in $Pool_{RX}$ **and** $Pool_{TX}$ **do**
3: **if** there exists a match for
at least one of the received $WarningID$s **then**
4: $warning_{decoded} \leftarrow$ XOR($warning_{encoded}$, $warning_{from\_pool}$)
5: **end if**
6: **end for**
7: **return** $warning_{decoded}$

Algorithm 2: Decoding algorithm

be decoded at the quickest possible time. On doing so, it is assumed that a pool of received warnings denoted as $Pool_{RX}$ is available that contains all received decoded warnings. This algorithm then takes the first warning from the pool and finds the best matched warning from the rest of the warnings and encodes them using exclusive-or operation. The followings explain how Algorithm 1 works in detail.

This algorithm could be executed when there are at least two warnings in the $Pool_{RX}$. $n_{first}$ and $n_{best}$ are the nodes that are going to provide with the first and the best matched warning respectively. $n_{first}$ will be straightforward to identify as it is the node that provides the first warning. However, finding the $n_{best}$ is challenging and this algorithm does that job.

At the beginning between line 1 – 5, a new set $R^{active}$ is formed from $R$ taking only those neighbours who have $TTL \geq TTL_{min}$. If $n_{first}$ does not belong to $R^{active}$ (line 7), encoding is not possible and thus the warning is returned as a singleton. However, if it exists in the active set, the initialisation process begins.

At first, $n_{best}$ is set null and $distance_{max} = 0$, $M$ is created by removing $R_{n_{first}}$ from $N^{R^{active}}$, a set containing neighbour of the members of $R^{active}$ except those whose $TTL < TTL_{min}$. In this algorithm line 13 – 21 find $n_{best}$, the best suited node for $n_{first}$. A *for loop* iterates over $M$ and $R_{n_{first}}$ to find a node whose neighbours are not neighbours of the $n_{first}$ except the host. If more than one such node is available, the furthest node gets selected. Line 23 – 28 encode two warnings together using XOR operation. If no $n_{best}$ is found, the coded warning is returned as a singleton.

### 5.3.5 Decoding Algorithm

NETCODE is designed to decode the encoded warning in the quickest possible time. The decoding algorithm performs this task if degree of a forwarding warning is 2. In addition to $Pool_{RX}$, there is another pool of warning denoted as $Pool_{TX}$ that contains all warnings that had already been sent. This pool contains warnings that have been sent in last 15 min.

This algorithm searches for a match in the $Pool_{RX}$ and $Pool_{TX}$, and decodes upon finding a suitable match. Normally a match cannot always be found. However, the way encoding algorithm pairs up two warnings together, a match can usually be found instantly.

In algorithm 2 between line 1 – 7, the decoding algorithm searches both pools for a matching warning ID. As soon as it finds one, it performs XOR operation with the found warning and decodes another warning coded inside the decoded one. If there is no match found, an empty warning is returned.

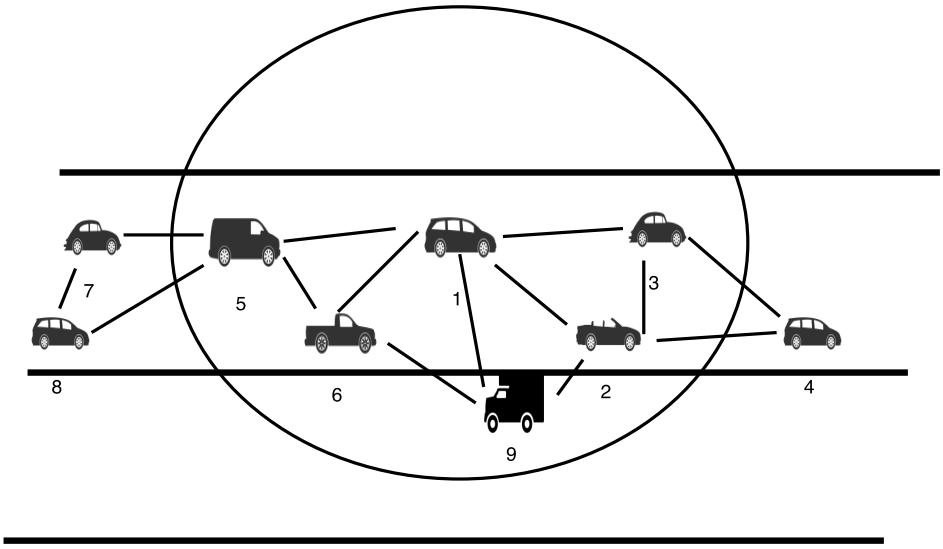



Figure 5.5: Vehicles commuting on a busy road at a speed of 70 mph.

### 5.3.6 Encoding and Decoding with a Case

This section presents a brief case with examples on how encoding and decoding works in NETCODE. Let us consider on a busy road vehicles are running at $70mph$ speed as presented in figure 5.5. The vehicle numbered $1$ (or $node_1$) is our centre of interest as it is our $host$ and shortly we see how it sends an encoded warning to its neighbours and its neighbours decode that afterwards.

We know that each of the vehicles from $node_1$ – $node_9$ presented in figure 5.5 maintains two sets called $R$ and $N$; and their values are as follow:

$$R_1 = [2, 3, 5, 6, 9],\ R_2 = [1, 3, 4, 9],\ R_3 = [1, 2, 4]$$
$$R_4 = [2, 3]\ ,\ R_5 = [1, 6, 7, 8],\ R_6 = [1, 5, 9]$$
$$R_7 = [5, 8]\ ,\ R_8 = [5, 7],\ R_9 = [1, 2, 6]$$

$$N_1 = [[3, 4, 9], [2, 4], [6, 7, 8], [5, 9], [2, 6]]$$
$$N_2 = [3, 5, 6, 9], [1, 4], [3], [1, 6]]$$
and so on.

Let us assume that in the $Pool_{RX}$ of $n_1$, the first warning is from $n_3$; therefore $n_{first} = 3$ and $R_{n_{first}} = [2, 4]$ (as defined in 5.3.2). Algorithm 1 removes $n_9$ when it creates $R^{active}$ between line 1 – 4 because $TTL_9 < TTL_{min}$ (Two vehicles moving at $70mph$ in opposite direction makes their relative velocity $140mph$ and therefore $TTL_9 = 1.40sec$). It leaves

us with $R^{active} = [2, 3, 5, 6]$. Hence, $n_{first} \in R^{active}$ and the algorithm progresses further to find $n_{best}$.

At the beginning of the next phase, the algorithm creates a set $M$ by removing $R_{n_{first}}$ from an updated $N$ of $n_1$ that only contains $R$s of all active vehicles from active vehicles (i.e. it does not count vehicles with $TTL < TTL_{min}$ inside entries of $R$s as well). Hence, we get $M = [[3, 4], [6, 7, 8], [5]]$. Finally, $R_{n_{first}} \cap M_i$ gives us $\{4\}$ for $n_2$ and $\{\emptyset\}$ for $n_5$ and $n_6$. However, because the distance between $n_1$ and $n_5$ is larger than the distance between $n_1$ and $n_6$, $n_5$ gets selected. Hence, the encoding algorithm encodes two packets from $n_3$ and $n_5$ together using an XOR operation.

It is likely that the warning goes to $n_2$, $n_3$, $n_5$, $n_6$ and possibly $n_9$. $n_2$ and $n_3$ already have the warning generated by $n_3$ and $n_5$ and $n_6$ the warning generated by $n_5$. It is therefore an easy task for the decoding algorithm to decode it using the available warning at its received pool. However, $n_9$ might not decode the warning because of the lack of the counterpart at its disposal. The *Processing Unit* of NETCODE eventually drops it after trying couple of times. This will be described in detail in the next section.

## 5.4 State Transitions in NETCODE

The individual components and coding algorithms of NETCODE have been described so far but how they work together to form an operational accident warning system has yet to be explained. This section presents a state transition diagram that tells how the warning system actually functions.

The design is based on the abstract model proposed in section 3.4, and so serves to provide a much more elaborate version of that model. Figure 5.6 shows the state transition diagram that systematically outlines the activity of NETCODE. Different states are presented in a rectangular-shaped box whilst transitions are detailed on the directional arrows. An edge without an arrow indicates the outgoing path whilst edge with pointed arrow implies where the previous state is going in. States are marked between 1 – 17 as shown on the figure but transitions are not given any numerical identifier. A blue state indicates the entering point of a warning into the NETCODE whilst a red state shows the end of the journey of a warning. There are two other states: An orange state that specifies where warnings wait for specific period and a green state that depicts the intermediate procedures. In order to keep the description simple and easy-to-understand, the rest of this section describes the operation of NETCODE based on the states.

$State - 1$: Vehicles generate warnings in two scenarios: If an incident occurs or to periodically warn neighbouring vehicles. The Warning Generator (WG) generates these warnings


Figure 5.6: State Transitions in NETCODE where blue indicates an initiating state, red indicates a terminating state, orange indicates a waiting state and green indicates an intermediate state in the diagram.

based on the circumstances. This warning is passed to the Processing Unit (PU) for further actions.

$State - 2$: In this state, the PU receives a warning. This warning may arrive from the WG or from another PU state. If the warning comes from the WG, it could be either EDM (L) or PWM (L). It will be then transitioned to an appropriate state depending on the type. However, if the warning arrives from a PU state, it must be a forwarding warning and therefore transitioned to a state that decodes warning.

$State - 3$: If the received warning in $State - 2$ is an EDM (L), this state makes it the top priority warning by setting its priority to $1$. It is then sent to a queue where all local warnings await.

$State - 4$: If the received warning in $State - 2$ is a PWM (L), this state sets priority 3. Like EDM (L), this warning is then sent to the queue where all local warning awaits.

$State - 5$: This state collects local warnings and keeps them in a priority queue. Upon receiving requests from a PU state responsible for encoding warnings, it dispatches warnings to that state.

$State - 6$: Instead of EDM (L) or PWM (L) if $State - 2$ receives a forwarding warning, it is passed to this state. In this state, the PU attempts to decode the encoded warning by checking both $Pool_{RX}$ and $Pool_{TX}$; and following the procedure described in Algorithm 2. If it is successful, then the decoded warning is sent to another state that keeps all received warning in $Pool_{RX}$. However, if the PU fails to decode it, the warning is sent to a waiting state.

$State - 7$: This is a waiting state where warnings are dispatched if the PU fails to decode. This state sets a timer for the warnings with a random non-zero value less than $500ms$ except for the case where three attempts had already been made. In that case, the warnings are sent off to a disposal state. Otherwise, when the timer expires, the warnings are sent back to $State - 6$.

$State - 8$: This is a state where the PU drops off warnings having failed to decode it successfully. The PU, however, takes three attempts before taking this decision.

$State - 9$: In $State - 6$ if the PU successfully decodes a warning, it is then forwarded here. This state puts all newly received warnings in the $Pool_{RX}$. However, if the warning is already inside the $Pool_{RX}$ or $Pool_{TX}$, PU does not take any other action unless they are 15 minute older. In this latter situation, it sends the warnings to another state that eventually drops them.

$State - 10$: In this state, the PU executes the encoding algorithm if it finds warnings waiting in the local warning priority queue. It takes the first warning from the $Pool_{RX}$ and attempts to encode it with a matching one from the rest of the warnings in the pool. Description of this

procedure is presented in Algorithm 1. At the end of the encoding process, the PU moves the warning(s) used for encoding from the $Pool_{RX}$ to the $Pool_{TX}$ and holds them for 15 min. However, if there is no warning in the received pool, the PU simply sends an empty warning to the next state or if the size of the received pool grows fast and there is lack of local warning in the queue, the PU deliberately encodes warning and sends that to the next state.

$State - 11$: In this state, the PU creates the actual packets that NETCODE transmits. Upon the arrival of the forwarding warning from the $State-10$, the PU takes the first local warning from the priority queue and constructs the packet. However, if the forwarding warning is empty, the PU leaves that part of the packet empty. There could have been another situation when there is no local warning but $State-10$ still sends a forwarding warning to be included in the packet. The PU handles it by leaving local warning part of the packet empty. This packet is then further held in a priority queue using the priority in Table 5.2. The priority of the packet is determined based on the highest priority warning available inside the packet. For example, if the packet contains an EDM (L), it receives priority $1$ but if there is no local message and encoded message includes two PWM (F)s, it receives priority $4$ and so on. The DU subsequently receives packets from this queue.

$State - 12$: This state represents the DU that receives packet from the PU. It then prepares the packet for the underlying IEEE 802.11p MAC protocol and passes it to another state that is responsible for broadcasting packets to the neighbours.

$State - 13$: In this state, nodes send data to their neighbours. The IEEE 802.11p entity broadcasts the packet received from the $State - 12$ wirelessly.

$State - 14$: In this state, the PU receives a packet from the DU. It inspects if there is any local or forwarding warning available in the packet. Local warnings are sent to the $State-2$ whilst forwarding warnings go to the $State - 9$.

$State-15$: In this state, the DU receives a packet from the underlying MAC layer and passes it to the $State - 14$ described above.

$State-16$: This state represents the receiver counterpart of the MAC layer where it receives data from the neighbour. If the data contains a packet, it sends it (packet) to the $State - 15$.

$State-17$: This state represents WR that receives warning from either $State-2$ or $State-9$ when the warning is meant for the $host$ node. The WR processes the received warning and passes it on to the On-board Unit (OBU).

## 5.5 Summary

Having identified the shortcomings of broadcast based data dissemination schemes in AWSs in Chapter 4, this chapter in course of accomplishing the third research objective of the thsis comes up with a proposal that seeks to improve performance in VANET-based warning systems. It provides a description of the system followed by a commentary on addressing, message types and packet format. Nevertheless, Section 5.3 presents the main contribution of this thesis – a pair of encoding and decoding algorithms that makes the use of XOR-based coding technique to reduce number of transmissions and subsequently creates space for more warnings to get delivered. A state-transition diagram is presented later showing how the system operates. This chapter, however, does not provide performance evaluations rather those are presented in next three chapters.

# Chapter 6

# Performance Analysis of Warning Transmissions

The preceding chapters presented a comprehensive requirement survey and evaluated the performance of a number of previously proposed warning systems for VANETs. Chapter 3 identified that broadcast is one of the most popular data dissemination schemes amongst the researchers who build warning systems and Chapter 4 unveiled how this scheme deteriorates from its acceptable behaviour in extreme situations particularly when the number of transmissions is large. It is, however, difficult to maintain fewer transmissions in high network density unless a solution is found that reduces the number of transmissions without having to limit the number of warning messages vehicles distribute.

In order to address this problem in Chapter 5, a new warning system called NETCODE was proposed. This new warning system uses an XOR-based network coding technique to reduce the number of transmissions by encoding two warnings together. This chapter aims to accomplish the forth research objective mentioned in Section 1.2 by evaluating the performance of this new warning system with regard to transmissions and attempts to validate the claim in the thesis statement that network coding can improve performance of data dissemination. This chapter, however, does not investigate performances in relation to preventing accidents and reaching vehicles who are in potential danger. These attributes will be evaluated later in Chapter 7 and 8 instead.

The rest of the chapter is organised as follows: Section 6.1 provides the description of the simulation environment, Section 6.2 discusses the performance metrics, Section 6.3 outlines the method of study, Section 6.4 and 6.5 present the analysis with moderate and heavy data traffic load respectively and Section 6.6 summarises the outcomes before this chapter concludes with a summary in Section 6.7.

## 6.1 Simulation Environment

This section provides detailed description on the simulation environment and the mobility of the vehicles. It was mentioned earlier in Section 4.4 on page 49 that a custom-built simulator is used throughout this thesis. This chapter uses that simulator but introduces some changes in the simulation environment. The rest of the section briefly mentions those changes.

### 6.1.1 Simulator and Warning Systems

The previously used open source simulator *Pamvotis* is chosen again as the network simulator in the studies presented in this chapter. It provides the support of the MAC layer by enabling IEEE 802.11p protocol in the vehicles. The application layer protocol used earlier is also used in these studies. This application generates periodic warnings at a defined rate for a specific period of time.

At network layer, two warning systems, RBSM and VSPCA, discussed in Chapter 4 will be reused. In these studies, there is a new addition at the network layer. The proposed warning system i.e. NETCODE is used at the network layer to compare the performance with RBSM and VSPCA. This warning system is developed as described in Chapter 5.

### 6.1.2 Mobility

The major change introduced in this chapter is the mobility model. The mobility model of Chapter 4 is not needed because the evaluation of transmissions conducted here does not require a large area such as the city centre. Instead, a single carriageway can provide the basis of this analysis. This simplified but enclosed environment in turn gives the opportunity to conduct some studies that are difficult to perform in a large and open space. For example, observing vehicles generating warnings for a specific time and letting them propagate until the last warning reaches its last destination was complex in the previous setup. However, by changing the mobility pattern and reducing the size of the simulation area, it is made possible to conduct the intended experiments and collect necessary data as outlined in this chapter.

This chapter uses a one-way[1] single carriageway where vehicles commute only in one direction. The simulation area is 15 miles in length and the network densities are varied as 5, 10, 20, 25, 30, 35, 40, 45 and 50 vehicles. It is noted that in earlier evaluations in Chapter 4 network density is measured using the unit “vehicle/min” but in this chapter the unit is just “vehicle”. This is because in Chapter 4, the simulator constantly injected vehicles into the

[1] A one-way street is a road where vehicles commute in a single direction. It could be a single carriageway but there will be no vehicles coming from the opposite direction.

simulation area but in this chapter vehicles are placed on the simulation area only once and allowed to commute according to the mobility rule.

In these studies, vehicles will be assigned velocities between $20mph$ and $30mph$ and placed on the road in such a way that they always form a connected graph but the structure keeps changing due to the variable velocities.

## 6.2 Performance Metrics

This chapter uses performance metrics that are associated with only the network layer. In total, eight metrics are used from three categories. Not all of them are directly related to transmission but they collectively aim to explore transmission-related improvement in data dissemination. The followings are the detailed description of these metrics.

***Transmission:*** There are two performance metrics that measure efficiency of transmission in NETCODE. These are *Total Transmissions* and *Transmissions/Warning*. The former gives the measurement of the number of transmissions during the whole of the simulation by a node on an average whilst the latter gives the number of transmissions required to distribute a warning on an average. It is noted that the latter metric does not only count transmissions required to distribute a warning from the host to its neighbour rather also include the transmissions required to transmit the warning to other nodes over multi-hop network.

***Collision:*** It has been previously observed in Chapter 4 that transmission has relation with collision. It will be tested again in this study. Three metrics are used to evaluate performance related to collision. These are *Total Collisions*, *Collisions/Warning* and *Collisions/Transmission*. The first metric gives the total number of collisions network encounters until the last warning is delivered to its last destination. The second metric gives the number of collisions a warning encounters during its lifetime whilst the last metric gives the number of collisions warning systems encounter for each successful transmission.

***Time:*** Although above metrics could give an understanding over the efficiency of the transmissions but they do not necessarily confirm the potential improvement in warning delivery time. Therefore, three metrics are recorded in the simulation that aim to explore efficiency of delivery time. These are *Total Time*, *Time/Transmission* and *Time/Warning*. The first metric records the time required to disseminate all warnings in the network until the last warning is delivered to its last destination. The second metric finds the average time for an individual transmission whilst the last metric gives the average time required for each warning to be disseminated in the network.

## 6.3 Method of Study

This chapter aims to analyse the performance of transmissions in presence of coding. The nature of the studies presented here is significantly different than what has been presented earlier. These studies do not evaluate potential accidents or the effect of data traffic load but rather only focus on data transmission-related parameters. To achieve this goal, the custom-built simulator described and used in Chapter 4 will be used again along with the changes described in section 6.1 of this chapter.

Two warning systems, RBSM and VSPCA, will be representative of data dissemination without the use of coding whilst NETCODE represents coding based dissemination. Amongst the systems, VSPCA operates based on flooding and RBSM is designed using limited-scoped broadcast. NETCODE uses a limited-scoped broadcast scheme but modified by the network coding technique.

The thesis statement in Section 1.1 argues that the use of network coding can reduce the number of transmissions and improve warning delivery time in AWSs. Performance of the three warning systems mentioned above will be compared with each other to observe how network coding reduces transmissions and eventually improves warning delivery time.

Two studies will be conducted by varying the density of the network with two fixed data traffic generation rate. Each study will have three categories of evaluation – *Transmission*, *Collision* and *Time*. At first, both studies examine how NETCODE performs against VSPCA and RBSM in terms of transmission. If it confirms that NETCODE does reduce the number of transmissions, still that would not necessarily confirm that it reduces number of collisions in the network to avoid creating contentions. Therefore, collision is also observed and compared between NETCODE and other two warning systems. Finally, the studies sum up the results by comparing the delivery time between coded and non-coded schemes.

## 6.4 Performance Analysis with Moderate Data Traffic

This performance analysis with moderate data traffic load is conducted by varying the number of vehicles in the network while keeping other parameters unchanged. NETCODE, RBSM and VSPCA are the warning systems used in this study.

The simulation scenarios consist of number of vehicles that varies from 5 to 50 as mentioned earlier. The data traffic load is created by generating 5 warning/sec. This rate was found and used as the moderate data traffic load in Chapter 4 and is used again in this study. During the simulation, vehicles are allowed to generate PWMs for the first five seconds only. They, however, keep forwarding the messages until all warnings are disseminated. A total of 20

| *Density* | *RBSM* | *VSPCA* |
|---|---|---|
| *(vehicle)* | *(%)* | *(%)* |
| 5 | 15.96 | 15.96 |
| 10 | 20.63 | 22.19 |
| 15 | 35.48 | 39.66 |
| 20 | 35.13 | 40.13 |
| 25 | 36.99 | 43.38 |
| 30 | 37.31 | 44.15 |
| 35 | 37.24 | 43.88 |
| 40 | 37.34 | 42.76 |
| 45 | 37.49 | 42.86 |
| 50 | 37.42 | 44.08 |

Table 6.1: The performance improvement of transmissions by NETCODE over RBSM and VSPCA while operating with the moderate data traffic load.

trials are run and later an average is taken for all metrics. It is noted that the same settings are used including identical mobility for each warning system observed in this study.

### 6.4.1 Transmission

Figure 6.1 and 6.2 demonstrate how the warning systems perform in relation to transmission. The thesis statement in Chapter 1 claims that network coding technique can be useful for reducing number of transmissions in the network. These two graphs confirm this claim under the scope of this chapter that NETCODE uses less transmission for delivering the same number of warnings in the network compare to RBSM and VSPCA.

Figure 6.1 shows that as network density increases, the number of transmissions also increases. It is obviously because with a fixed data traffic load more warnings enter into the network as number of node increases. However, the results demonstrate that NETCODE significantly reduces the number of transmissions generated compared to other two warning systems that do not use coding. For example, when 50 vehicles commute in the network, a total of 1250 warnings are generated after the first five seconds of the simulation. The rest of the time these vehicles only forward each other's warnings. It is notable from the figure that NETCODE uses below 800 transmissions for each node to disseminate the warnings whilst RBSM and VSPCA use more than 1200 transmissions. It is also notable from this figure that VSPCA tend to use more transmissions than RBSM in network density 20 or more. This behaviour can be explained by realising their broadcasting mechanism. As RBSM only forwards data up to 5 hops, warnings are disseminated within a limited number of nodes. However, VSPCA floods the network until all nodes receive a particular warning. This behaviour makes this warning system to transmit more in high network density.

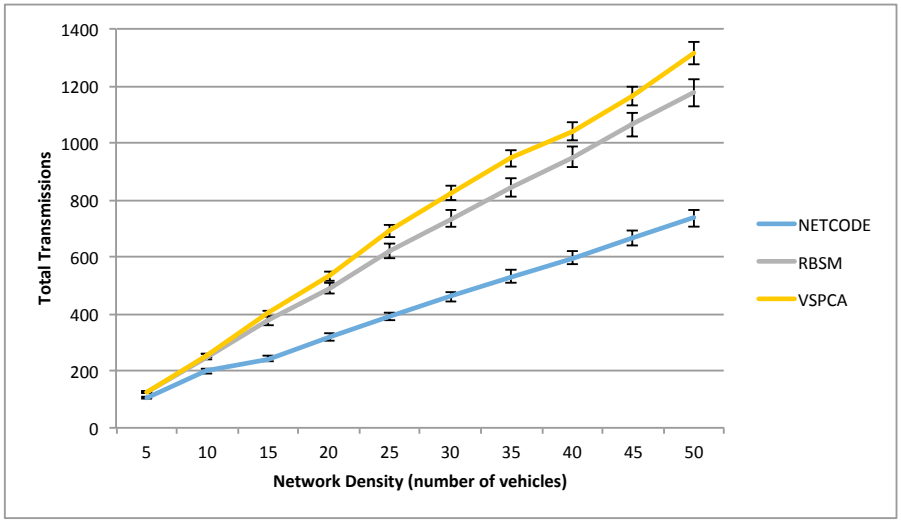



Figure 6.1: The number of total transmissions made by the warning systems in the network at various network density levels with the moderate data traffic load.

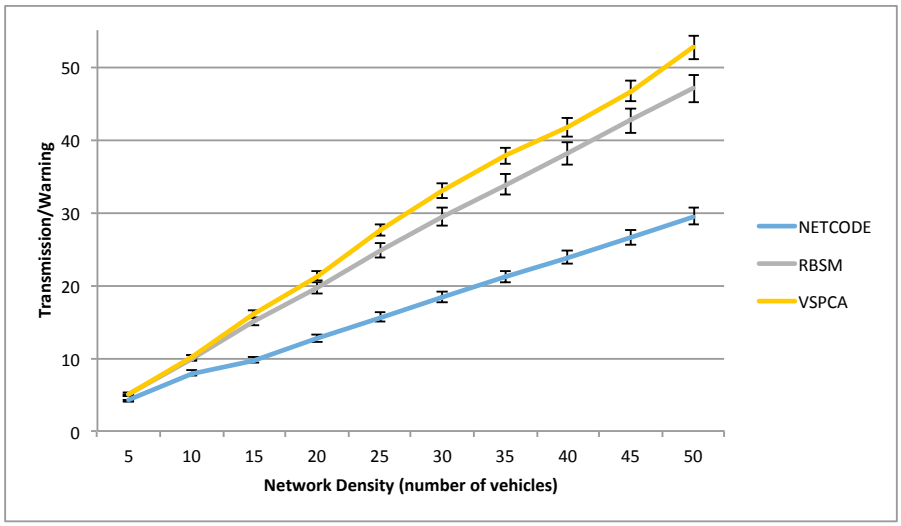



Figure 6.2: The number of transmissions required by the warning systems to disseminate a warning in the network at various network density levels with the moderate data traffic load.

| *Density* | *RBSM* | *VSPCA* |
|---|---|---|
| *(vehicle)* | *(%)* | *(%)* |
| 5 | 6.15 | 6.15 |
| 10 | 40.53 | 41.73 |
| 15 | 52.60 | 56.50 |
| 20 | 58.47 | 58.51 |
| 25 | 58.19 | 59.72 |
| 30 | 58.41 | 60.62 |
| 35 | 58.45 | 61.07 |
| 40 | 58.22 | 60.48 |
| 45 | 58.26 | 60.20 |
| 50 | 58.20 | 60.85 |

Table 6.2: The performance improvement of collisions by NETCODE over RBSM and VSPCA while operating with the moderate data traffic load.

In this study, an improvement of up to 35% in total transmissions is observed against RBSM and 44% against VSPCA by the NETCODE. Table 6.1 summarises the improvement at different network density levels. From this table, it is also noteworthy that when network density is below 15 nodes, improvement is not significant. But as network density increases NETCODE outperforms RBSM and VSPCA by a significant margin.

Because of the fact that the network is enclosed and all vehicles remained connected during the simulation, Figure 6.2 gives the number of transmissions required for each warning to be disseminated in the network. Although previous figures show total transmissions, they do not clarify how the warning systems are performing on a per-warning basis. For example, this figure shows that for each warning at 50 node network density, NETCODE uses less than 30 transmissions but RBSM and VSPCA use nearly 50 transmissions.

### 6.4.2 Collision

Figure 6.3 and 6.4 demonstrate how the warning systems perform in relation to collisions. It is previously observed that collisions are a key factor in introducing broadcast storms into the network and a reduction in collision frequency potentially improves warning delivery times. Earlier in this chapter it was argued that if we reduce the number of transmissions, that in turn helps reduce contention and collisions in the network. Section 6.4.1 confirms that NETCODE successfully reduces the number of transmissions compared to the other two systems. This should result in a reduction in collisions and following confirms that expectation.

Figure 6.3 demonstrates the performance of RBSM, VSPCA and NETCODE as to how these systems respond to network density in relation to total collisions when all other parameters

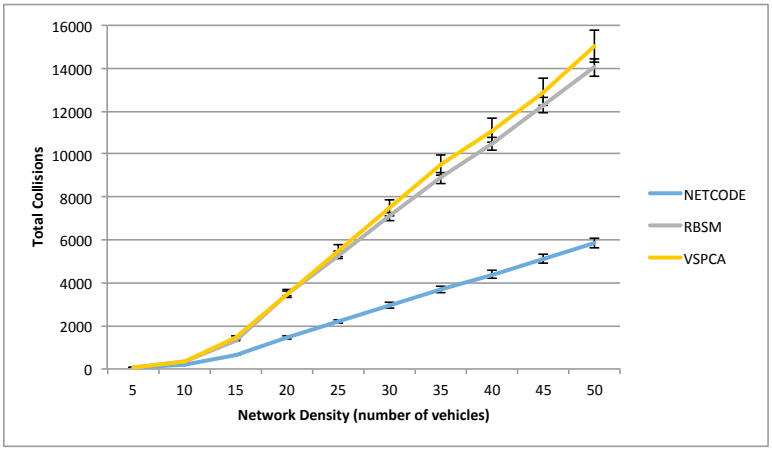



Figure 6.3: The number of total collisions encounterd by the warning systems in the network at various network density levels with the moderate data traffic load.

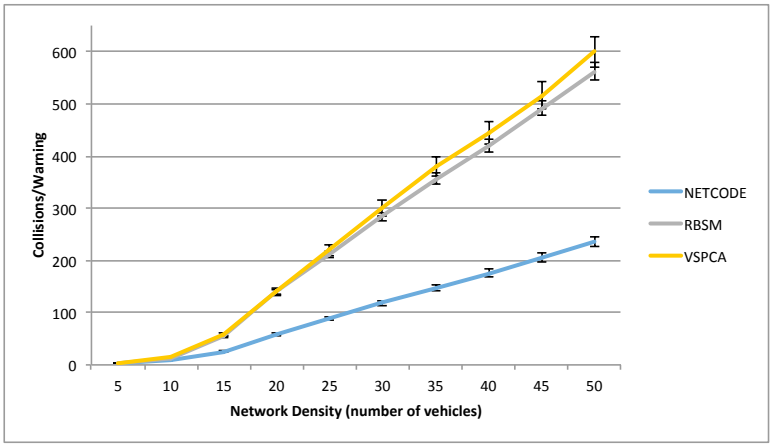



Figure 6.4: The number of collisions encounterd by the warning systems to disseminate a warning in the network at various network density levels with the moderate data traffic load.

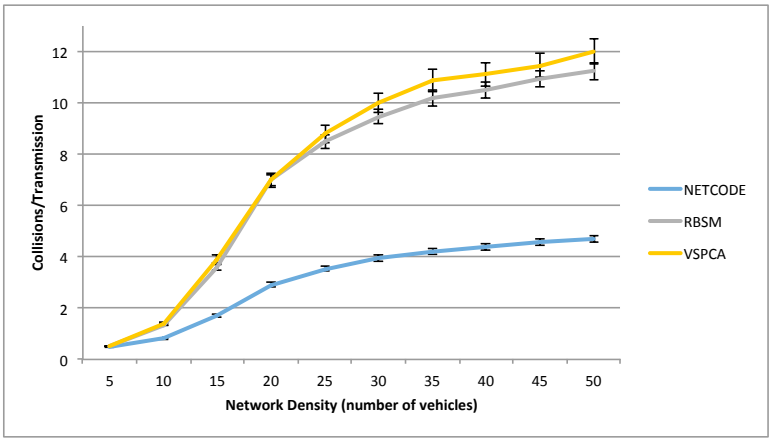



Figure 6.5: The number of collisions encountered by the warning systems to make a successful transmission in the network at various network density levels with the moderate data traffic load.

are fixed. It is evident that NETCODE successfully reduces the number of collisions in the network. Chapter 4 previously stated that broadcast storm occurs when vehicles operate in a high density network. This figure confirms that assertion by showing a large number of collisions being experienced by the vehicles when network density is more than 20 vehicles. Results show that RBSM and VSPCA encounter between 4000 and 14000 collisions in that density. NETCODE, however, take that number down to between 1000 and 6000 collisions. It is no surprise that at high network density NETCODE encounters less than half of the collisions other two warning systems do. If we compare these results with those obtained in Section 6.4.1, it becomes obvious that as the number of transmissions gets reduced, the number of collisions decreases.

Table 6.2 shows the improvement by NETCODE at different network density levels. With network density more than 15, the improvement is significant. However, when network density is very small such as 5 node, all warning systems perform nearly identically.

Although the previous figure gives the total number of collisions but figure 6.4 and 6.5 add more context into it. The former of these two figures shows the number of collisions warning systems encounter during the dissemination process of each warning. For example, at a network density of 50 vehicles, a warning encounters nearly 600 collisions when distributed by VSPCA and RBSM. However, at the same network density level, NETCODE encounters just over 200 collisions. With network density 20 or more, NETCODE encounters only half of the collisions than that of VSPCA and RBSM. The later figure shows the number of collisions these systems encounter against each successful transmission. It reveals that NETCODE encounters just over 4 collisions against a successful transmission whereas RBSM and VSPCA encounter nearly 12 collisions. These results are evident that the proposed scheme significantly reduces the competition in the network that in return should put huge impact on the improvement of the warning delivery time.

### 6.4.3 Time

Previously in this chapter the performances were evaluated based on the number of transmissions and collisions. In spite of the fact that there is significant improvement in both metrics, the ultimate goal of NETCODE is to reduce warning delivery time and this remains to be confirmed. This section looks into three other metrics related to delivery time and compares the results amongst NETCODE, VSPCA and RBSM.

Figure 6.6, 6.7 and 6.8 jointly present the improvement achieved by NETCODE over the other two warning systems. It is evident from the figures that the proposed warning system not only reduces the number of transmissions and collisions, it also improves warning delivery time. Figure 6.6 shows the total time required to deliver all the warnings to their

| *Density* | *RBSM* | *VSPCA* |
|---|---|---|
| *(vehicle)* | *(%)* | *(%)* |
| 5 | 0 | 0 |
| 10 | 28.81 | 30 |
| 15 | 45.77 | 50.38 |
| 20 | 45.65 | 52.71 |
| 25 | 46.37 | 52.62 |
| 30 | 46.13 | 52.73 |
| 35 | 46.77 | 52.74 |
| 40 | 46.27 | 52.63 |
| 45 | 46.20 | 52.88 |
| 50 | 46.56 | 52.71 |

Table 6.3: The performance improvement of time by NETCODE over RBSM and VSPCA while operating with the moderate data traffic load.

destination during the simulation. At high network density, RBSM and VSPCA require almost 400 sec but NETCODE improves that performance by requiring only half of the time to deliver the same number of warnings. Table 6.3, summarises the improvement at different density levels.

The results presented in figure 6.7 show the average time required for a transmission. It is evident from the figure that NETCODE maintains a transmission time below 150 ms throughout the study. In contrast, RBSM and VSPCA require time between 250 to 300 ms. Figure Figure 6.8 further confirms the performance by showing the average time required for a warning to be disseminated throughout the network. It is apparent from the results that where NETCODE requires just below 8 sec, RBSM and VSPCA require nearly 16 sec for delivering each warning in the same network.

With these observations, it is now evident that the reduction in the number of transmissions helps reducing competitions in the network by minimising the number of collisions. This less competitive environment in return allows vehicles to quickly deliver warning messages to their neighbours.

## 6.5 Performance Analysis with Heavy Data Traffic

This performance analysis with heavy data traffic load is conducted by varying the number of vehicles in the network while keeping other parameters unchanged. NETCODE, RBSM and VSPCA are the warning systems used in this study. The simulation scenarios will be identical of what was described in section 6.4 except the data traffic load which is 15 warning/sec in this study to represent the heavy load.

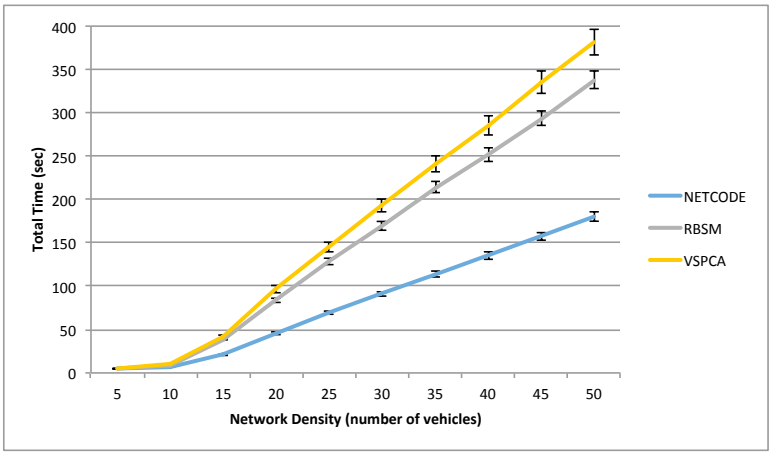



Figure 6.6: The required time to disseminate all warnings in the network at various network density levels the with moderate data traffic load.

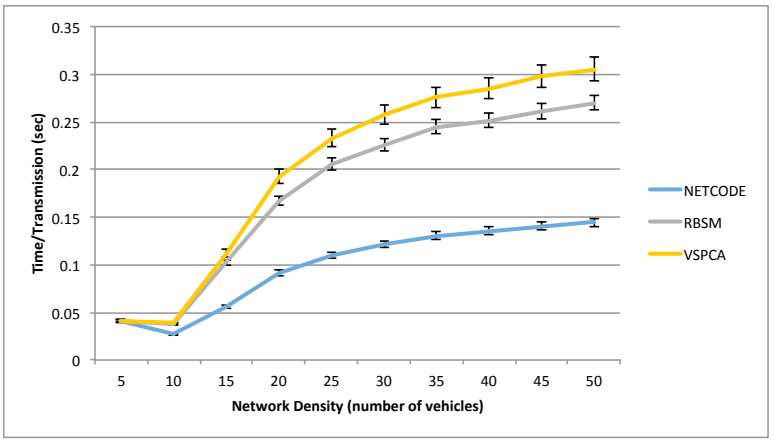



Figure 6.7: The required time to make a successful transmission the network at various network density levels with the moderate data traffic load.

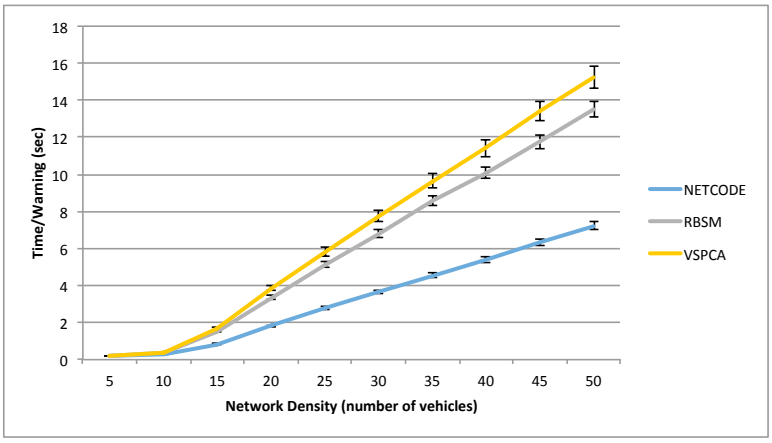



Figure 6.8: The required time to disseminate each warning in the network at various network density levels with the moderate data traffic load.

| *Density* | *RBSM* | *VSPCA* |
|---|---|---|
| *(vehicle)* | *(%)* | *(%)* |
| 5 | 16.04 | 16.04 |
| 10 | 21.46 | 21.46 |
| 15 | 35.46 | 35.80 |
| 20 | 35.81 | 40.25 |
| 25 | 36.04 | 42.29 |
| 30 | 36.87 | 43.29 |
| 35 | 37.61 | 43.10 |
| 40 | 37.83 | 44.25 |
| 45 | 38.02 | 44.30 |
| 50 | 38.91 | 44.87 |

Table 6.4: The performance improvement of transmissions by NETCODE over RBSM and VSPCA while operating with the heavy data traffic load.

### 6.5.1 Transmission

Figure 6.9 and 6.10 demonstrate how the warning systems perform in terms of transmission with heavy data traffic load. While conducting experiments with moderate data traffic load, previous section reiterated the claim of the thesis statement in Chapter 1 that network coding technique can be useful in reducing the number of transmissions in the network. These two graphs further reconfirm this claim with heavy data traffic. It is clearly evident that NETCODE uses significantly fewer transmission to deliver the same number of warnings in the network compare to RBSM and VSPCA from table 6.4.

Figure Figure 6.9 again shows that NETCODE significantly reduces the number of transmissions compare to other two warning systems that do not use coding. For example, in 50 network density, vehicles generate a total of 3750 warnings after the first five seconds of the simulation. Like the previous study, the rest of the period these vehicles only forward each other's warnings. It is noteworthy that NETCODE uses just over 2000 transmissions to disseminate these warnings in the networks whilst RBSM and VSPCA requires over 3500 and 4000 transmissions respectively. This trend can also be observed for network densities below 50 vehicles as well.

In this study, an improvement of 35% to 45% in total transmissions is achieved by NETCODE when network density remains between 15 and 50 vehicles. Table 6.4 shows a comprehensive picture of the improvement at different network density levels where NETCODE outperforms other two systems by a significant margin. It is notable from this comparison that although the improvement tends to grow up to 40% against RBSM, it nearly reaches up to 45% against VSPCA at the same network density levels. This behaviour is characterised by the fact that despite having the density same, VSPCA forwards warnings to a wider audience compare to RBSM; thus uses more transmissions.

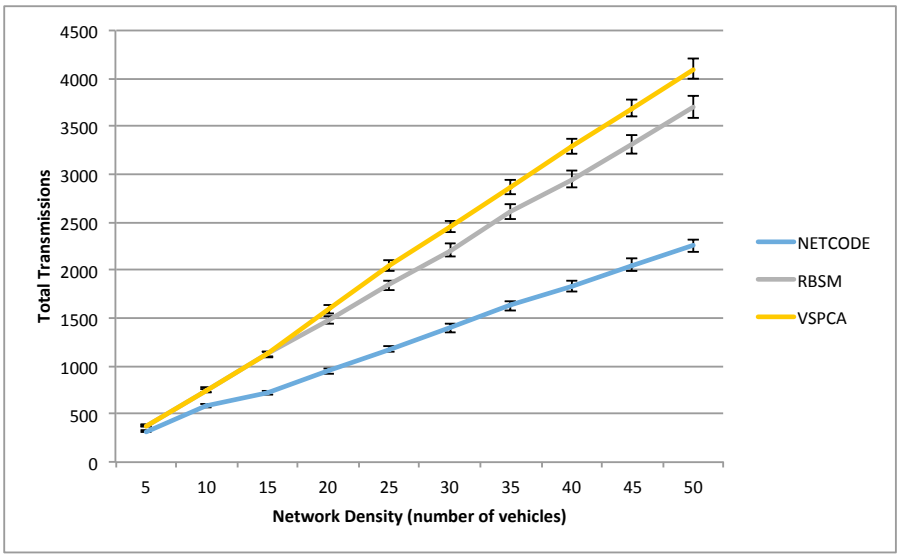



Figure 6.9: The number of total transmissions made by the warning systems in the network at various network density levels with the heavy data traffic load.

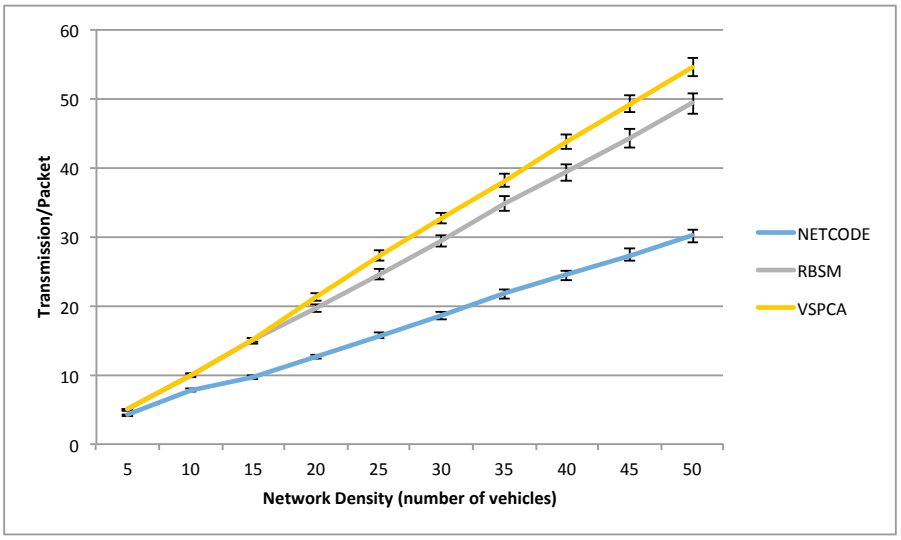



Figure 6.10: The number of transmissions required by the warning systems to disseminate a warning in the network at various network density levels with the heavy data traffic load.

| *Density* | *RBSM* | *VSPCA* |
|---|---|---|
| *(vehicle)* | *(%)* | *(%)* |
| 5 | 0.99 | 0.99 |
| 10 | 44.51 | 46.80 |
| 15 | 53.97 | 55.11 |
| 20 | 58.38 | 61.49 |
| 25 | 59.13 | 63.69 |
| 30 | 59.11 | 63.25 |
| 35 | 59.98 | 64.73 |
| 40 | 59.90 | 64.83 |
| 45 | 59.96 | 64.19 |
| 50 | 59.07 | 64.67 |

Table 6.5: The performance improvement of collisions by NETCODE over RBSM and VSPCA while operating with the heavy data traffic load.

As mentioned earlier, the network is an enclosed one and all vehicles remain connected during the simulation. Figure Figure 6.10 gives the number of transmissions required for each warning to be disseminated in the network and shows how the systems are performing on a per warning basis. For example, it demonstrates that for each warning at 50 node network density, NETCODE uses around 30 transmissions whilst VSPCA and RBSM use more than 50.

### 6.5.2 Collision

Figure 6.11 demonstrates the performance of the warning systems as to how they respond to the heavy data traffic load in terms of collisions. It has been observed in Chapter 4 that collisions are a key factor in broadcast storm generation and in 6.4.2 that a reduction in collision rates improves warning delivery time. This section further investigates this with a heavier data traffic load. Section 6.5.1 has already confirmed that NETCODE successfully reduces the number of transmissions compared to the other two systems while operating with a heavier data traffic load and the results presented in this graph supports that findings by confirming a similarly significant reduction in the number of collisions.

Chapter 4 previously stated that broadcast storm occurs when vehicles operate in a high density network. This figure reconfirms that, for example, by showing a large number of collisions encountered by RBSM and VSPCA when network density is between 15 and 50 vehicles. However, NETCODE reduces the number of collisions significantly for the same network densities. This performance is characterised by the fact that if the number of transmissions gets reduced, the number of collisions gets decreased too. Table 6.5 shows the improvement by NETCODE at different network density levels.

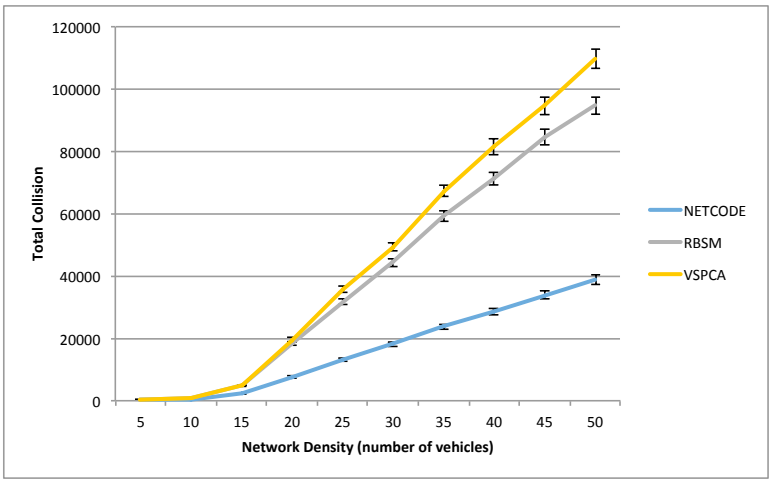



Figure 6.11: The number of total collisions encountered by the warning systems in the network at various network density levels with the heavy data traffic load.

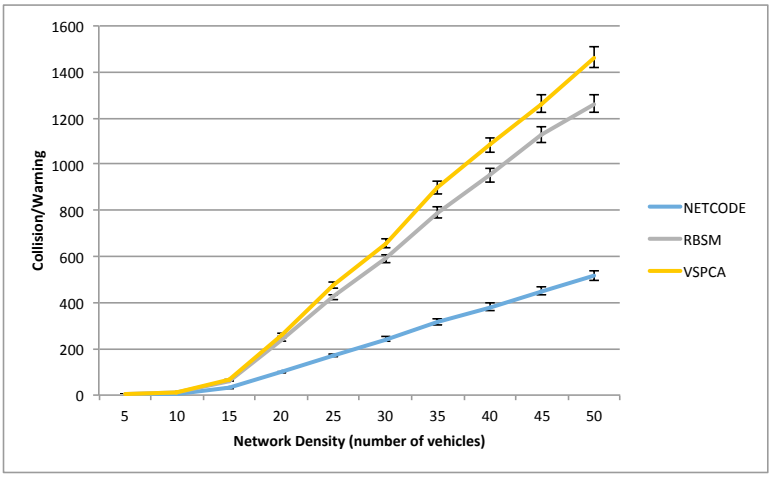



Figure 6.12: The number of collisions encountered by the warning systems to disseminate a warning in the network at various network density levels with the heavy data traffic load.

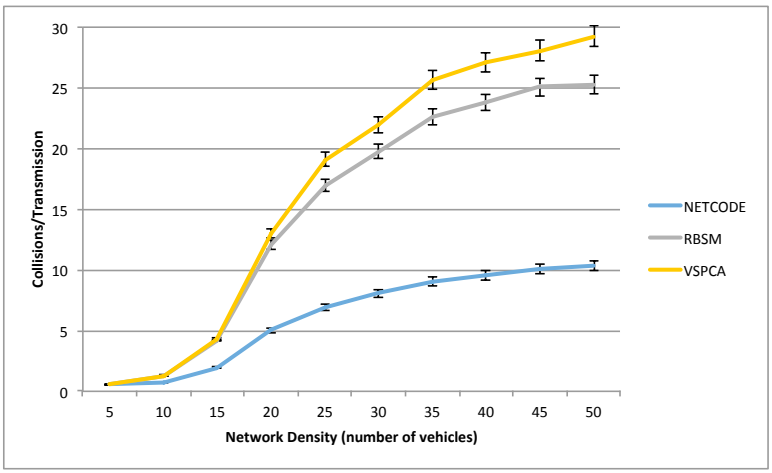



Figure 6.13: The number of collisions encountered by the warning systems to make a successful transmission in the network at various network density levels with the heavy data traffic load.

| *Density* | *RBSM* | *VSPCA* |
|---|---|---|
| *(vehicle)* | *(%)* | *(%)* |
| 5 | 0 | 0 |
| 10 | 28.81 | 30.27 |
| 15 | 45.77 | 50.38 |
| 20 | 45.65 | 52.71 |
| 25 | 46.37 | 52.62 |
| 30 | 46.13 | 52.73 |
| 35 | 46.77 | 52.74 |
| 40 | 46.27 | 52.63 |
| 45 | 46.20 | 52.88 |
| 50 | 46.56 | 52.71 |

Table 6.6: The performance improvement of time by NETCODE over RBSM and VSPCA while operating with the heavy data traffic load.

Figures 6.12 and 6.13 add more context in this discussion as they demonstrate the number of collisions against each warning delivery and successful transmission. The former shows that RBSM and VSPCA encounter more than 1200 collisions in the highest network density while delivery a warning. This is twice the number these two system encounter in moderate counterpart of this study. On the other hand, NETCODE also encounters nearly 500 collisions for the same network density. This number is also as large as almost twice than what has been observed in moderate study, but it still shows significant reductions compare to the other two systems. The latter figure shows that NETCODE, to make a successful transmission, encounters just over 10 collisions at the highest network density, more than twice of what it encounters in moderate study whilst RBSM and VSPCA encounter 25 to 30 collisions for each successful transmission. This makes NETCODE encountering less than half of the collisions than VSPCA and RBSM encounter for each successful transmission.

### 6.5.3 Time

Previously in 6.5.1 and 6.5.2 the performance analysis of transmission with heavy data traffic load is evaluated based on the number of transmissions and collisions respectively. In spite of the fact that both metrics demonstrated significant improvement, the key goal of reducing warning delivery time has not been observed yet. This section looks into three other metrics related to delivery time and compares the results with NETCODE, VSPCA and RBSM.

Figures 6.14, 6.15 and 6.16 jointly present the improvement achieved by NETCODE over other two warning systems while operating with a heavier data traffic load. As with the more moderate traffic load, it is evident from the results that the proposed warning system not only reduces the number of transmissions and collisions, it also improves warning delivery time. Figure 6.14 particularly shows improvement of the total delivery time. At high network

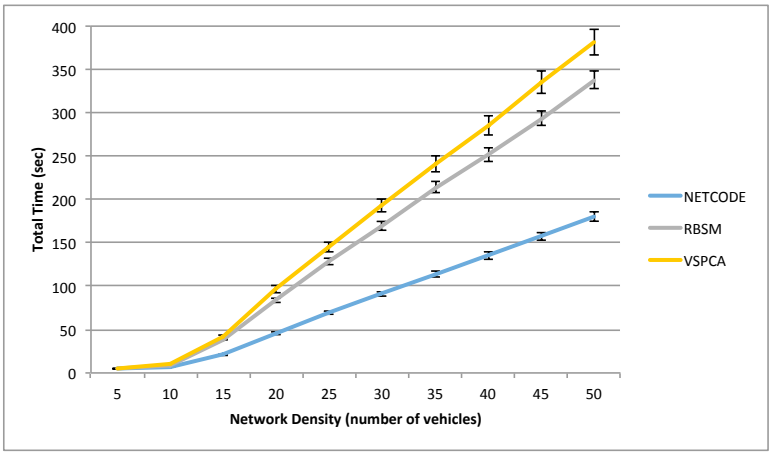



Figure 6.14: The required time to disseminate all warnings in the network at various network density levels with the heavy data traffic load.

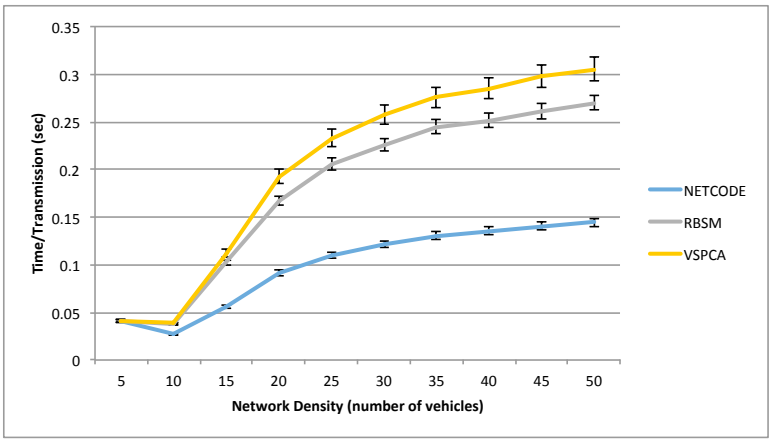



Figure 6.15: The required time to make a successful transmission in the network at various network density levels with heavy data traffic load.

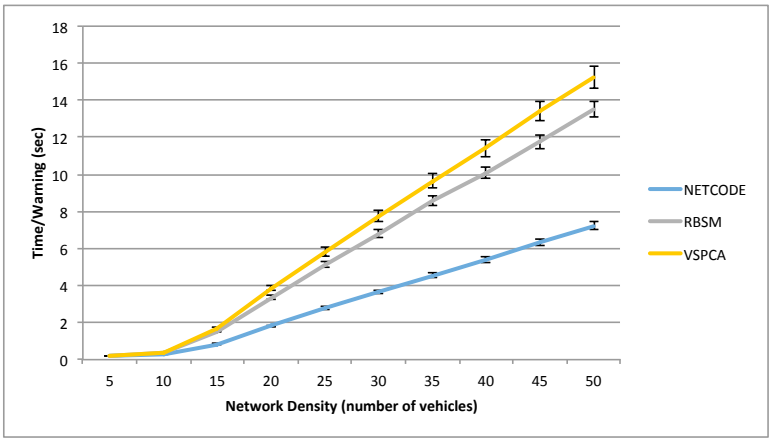



Figure 6.16: The required time to disseminate each warning in the network at various network density levels with heavy data traffic load.

densities of NETCODE improves the performance by 45% to 50% compare to the other two systems. Table 6.6 summarises this improvement at different density levels.

The results presented in figure figure 6.15 shows the time required for making a successful transmission. It is evident from the graph that NETCODE takes half of the time that the other two systems require to make a transmission. This indicates that the proposed system will be able to deliver warning messages significantly faster than the previous schemes. Figure 6.16 further confirms the performance by showing the time required for a warning to be disseminated throughout the network. The significant improvement by NETCODE is clear from the graph, for example, NETCODE requires just over 2 sec at the highest network density whilst RBSM and VSPCA take nearly 3.5 sec for disseminating a warning in the same network.

## 6.6 Summary of the Studies

The studies presented in this chapter combindly fulfil the forth research objective of the thesis by showing that NETCODE significantly reduces the number of transmissions compared to other two warning systems. It is significant from these results that XOR-based data dissemination can be effective because these transmission related improvements directly impact on the performance metrics of collision as studies revealed that the number of collisions in the network decreases significantly when NETCODE operates. In spite of such success, however, this was not confirmed yet that the new scheme is actually capable of improving warning delivery time. Later performance evaluation involving various time related metrics confirm that the new scheme successfully reduces warning delivery time as much as 45% over limited-scoped broadcast and 50% over flooding in high network densities.

In these studies, all evaluated systems are also tested against a heavy data traffic load with a view to observing their ability to perform in stressed environment. When other two warning systems compared in this chapter demonstrate poor performance, NETCODE still maintains a fair display.

It is noteworthy that having this objective fulfilled, this is not proven that NETCODE is capable of making timely delivery of warning message to detect potential accidents. This is, of course, a promising sign that this new scheme significantly performs better than the other systems compared here, but this will only be established that it is able to prevent accidents if this scheme is tested to detect potential accidents.

## 6.7 Summary

A new warning system called NETCODE was proposed in Chapter 5 with a view to reduce the number of transmissions by encoding two warnings together. This chapter accomplished the forth research objective and partially validated the claim mentioned in the thesis statement that network coding can improve performance of data transmissions by evaluating transmission related metrics of the new scheme. The core contribution of this chapter is two studies presented in section 6.4 and 6.5. These studies show that the reduction in the number of transmissions helps reducing competitions in the network by minimising the number of collisions. This less competitive environment in return allows vehicles to quickly deliver warning messages to their neighbours. It is, however, not confirmed yet that this quickly delivery is fast enough to prevent accidents. Chapter 7 and 8 of this thesis looks into this and attempt to validate the thesis statement completely.

# Chapter 7

# Analysis of Periodic Warning Message Dissemination

The evaluations presented in Chapter 4 encompass the performance of broadcast-based data dissemination schemes and give insight into the effectiveness of sending warnings in a contentious environment. Having carefully reviewed these schemes and identified their pitfalls, a new accident warning system is proposed in Chapter 5. This chapter, in course of accomplishing the fifth research objective set in this thesis, evaluates the performance of the newly proposed warning system against two previously discussed systems – RBSM and VSPCA with regard to disseminating Periodic Warning Message (PWM). It investigates how effectively these systems disseminate PWMs in response to the change of network density and data traffic load in the network and ultimately how efficacious they are in detecting potential accidents. The studies also scrutinise the ability of the warning systems in keeping transmission queuing delay below the *Maximum Tolerable Queuing Delay (MTQD)*. This is particularly important because in Chapter 4, it has been observed that failing to comply with this stipulation makes warning systems vulnerable.

The evaluation takes place at both network and application layer. Network layer performances are evaluated based on transmission collision and queuing delay whilst application layer performances are tested using metrics such as accident-at-junction, potential accident undetected, potential accident detected etc. With these evaluations, this chapter ultimately seeks to establish the claim made in the thesis statement that warning distribution can be improved using network coding technique in the data dissemination procedure.

The rest of the chapter is organised as follows: Section 7.1 presents the simulation environment, Section 7.2 introduces the performance metrics, Section 7.3 describes the method of study, Section 7.4 and 7.5 present the study of the effect of data traffic load and network density respectively, and finally Section 7.6 concludes the chapter with a summary.

## 7.1 Simulation Environment

The custom-built simulator and the mobility model described in Section 4.4 of Chapter 4 will be reused in the studies presented in this chapter. The Glasgow Mobility Model (GMM) used in the evaluations of the earlier chapters makes the use of a predefined vehicle generation rate presented in table 4.1 on page 52. In this model, the source acts as the vehicle generator on the street and the sink as absorber. Having absorbed a vehicle, the sink immediately sends it to the corresponding source for redeployment on the street without changing any communication parameter such as number of collisions, queuing delay etc. In this way the movements of the vehicles are kept uninterrupted throughout the simulation.

It is notable that vehicles only move in straight lines in this study and do not turn left or right at the junctions. Such states will be observed and evaluated later in Chapter 8. Due to the fact that vehicles travel with three different velocities and are passed from the sink to the source numerous time, the initial placement of vehicles does not strictly follow a common pattern and keeps changing as simulation progresses. This brings variation into the mobility and consequently makes the study more compelling.

## 7.2 Performance Metrics

The performance metrics are indicators of how worthwhile an investigated feature is. This chapter analyses the effectiveness of PWMs in NETCODE and uses RBSM and VSPCA as the benchmarking warning systems to compare the performance with. All three systems are evaluated using two broad categories of metrics. These are part of the metrics elaborately described in Chapter 4 but for the convenience of the reader, very brief description of each of those metrics are presented below.

The first category includes two network layer metrics:

- *Rate of Collision* – a metric expressing the number of transmission collisions encountered by a vehicle every second (on an average) during the simulation time.
- *Queuing Delay* – a metric expressing the time a warning requires to wait at the respective transmission queue (on an average) from the time of its generation (in milliseconds).

The second category involves five application layer metrics:

- *Accident-at-junction* – a metric expressing the fact that a potential accident had occurred at a particular junction. A junction will be counted towards this metric if it encounters at least one potential accident.

- *Blind-move* – a metric expressing that a particular junction had blind movement. A junction will be counted towards this metric if it does not encounter any potential accident at all and encounters at least one blind movement.
- *Safe-move* – a metric expressing that a particular junction had safe movement. A junction will be counted towards this metric if it does not encounter any potential accident or blind movement at all.
- *Potential Accident Undetected* – a metric expressing the number of potential accident undetected while a particular warning system is in operation during a simulation.
- *Potential Accident Detected* – a metric expressing the number of potential accident detected by a particular warning system during a simulation.

## 7.3 Method of Study

This chapter aims to analyse periodic warning messages focusing on the competition they experience and queuing delay they encounter during the transmission process. It also seeks to estimate their ability to detect potential accidents on the street. In order to achieve this goal, two studies have been conducted in this chapter with each having two versions – *moderate* and heavy. Like the previous chapters, the moderate version examines the network with a moderate data traffic load or network density whilst the heavy version stresses the network with a variable that is generally considered aberrant.

The first study investigates the effect of data traffic load on the performance metrics. Periodic Warning Messages (PWMs) are used to generate data traffic load in the network between 1 to 25 warning/sec to investigate how performance metrics react in response to the change of the load. The objective of this study is to observe how NETCODE and the other two protocols cope with the growing data traffic load in the network.

The second study investigates the effect of network density on the performance metrics of the warning systems. This study uses network densities between 10 to 50 vehicle/min by grouping streets based on their vehicle generation rate. For example, all streets having 50 vehicle/min network density are grouped together by averaging their performance metrics and so on.

This study has two pivots as it evaluates both network and application layer metrics. The network layer element examines collisions and queuing delays whilst the application layer counterpart reveals how the protocols perform in terms of detecting potential accidents. There will be careful evaluations to show the extent to which NETCODE stops or reduces number of accidents. In order to do that, the junctions presented in figure 4.4 (Page 55) are tested again

for safe-move, blind-move and accident-at-junction. In addition, the number of potential accident detected both at junctions and on straight streets (oneway single carriageways) during the simulation are also evaluated.

Both studies assume for simplicity that there are two lanes on each street and three fixed velocities available for vehicles. However, instead of randomly assigning lane and velocity, there will be an initial order of the placement of the vehicles. This order maintains the two second delay rule i.e. vehicles will be separated by a distance that requires at least two-seconds to travel. Besides, this order is intentionally prepared in such a way that at the beginning a vehicle with higher velocity cannot follow a vehicle with lower velocity in the same lane as to avoid any initial collision. This rule is only broken for two highest velocity vehicles who are placed at the very back of the street. These two vehicles pass through slower vehicles in front of them as simulation progresses. As mentioned earlier, when a vehicle is absorbed by a sink, it will be passed on to the corresponding source for redeployment on the street with its all parameters intact. With the help of this setup, potential accidents are deliberately created throughout the simulation to evaluate how many such accidents go undetected when vehicles operate with NETCODE, RBSM and VSPCA in the second study. It is also notable that the simulation is run reasonably long enough (600 sec) for generating coherent and stable results. An average of 20 trials is taken for each performance metrics at the end of the studies.

## 7.4 The Effect of Data Traffic Load

The study of the effect of data traffic load is performed by varying warning generation rate of the vehicles while keeping other parameters fixed. This study uses two different network densities. The first density is called *moderate* because it runs the simulation with 5 vehicle/min network density whilst the second density is called *heavy* and it uses 15 vehicle/min network density. There are two performance metrics evaluated in this study. These are *rate of collision* and *queuing delay*.

### 7.4.1 Network Density: *Moderate*

The study of the effect of data traffic load in moderate network density is used to evaluate PWMs in accident warning systems. The data traffic load is varied from 1 to 25 warning/sec in this study.

#### 7.4.1.1 Rate of Collision

It has been previously discussed in the literature that excessive rebroadcast is one of the factors that creates contentions in the wireless networks [104, 105]. This characteristic of the broadcast scheme was observed in relation to warning systems in Chapter 4. In this section, the evaluation further investigates this issue and shows that NETCODE significantly reduces contention in the network.

Figure 7.1 demonstrates the effect of data traffic load on the rate of collision in moderate network density. It shows that NETCODE encounters half of the collisions of RBSM and VSPCA confront during the simulation. This is due to the fact that NETCODE requires fewer transmissions to send the same number of warnings compared to the other two systems. Moreover, fewer transmissions imply less competition; hence the number of collisions also gets reduced.

This study observes that when the network operates with 5 vehicles generating a single PWM every second, the collision is very small in number. The network, however, starts to experience competitions when data traffic load is increased and at a rate of 10 warning/sec and onwards, there is no change in the rate of collision for all observed warning systems.

#### 7.4.1.2 Queuing Delay

This study examines the delay experienced by warnings in the transmission queue as they wait for access to the wireless medium.

This study shows the state of warnings at the transmission queue as to how they keep waiting to be able to obtain access to the wireless medium due to contentions. It was discussed earlier in Section 2.4 of Chapter 2 that wireless networks are inherently sequential and when a node attempts to make a transmission using the wireless medium, other nodes within its transmission range must backoff to avoid potential interference. Because of this procedural implication warnings waiting in the transmission queue must stay there until the sender node is granted access to the medium.

Figure 7.2 shows that all three warning systems experience negligible queuing delay when the data traffic load is 5 warning/sec or less. However, their performance diverges as the data traffic load increases. It is important to realise that both RBSM and VSPCA reach *MTQD* of 2 sec at 15 warning/sec traffic load and still keep growing to hit a queuing delay between 3500 and 4000 ms at 25 warning/sec traffic load. The proposed warning system, on the other hand, exhibits a slow growth and stays below 1500 ms at 25 warning/sec traffic load.

This study further confirms the claim made in the thesis statement that the network coding based approach is an effective technique to reduce transmissions and subsequently delays in

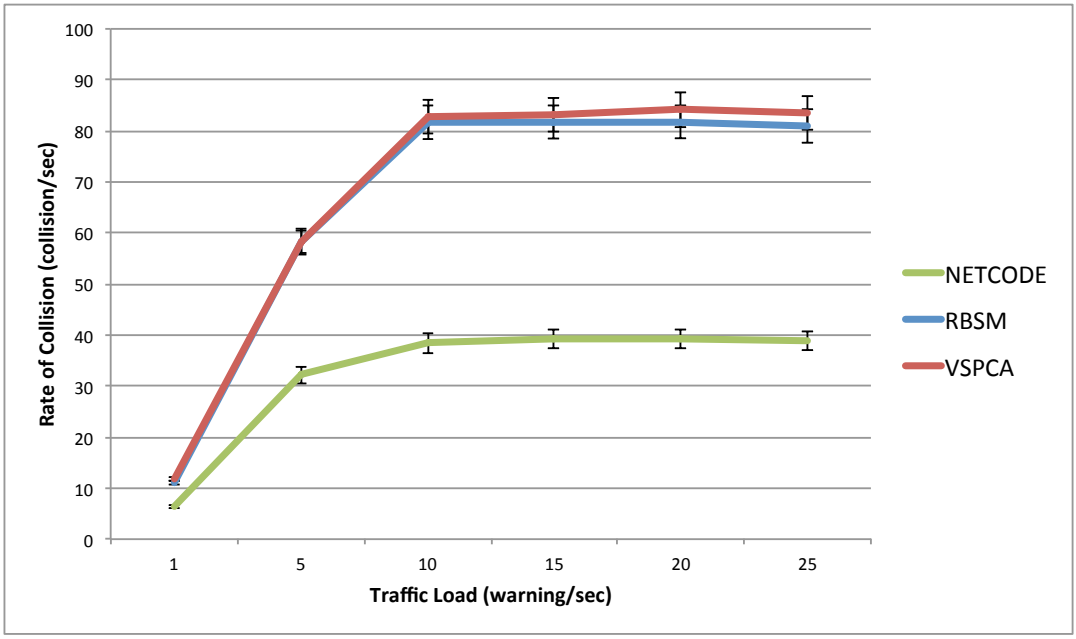



Figure 7.1: The effect of data traffic load on the rate of collision in moderate network density.

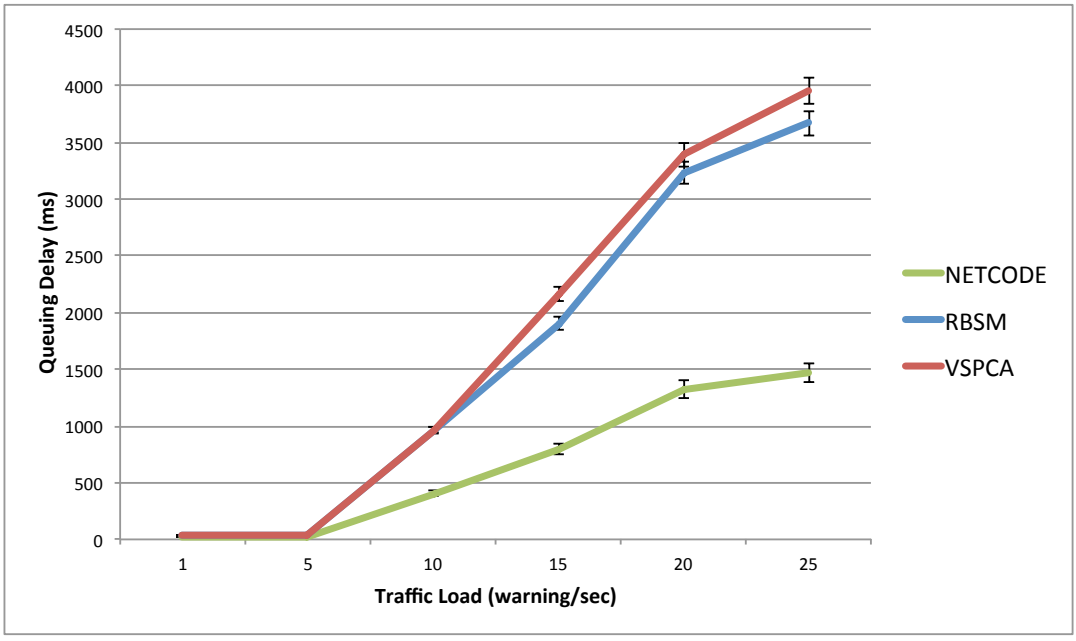



Figure 7.2: The effect of the data traffic load on the queuing delay in moderate network density.

the warning delivery process. The encoding and decoding algorithms presented in Chapter 5 form the basis of the data dissemination scheme that helps keeping the transmission queuing delay within the threshold of *MTQD*.

### 7.4.2 Network Density: *Heavy*

The study of the effect of data traffic load in heavy network density, like its *moderate* counterpart, is used to investigate PWM in accident warning systems and conducted by varying the data traffic load between 1 to 25 warning/sec. However, the network density in this study will be 15 vehicle/min. The performance metrics used in previous section will be reused here.

#### 7.4.2.1 Rate of Collision

Figure 7.3 is the counterpart of the figure 7.1 shown earlier. This current figure demonstrates a continuation of its counterpart and reveals that with 15 vehicle/min network density, rate of collision climbs from the very beginning. There is a notable feature in this observation. All three warning systems experience a steady rate of collision that is different than what had been observed with moderate network density.

In this simulation, the NETCODE rate is nearly half of the rate of RBSM and VSPCA. This is again due to the fact stated earlier that with the help of network coding, NETCODE reduces transmission and subsequently reduces collisions too. This improvement is likely to reduce the transmission queuing delay observed in the next section.

#### 7.4.2.2 Queuing Delay

Figure 7.4 demonstrates that the transmission queuing delay in heavy network density starts to grow earlier than that observed in moderate network density. This is because of the presence of more vehicles on the roads that not only fight for the access to the wireless medium but also generate more warnings (i.e. data traffic) in the network. In the moderate network density where more than 5 warning/sec data traffic was required to get a queuing delay of around 300 ms, in this heavy network density warning systems experienced same delay with only 1 warning/sec traffic load.

It is notable that despite early growth the NETCODE delay copes with the increase in load and prevents the transmission queuing delay from growing unacceptably. It successfully keeps the delay within 1500 ms, the same delay observed in moderate network density and below the *MTQD*; however, RBSM and VSPCA fail to meet this requirement with delays

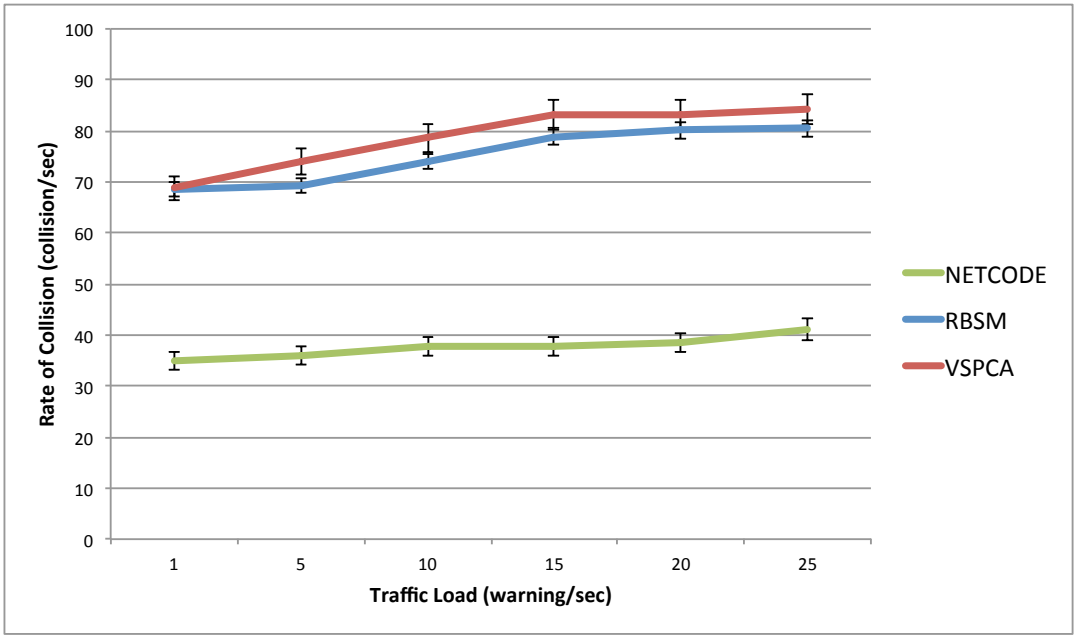



Figure 7.3: The effect of data traffic load on the rate of collision in heavy network density.

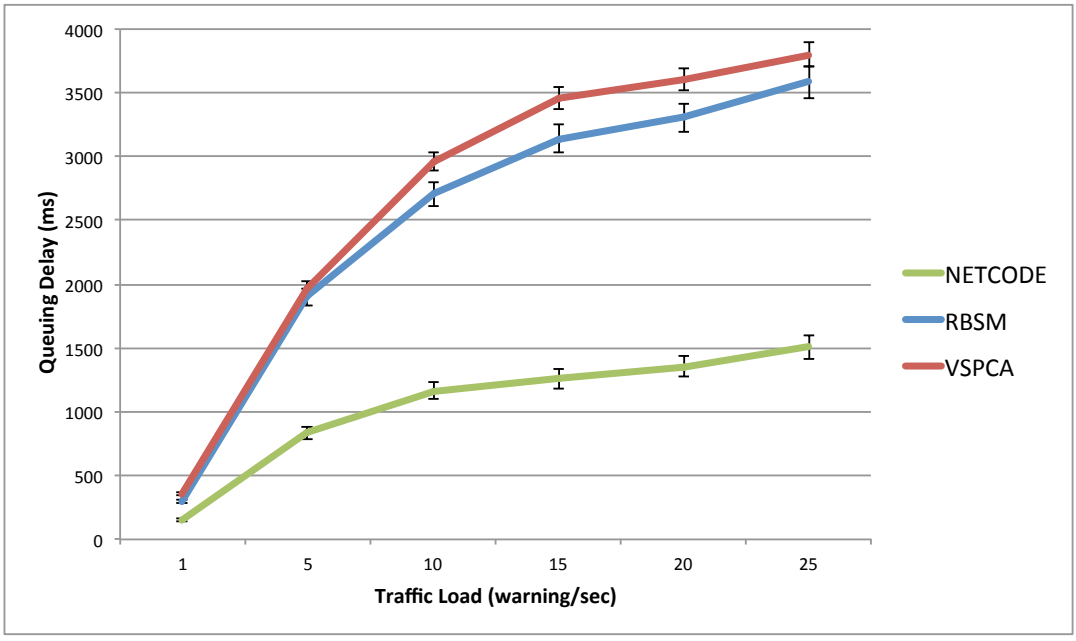



Figure 7.4: The effect of data traffic load on the queuing delay in heavy network density.

surpassing the *MTQD* at a load of only 5 warning/sec. They again hit the region between 3500 and 4000 ms when traffic load is 25 warning/sec.

### 7.4.3 Summary of the Study

The study of the effect of data traffic load is one of the two studies performed in this chapter to accomplish the fifth research objective, i.e. analysing the performance of the proposed scheme concerning PWMs as to how effectively they keep neighbouring vehicles informed about the presence of the host vehicle and how this information is materialised to detect potential accidents.

This indicates that with vehicles generating a single PWM every second, the collision is very small in number but it quickly accelerates as the network starts to have growing number of data traffic load. This behaviour subsequently results in longer queuing delay. It is, however, notable that despite this growth the NETCODE delay copes with the increase in load and prevents the transmission queuing delay from growing unacceptably.

This study further confirms that the use of network coding is an effective method for reducing the number of transmissions and subsequently collisions. It improves the performance of the data dissemination scheme by allowing NETCODE to operate with a transmission queuing delay that is half that of the other two observed systems. This study also confirms that at both moderate and heavy network densities, NETCODE complies with the *MTQD* requirement and is therefore be likely to detect more potential accidents than the other systems.

## 7.5 The Effect of Network Density

The study of the effect of network density is performed by varying the rate of vehicle generation while keeping other parameters fixed. This study uses two different data traffic loads. Like the previous study, the first data traffic load is named *moderate* and uses 5 warning/sec as recommended in Chapter 4. The second is called *heavy* and uses 15 warning/sec. This study will evaluate all performance metrics mentioned in section 7.2.

### 7.5.1 Data Traffic Load: *Moderate*

The network density of this study is determined by the rate of vehicle on streets shown in table 4.1 of Chapter 4. Five network densities, 10, 20, 30, 40 and 50 vehicles/min, are used in this study and the average over 20 trials is taken for each metric.

#### 7.5.1.1 Rate of Collision

Figure 7.5 shows the rate of collisions in the network. In addition to the observation made in Chapter 4, it further confirms that when more vehicles enter into the same enclosed area, competition for accessing the medium gets stiffer and streets with more vehicles tend to have more collisions. This figure also suggests that as network density increases, the number of rebroadcasts by RBSM and VSPCA significantly increases in the network raising the likelihood of experiencing broadcast storms.

It is, however, noteworthy that NETCODE encounters less than half of the collisions the other two systems experience. The network coding based data dissemination scheme demonstrates stable performance throughout the simulation and despite the change in network density, there is no growth in the rate of collisions for NETCODE. This behaviour suggests that the newly proposed system avoids creating broadcast storms in the network for the network densities used in the simulation.

#### 7.5.1.2 Queuing Delay

The results in figure 7.6 demonstrate the effect of network density on the queuing delay while operating with moderate data traffic load. It further confirms the claim that as more vehicles enter a street, competition for accessing the medium gets stiffer. It also demonstrates that RBSM and VSPCA experience long queuing delays as a consequence of the competition shown in Section 7.5.1.1 due to excessive collisions.

VSPCA exhibits a sharp rise that begins with a delay just below 2 sec and doubles as the network density doubles. Subsequently this delay touches 6 sec mark when network density is between 30 and 50 vehicle/min. As RBSM only forwards warnings up to five hop distance, it generates less rebroadcasts than VSPCA. It is reflected in its queuing delay that lies between 4 and 5 sec mark. Nonetheless, NETCODE maintains a steady queuing delay below *MTQD* which does not grow with the increasing network density.

#### 7.5.1.3 Junctions

There are total 44 junctions in the simulation as shown in figure 4.11 of Chapter 4. When vehicles moved through these junctions, three situations can occur: i) Accident-at-junction; ii) Blind-move; and iii) Safe-move. At the end of the simulation of each trial, these junctions are observed and marked i, ii or iii as appropriate.

Figure 7.7 clearly demonstrates that by keeping a transmission queuing delay below *MTQD*, NETCODE is successful in achieving most safe-moves at the junctions. Out of 44 junctions, only a few of them experience potential accident or blind-movement whilst most of

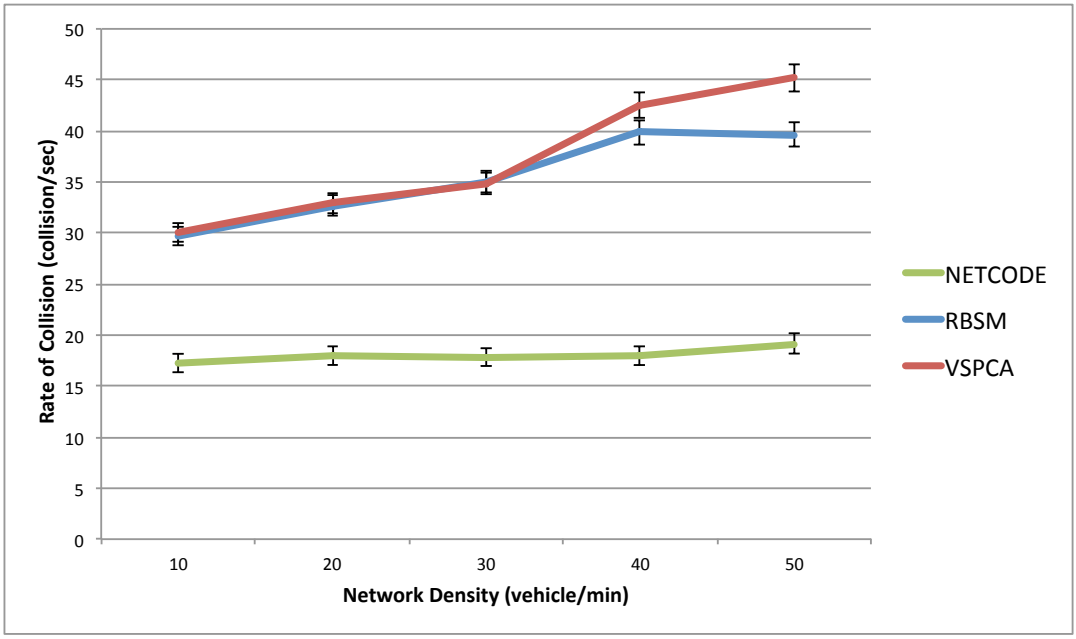



Figure 7.5: The effect of network density on the rate of collision in moderate data traffic load.

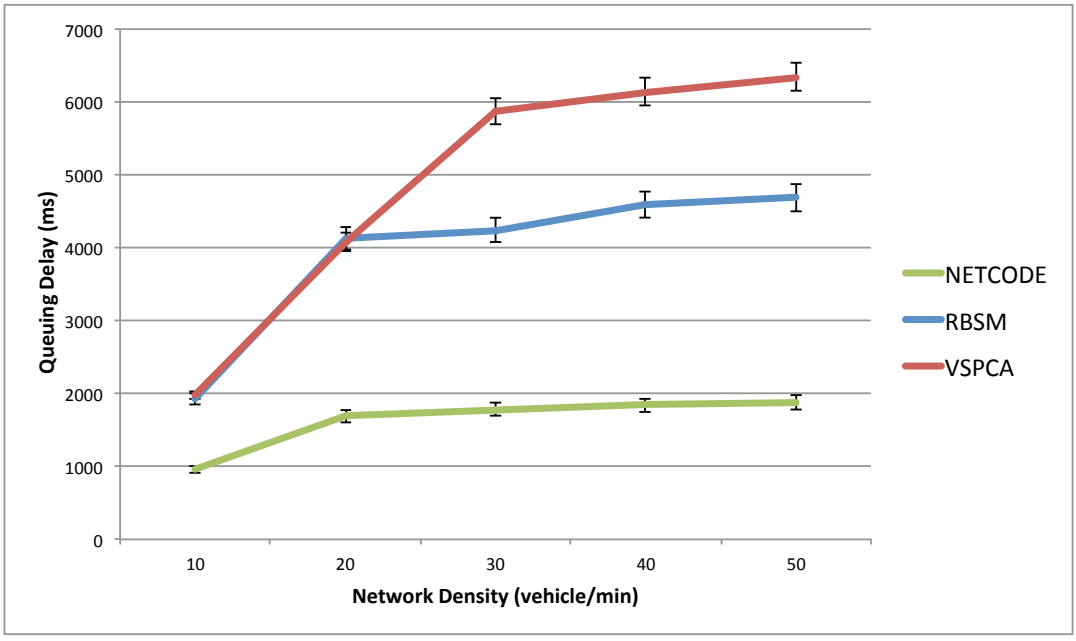



Figure 7.6: The effect of network density on the queuing delay in moderate data traffic load.

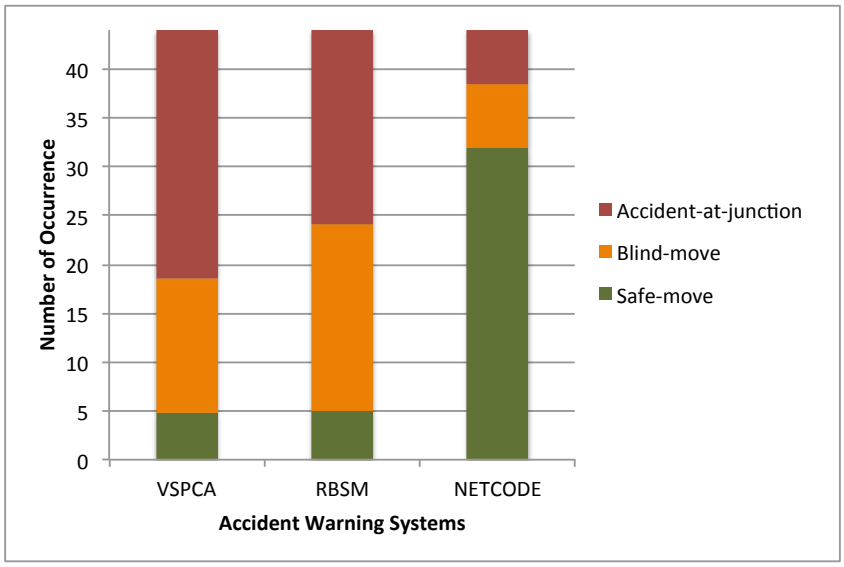



Figure 7.7: The movement at the junctions in moderate data traffic load.

the junctions have safe-movement. In contrast, VSPCA and RBSM experience potential accident or blind-movement on most of the junctions. This behaviour can be explained by the results presented in Section 7.5.1.1 and 7.5.1.2 earlier. As RBSM and VSPCA experience long queuing delays in high network densities, they encounter more potential accidents and blind-movements at the junctions. However, NETCODE efficiently controls the competition and subsequently the delay; hence most of the junctions experience safe-move.

#### 7.5.1.4 Potential Accident Undetected

In this study, the streets are grouped together based on their network densities and the number of potential accidents undetected in those groups are observed. In section 7.3, it is mentioned how vehicles are placed in the street at the beginning of the simulation. Two vehicles running at 50 mph velocity from the back of the streets will hit slower vehicles on course of moving forward. These actions make sure that deliberate potential accidents occur from the beginning in the simulation and this paves the way for testing the effectiveness of the warning systems.

Figure 7.8 shows the number of accidents undetected against different network densities. In the lowest network density, RBSM and VSPCA perform almost identically and fail to detect slightly more than 10 potential accidents. In contrast, NETCODE in the same density detects every single potential accidents. As the network density grows, RBSM and VSPCA fail to detect more potential accidents and in the highest network density roughly 40 to 50 potential accidents go undetected when these two warning systems are in operation.

The performance observed here is quite simple to understand: when vehicles experience long queuing delay, they fail to disseminate warning messages on time which ultimately

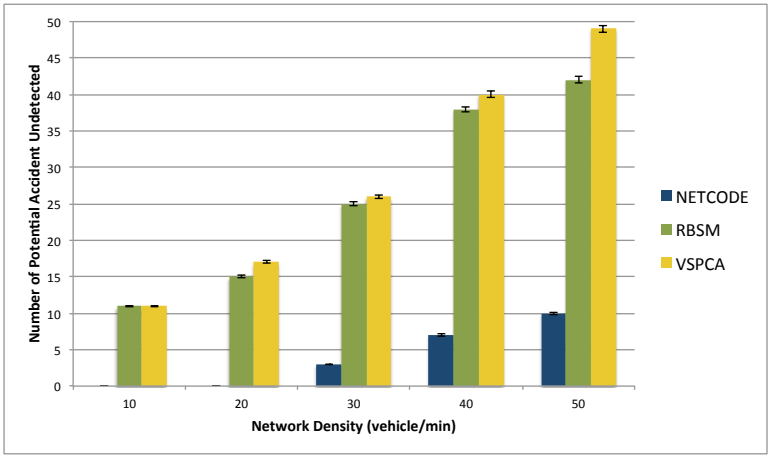



Figure 7.8: The number of potential accident undetected in moderate data traffic load.

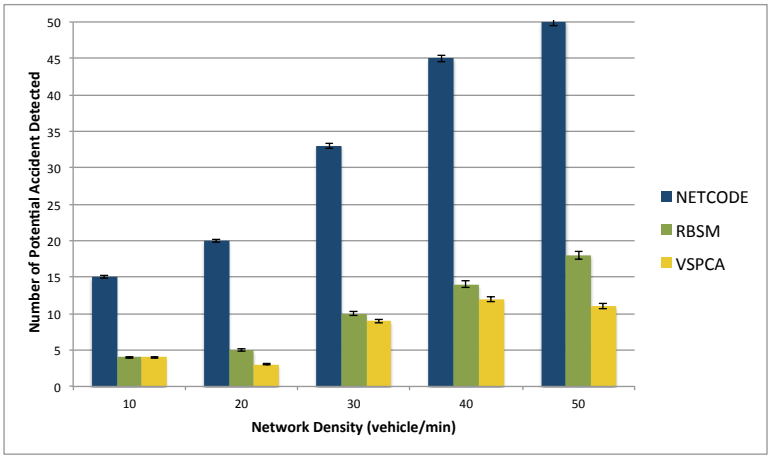



Figure 7.9: The number of potential accident detected in moderate data traffic load.

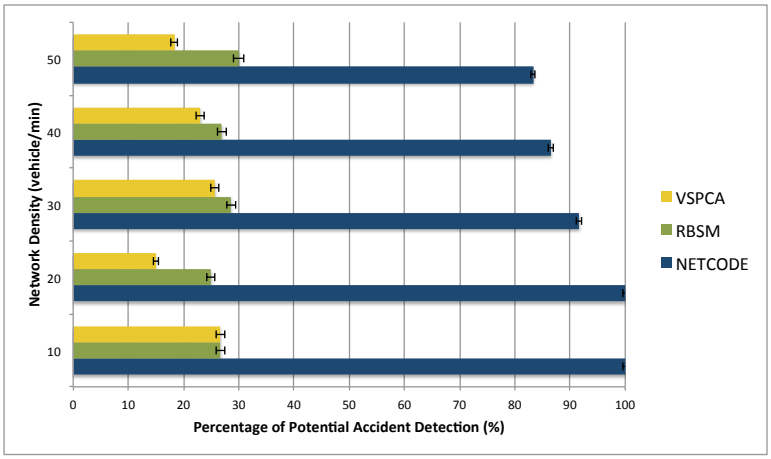



Figure 7.10: The percentage of potential accident detection in moderate data traffic load.

| *Network Density* | *VSPCA* | *RBSM* | *NETCODE* |
|---|---|---|---|
| *(vehicles)* | *(out of)* | *(out of)* | *(out of)* |
| 10 | 1 out of 4 | 1 out of 4 | 1 out of 1 |
| 20 | 1 out of 7 | 1 out of 4 | 1 out of 1 |
| 30 | 1 out of 4 | 1 out of 4 | 5 out of 6 |
| 40 | 1 out of 5 | 1 out of 4 | 5 out of 6 |
| 50 | 1 out of 6 | 1 out of 4 | 5 out of 6 |

Table 7.1: The prevention rate of the potential accident by VSPCA, RBSM and NETCODE in presence of *moderate* data traffic load.

makes their warning systems vulnerable. It is important to realise that by maintaining a lower queuing delay NETCODE effectively detects most of the potential accidents in the simulation. The next observation will complement this discussion by showing the number of potential accidents detected by these systems during the simulation.

#### 7.5.1.5 Potential Accident Detected

The total number of undetected potential accidents tells us how badly the systems perform but does not give the account of how many accidents are detected. A complete picture cannot be observed without exploring both metrics. Hence, the current observation will complement the discussion presented in previous section by showing the potential accident undetected and detected ratio. Figure 7.9 demonstrates the number of accident detected during the simulation and figure 7.10 shows the percentage of potential accident detection out of the total possible accidents. From these observations, it is clear that when RBSM and VSPCA fail to detect just over 10 potential accidents in the lowest network density, they detect slightly less than 5 potential accidents on the same streets. So for every four potential accidents these two systems are able to detect only one in the lowest network density. NETCODE on the same streets with same network density detects all potential accidents that it encounters.

The performances on the streets with 50 vehicle/min network density show more vulnerability with regard VSPCA but RBSM performs almost identical. When these two systems have nearly 40 and 50 undetected potential accidents respectively, they can only detect around less than 20 and slightly more than 10 potential accidents. So RBSM and VSPCA are capable of detecting one for roughly every four and six potential accidents respectively. However, on the same streets with same network density NETCODE detects around 50 potential accidents whilst missing only 10. This makes NETCODE detecting five accidents for every six possibilities.

### 7.5.2 Data Traffic Load: *Heavy*

The evaluated warning systems have been tested using a moderate traffic load in the above studies. Now at this phase of the study, a traffic load of 15 warning/sec is used to observe how performance metrics respond to such a heavy traffic load. The use of 15 warning/sec data traffic load is not normal but still used in this study as stress test to see how much the performance deviates from the expected behaviours. It is, therefore, not the objective of this study to observe how effectively systems are performing in this study.

Like the previous study, the network density is determined by the rate of vehicle on streets shown in table 4.1. Five network densities, 10, 20, 30, 40 and 50 vehicles/min, are used and an average over 20 trials is taken for each metric.

#### 7.5.2.1 Rate of Collision

Figure 7.11 shows the rate of collisions in the network in the presence of a heavy data traffic load. If this result is compared with the previous results described in 7.5.1.1, a slight increment in rate of collision can be observed for network density over 30 vehicle/min. VSPCA, RBSM and NETCODE – all three warning systems, however, encounter same number of collisions as they encounter in Section 7.5.1.

#### 7.5.2.2 Queuing Delay

The results in figure 7.12 demonstrate the effect of network density on the queuing delay of warnings while operating with heavy data traffic load. The previous section shows a large rate of collisions in the network at higher network densities. If we compare that results with queuing delay observed here, we find that in presence of heavy data traffic load – in this case created by 15 PWMs per sec – VSPCA and RBSM experience as large as 9 and 7 sec delays respectively. Although NETCODE outperforms those systems in performance, it also fails to maintain the *MTQD* threshold. This indicates that despite having a better performance, NETCODE is unlikely to match the performance it demonstrated with moderate data traffic load in terms of detecting potential accidents.

It is also interesting to observe in these results that for lower network densities due to small change in the rate of collision, queuing delay increases remarkably. This behaviour can be explained by realising that because of the prolonged queuing delay vehicles enter into a state where they cannot transfer data that in turns reduces competition; hence the collisions. This scenario changes after some time when vehicles start to transmit data and again create a fierce competition. As this practice continues back and forth in presence of a heavy data

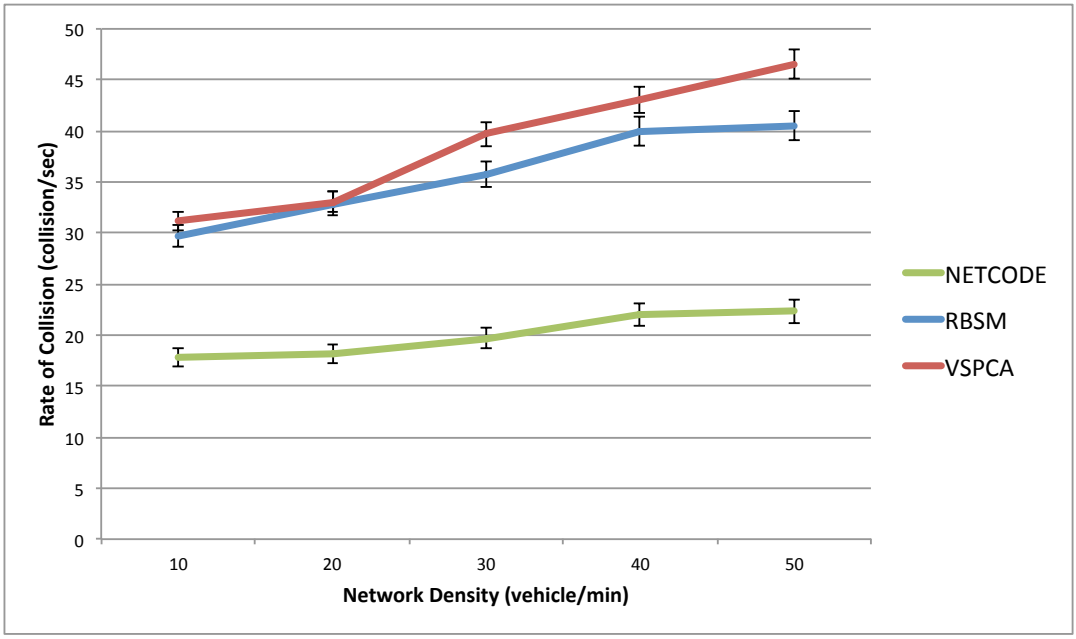



Figure 7.11: The effect of network density on the rate of collision in heavy data traffic load

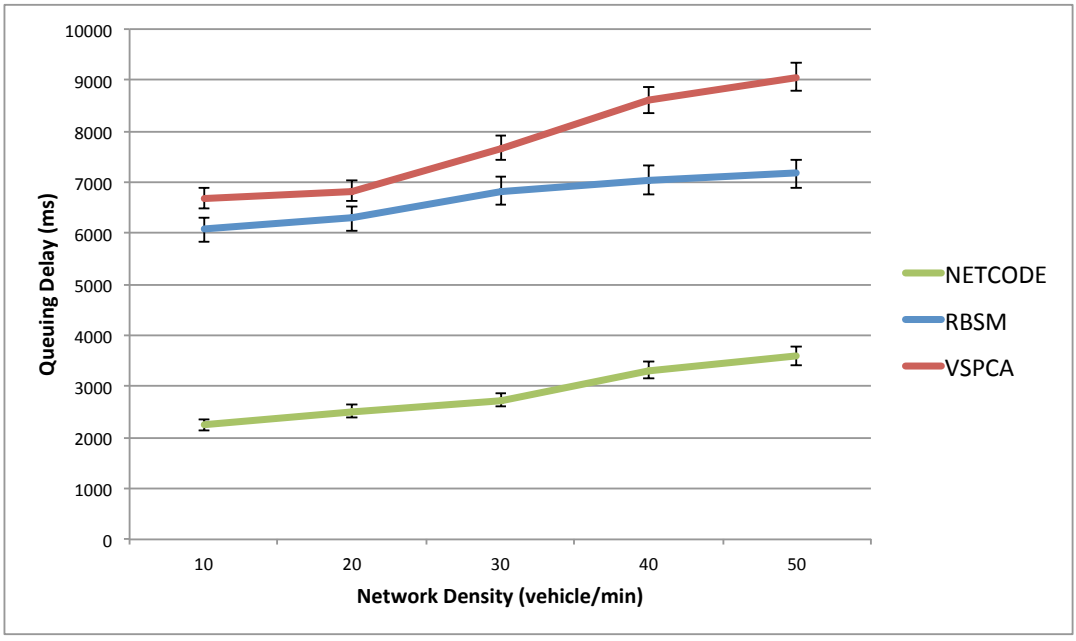



Figure 7.12: The effect of network density on the queuing delay in heavy data traffic load

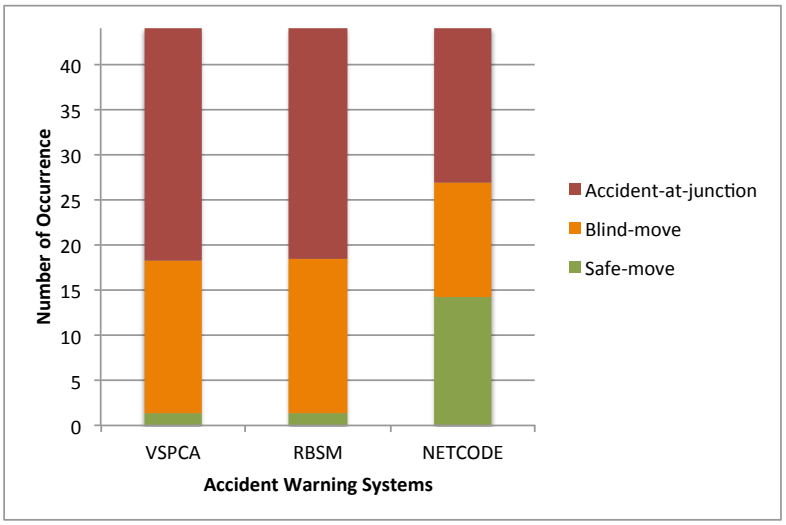



Figure 7.13: The movement at the junctions in heavy data traffic load.

traffic load, the rate of collision does not experience a hike in lower densities but queuing delay does.

#### 7.5.2.3 Junctions

The junctions described in Section 7.5.1.3 will be reused here. In presence of the heavy data traffic load, the queuing delays for all three warning systems rise at different rates from the very beginning and deviate from the performance demonstrated for a moderate data traffic load in Section 7.5.1.2. This change in queuing delay significantly affects the statistics measured for the circumstances recorded at the junctions.

Figure 7.13 demonstrates that RBSM and VSPCA encounter almost same number of accident-at-junction, blind-move and safe-move. NETCODE shows significantly better performance than these two systems. However, as anticipated in the previous section, its performance degrades substantially compared to the results observed with moderate data traffic load in figure 7.7.

#### 7.5.2.4 Potential Accident Undetected

It is mentioned earlier that the streets are grouped based on their densities in this simulation and the number of accidents undetected in those groups are recorded during the simulation. Figure 7.15 shows that all systems have more undetected potential accidents than they have in moderate traffic load. VSPCA and RBSM fail to detect nearly 15 and 60 potential accidents in the lowest and the highest network densities respectively. Although this performance is not unexpected after what we have observed earlier, the performance NETCODE exhibits is more interesting. With a heavy data traffic load, it fails to detect more than 30 potential

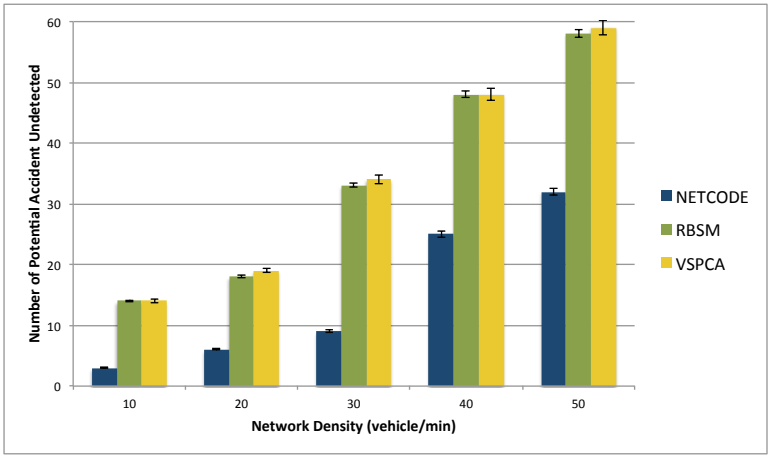



Figure 7.14: The number of potential accident undetected in heavy data traffic load.

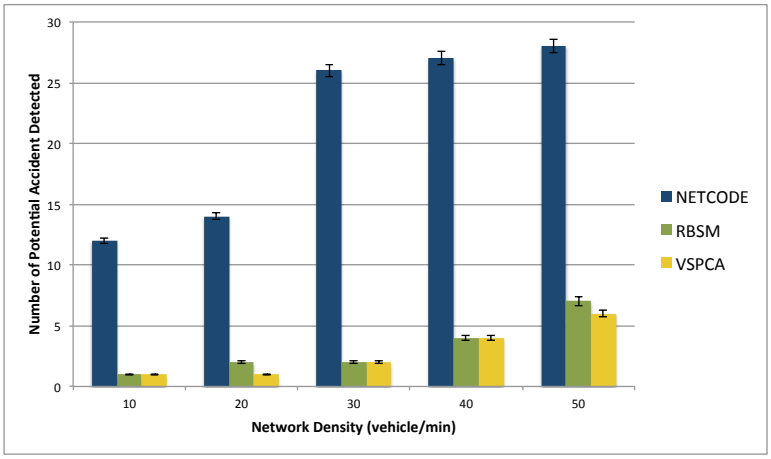



Figure 7.15: The number of potential accident detected in heavy data traffic load.

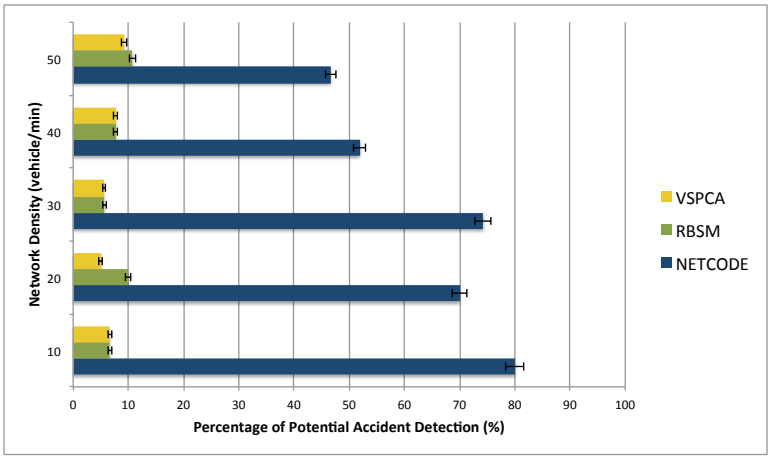



Figure 7.16: The percentage of potential accident detection in heavy data traffic load.

accidents; three times larger than what NETCODE does with moderate traffic load. This downfall in NETCODE's performance can be explained by realising that with a transmission queuing delay more than *MTQD* (particularly as large as almost twice on the streets having 50 vehicle/min network density demonstrated in figure 7.12), the proposed warning system finds itself isolated failing to send data to the neighbour vehicles. This isolation turns out to be fatal as NETCODE is unable to detect significantly many potential accidents.

#### 7.5.2.5 Potential Accident Detected

The number of potential accident detected shows us the vulnerability of the systems but does not tell how bad they performed until the results are compared with the number of accident undetected. Hence, the current observation will complement the discussion presented in previous section by showing the potential accident undetected and detected ratio. Figure 7.15 demonstrates the number of accident detected during the simulation and figure 7.16 shows the percentage of potential accident detection out of the total possible accidents. From these observations, it is clear that even under heavy data traffic load, NETCODE performs significantly better than its counterparts. Table 7.2 further summarises the results and shows that in the lowest network density, when RBSM and VSPCA fail to detect nearly 15 potential accidents, they detect around one. In contrast, NETCODE fails to detect around 3 potential accidents and detects more than 10; making it detecting four out of every five potential accidents. NETCODE's performance, however, degrades significantly on the streets having the highest network density in the simulation. When RBSM and VSPCA are capable of detecting one out of 9 and 11 potential accidents respectively, NETCODE detects around one for every two possibilities (downgraded from four for every five possibilities).

### 7.5.3 Summary of the Study

The study of the effect of network density is performed in this chapter with a view to accomplish the fifth research objective stated in Chapter 1. In Section 7.4.3, a summary of the effect of data traffic load is presented to partially fulfil this objective and with this summing-up, it will be completed.

This study unfolds how warning systems perform in response to growing network densities in the network. As this is comprised of evaluations covering both application and network layer, it provides with an analysis on the performance of the warning systems, particularly on the newly proposed NETCODE. The outcomes of this study clearly shows that NETCODE is capable of detecting potential accidents, the principal objective of any warning system. While doing so, it also successfully keeps the transmission queuing delay below the threshold *MTQD*.

| *Network Density* | *VSPCA* | *RBSM* | *NETCODE* |
|---|---|---|---|
| *(vehicles)* | *(out of)* | *(out of)* | *(out of)* |
| 10 | 1 out of 15 | 1 out of 15 | 4 out of 5 |
| 20 | 1 out of 20 | 1 out of 10 | 7 out of 10 |
| 30 | 1 out of 18 | 1 out of 18 | 13 out of 18 |
| 40 | 1 out of 13 | 1 out of 13 | 1 out of 2 |
| 50 | 1 out of 11 | 1 out of 9 | 1 out of 2 |

Table 7.2: The prevention rate of the potential accident by VSPCA, RBSM and NETCODE in presence of *heavy* data traffic load.

This study sums up that as network density increases, existing warning systems struggle to cope with and fail to disseminate warning messages on time. However, the newly proposed warning system overcomes those difficulties by using network coding based dissemination technique that uses less transmission and subsequently creates less competition in the network. As a result of this behaviour, it keeps a small transmission queuing delay and delivers warnings messages in a timely manner to detect potential accidents. Thus, these achievements successfully establish the fact that the XOR-based network coding provides a potential solution that effectively constructs a data dissemination scheme to make timely delivery of warning message.

## 7.6 Summary

The observation made in Chapter 4 finds that broadcast-based data dissemination schemes are not efficient enough to cope with the environment where data traffic load or network density significantly grows. In order to overcome their shortcomings, a new XOR-based accident warning system, NETCODE, is proposed in Chapter 5. This current chapter presents the performance analysis of Periodic Warning Message (PWM) dissemination by this new system. While doing so, the studies conducted in this chapter reuse two previously observed warning systems (RBSM and VSPAC) and compares the performance of newly proposed NETCODE in response to the change of data traffic load and network density. The observations made in this chapter find that NETCODE disseminates PWMs effectively and efficiently compared to other two systems and are capable of detecting potential accidents even if the network density grows substantially. This chapter reconfirms the claim (T1) made in the thesis statement that XOR-based network coding provides a potential solution on which a data dissemination scheme can be built, a solution that helps reduce the warning delivery time without restricting the regular flow of warning message.

# Chapter 8

# Analysis of Event Driven Message Dissemination

The earlier chapters of this thesis focused on evaluating Periodic Warning Message (PWM) disseminated by both existing and newly proposed warning systems. Those chapters demonstrated the deficiency of the existing warning systems as to how they get exposed to broadcast-storms while delivering warning messages and how network coding plays a role in reducing the number of transmissions and subsequently delivery time. It is, however, still unexplored as to how those systems respond when deliver Event Driven Messages (EDMs) and the current chapter addresses this issue.

This chapter will show that priority-based warning dissemination can potentially improve the performance of EDM. The motivation behind this idea is that, as EDMs represent actual existing events as opposed to PWMs which are generated periodically and allowed to propagate even if there is no real threat, the former should receive priority over the latter in the dissemination process. The studies presented in this chapter scrutinise this proposition by comparing performance of warning systems with and without priority. In addition, these studies also explore the prospect of sending multiple EDMs for the same event.

The rest of the chapter is organised as follows: Section 8.1 provides a rounded discussion on the priority-based warning dissemination, Section 8.2 talks about the effectiveness of using multiple EDMs, Section 8.3 presents the simulation environment, Section 8.4 discusses the performance metrics used in the studies, Section 8.5 provides with the method of study and Section 8.6 and 8.7 present two studies involving a free-flow road and a roundabout respectively before the chapter concludes with a summary in Section 8.9.

## 8.1 Priority-based Warning Dissemination

It is important to consider, for the design of an Accident Warning System (AWS), that the introduction of priority-based dissemination should be complementary to its operation not compulsory. Prioritising warnings determines precisely what type of warning should be favoured over other types at each node, and thus forms the basis of a decision as to who should get the access to the medium first. It is, however, hardly seen in the design of the existing warning systems and a serious effort to evaluate its full potential is long overdue.

It is argued in the thesis statement that priority-based warning delivery can potentially improve performance of AWSs particularly in regard to EDMs. This is due to the fact that, unlike PWMs that nodes generate at a regular intervals, EDMs are sporadically generated and the presence of such warnings in the network clearly indicates there exists a real danger because an incident[1] has already taken place. A warning carrying such vital information naturally holds immense importance and timely delivery of such warnings could potentially prevent actual fatalities.

Previously, priority-based dissemination was explored by SAVN and VSPCA as described in Section 3.2 of Chapter 2 but a complete classification of warning messages was never seriously attempted [62, 59]. It is particularly important because all warnings do not hold the same degree of importance and if we are to give them priority-based access to the medium, their urgency needs to be assessed carefully. As we have seen in Chapter 5, the design of NETCODE prioritises warning messages based on their types as well as where those warnings are coming from. Warnings generated within the node are called *local warning* and denoted as "L" whereas other warnings that nodes generally forward are called *forwarding warning* and denoted as "F". An EDM (L) is very time-sensitive as it is likely to carry important information for the vehicles who either directly follow or are located around the hosts. An EDM (F) is also important, if not as vital as an EDM (L), because this kind of warning forwards information about an incident that occurred within couple of hops. Naturally, NETCODE assigns the highest priority to EDM (L) followed by the second-highest to EDM (F). The complete list of priorities are presented in Table 5.2 (Page 78).

## 8.2 Single vs. Multiple EDMs

To the best of author's knowledge, there is no discussion in the literature as to how many EDMs should be sent in event of an incident. It is of course not sensible to send many repeated EDMs as this could create another flow of warnings capable of creating contention

[1]The phrase *incident* could indicate an accident or an event that could potentially lead to an accident such as emergency stop, dangerous driving, arrival of a vehicle at a junction, sensor generated notification and so on.

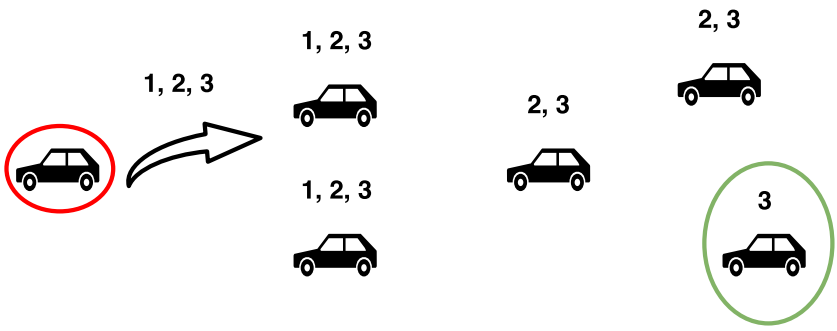



Figure 8.1: Multiple EDM dissemination in the network.

in the network; however; sending a small number of repeated warnings could potentially improve dissemination performance.

Although in event of an incident or emergency stop it is not always guaranteed that multiple EDMs can improve dissemination performance, particularly when the queuing delay is more than *MTQD*. Likewise when the queuing delay is short a single EDM is generally sufficient to inform the following vehicles about an incident. It is, however, different if the delay stays at the threshold of the *MTQD*. In such circumstances, an EDMs could face the long queuing delay resulting in expiration of a warning or might get stuck in a vehicle unable to forward it further due to isolation. This kind of situation is most likely when warnings travel over multi-hop paths and in these circumstances sending multiple EDMs might help reaching more vehicles.

Figure 8.1 demonstrates an example where vehicle marked with a red circle sends EDMs that flow over multi-hop path and reach other vehicles who are following the affected vehicle. During their journey, if one or two EDMs fail to reach a vehicle, a third EDM will certainly increase the possibility as shown in the figure by marking a vehicle with green circle. Although this is just an example but experimental study can show whether this claim is valid.

It is also noteworthy that Warning Generation (WG) unit of NETCODE in this chapter will be configured with three setups each sending 1, 2 and 3 EDMs respectively. Later the observation made in the analysis will confirm the effectiveness of using multiple EDMs over sending single message.

## 8.3 Simulation Environment

The simulation studies conducted in this chapter use two custom-built mobility models involving a free-flow road and a roundabout. These models are different from those previously used and are built for specific purposes to analyse the performance of EDMs. It is also no-

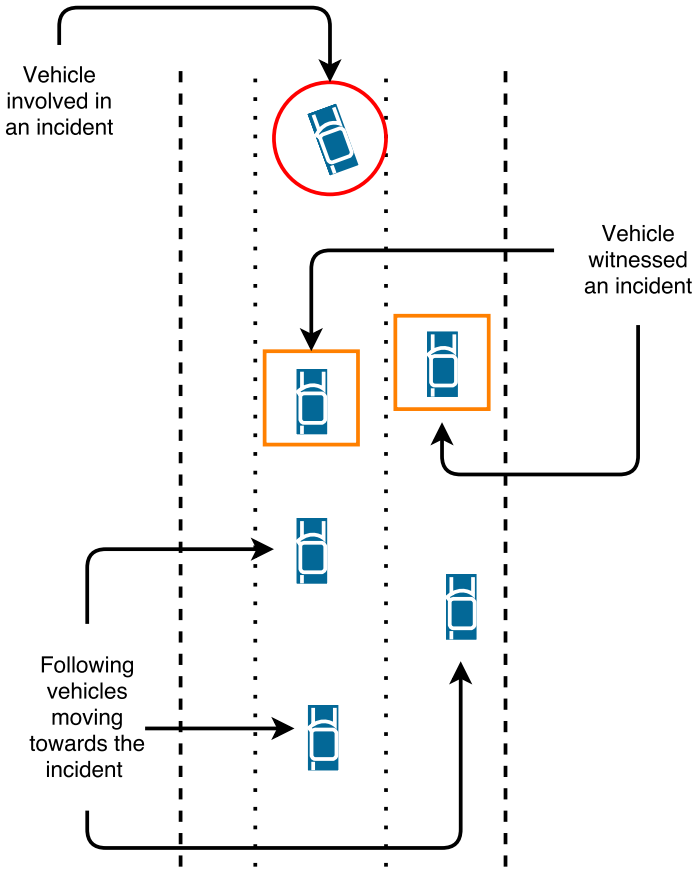



Figure 8.2: Free-flow Road: A two-lane motorway scenario with hard-shoulder on the left.

table that the scenarios used to build the models are perceived from the discussion presented in Section 3.3.1 of Chapter 3 (Page 32).

These mobility models are constructed on top of the network simulator Pamvotis and the simulation framework remains the same as described in Section 4.4.1 (Page 49). In addition to NETCODE, two other warning systems RBSM and VSPCA will reprise their role in the studies and form the basis of a performance comparison with the newly proposed warning system. The remaining part of this section describes the mobility models used in this study in detail.

### 8.3.1 Free-flow Road

The first mobility model is a free-flow road as shown in figure 8.2. It has two layouts: highway and urban. The highway layout uses a motorway scenario comprised of two-lanes with a hard-shoulder on the left. This mobility model works as follows: A set of vehicles with specific network density will be allowed to run 10 miles with 70 mph velocity in order to create a simple motorway situation before being abruptly interrupted by the lead vehicle stopping suddenly. Later observation will be made as to how effectively this stopped vehicle

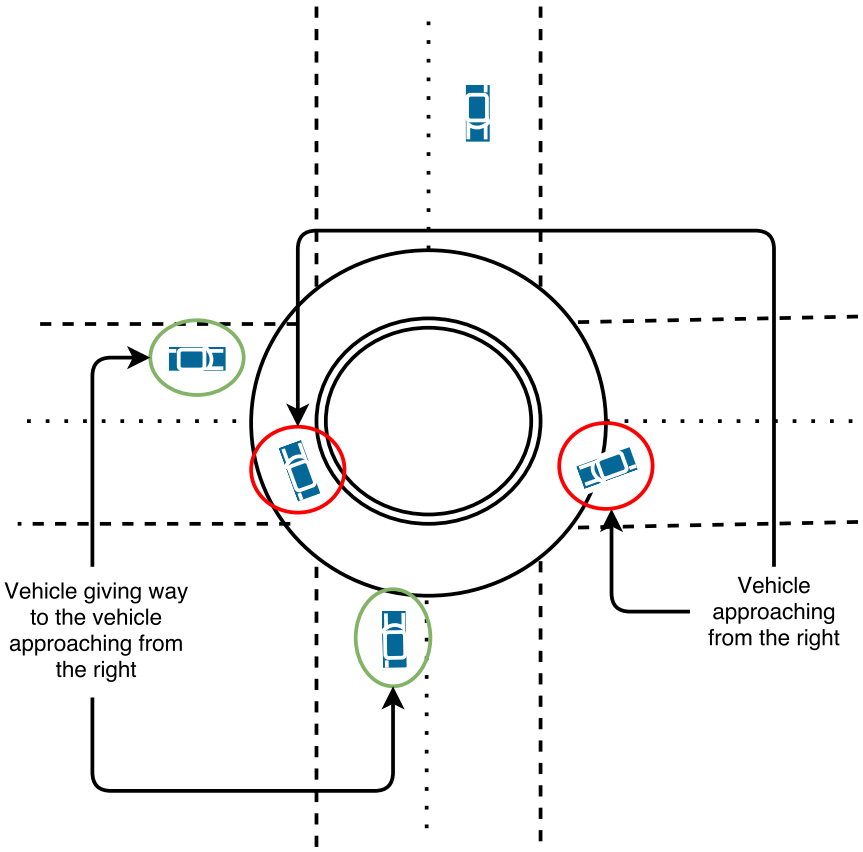



Figure 8.3: Roundabout.

disseminates EDMs to the following vehicles in preventing any potential collision.

This setup is also used to evaluate an urban layout with a dual-carriageway where vehicles move with a velocity of 30 mph. In the urban layout, however, the vehicles are allowed to run for 1 mile only before the incident is produced. The reduced distance simulate the fact that in contrast to a motorway, in the urban layout vehicles rarely get to move for more than a mile or so without stopping at junctions or in signal lights.

### 8.3.2 Roundabout

The second mobility model is a roundabout where vehicles approach from four sides and try to access the roundabout. There are two layouts like the previous model: a highway represented by a motorway and an urban layout represented by a dual-carriageway. In the highway layout, vehicles are placed 10 miles far from the roundabout (on the four sides) and allowed to commute at 70 mph velocity towards the roundabout on the motorway before stopping at the roundabout to give way to the vehicles approaching from the right. Having given way, vehicles start to move at 30 mph velocity towards one of the three options: left (first exit), moving straight ahead (second exit) or right (third exit). It is noted that only the vehicles on the right lane of the motorway are allowed to go to right and vehicles on the left

lane are randomly assigned exits to comply with the highway code of the United Kingdom [123]. In event of no vehicle approaching from the right, they are allowed to access the roundabout instantly at a velocity of 40 mph. This setup is, however, deliberately broken by a vehicle that approaches the roundabout despite having a vehicle on its right to which it should give way. At this point, the vehicle deprived off its right of receiving the way stops and generates an EDM for vehicles all around. The aim is to find how many vehicles who are supposed to receive the warning actually receive it.

This setup is also used for the urban layout with a modified velocity. In this case, vehicles approach the roundabout within 1 mile distance with a velocity of 30 mph. Upon stopping at the roundabout due to the presence of an approaching vehicle from the right, they start moving with a velocity of 20 mph. However, if there is no vehicle on the right, these vehicles pass through the roundabout with a velocity of 25 mph. The rest of the setup remains as described above.

## 8.4 Performance Metrics

The objective of the studies presented in this chapter is to observe and evaluate the effectiveness of the EDM in the context of warning systems in general and how NETCODE improves warnings of this type in particular. In order to achieve this goal, only one performance metric, *vehicle reached* is used in this chapter. This metric expresses the proportion of expected vehicles EDM reaches within the threshold time of 2 sec in the form of percentage. Despite the fact that only one metric is used, this does not detract from the usefulness of the studies here which focus on reachability.

One of the difficulties in observing this metric is to determine the vehicles who expect the EDM. It is challenging because of the fact that not all evaluated warning systems operate similarly while disseminating warnings. For example, VSPCA uses a flooding technique and sends warning to all connected vehicles; but RBSM incorporates only those vehicles that are connected within 5 hop distance. The multi-hop paths are also not same for all systems and the possibility of having alternative paths increases in dense situations depending on who receives and forwards warnings ahead of whom. Therefore, to overcome this challenge and discover the expected vehicles, each warning system is evaluated twice with identical settings. The first time EDMs are sent through a utopian MAC layer overlooking the delay. In this way EDMs are allowed to travel maximum 5 hops distance and the vehicles who receive the warning are marked. These marked vehicles are called *expected vehicles* in this chapter. This process will be followed by a second dissemination with identical setup but this time MAC layer behaves as standard [38]. The vehicles that receive EDMs within 2 sec of their generation are also marked and called *received vehicles*. Later the metric *vehicle*

*reached* will be calculated as follows:

$$Vehicle\ Reached\ =\ 100 \times \frac{Received\,Vehicles}{Expected\,Vehicles}\ \% \tag{8.1}$$

## 8.5 Method of Study

This chapter aims to analyse performance of EDM dissemination focusing on the coverage of the vehicles who are supposed to receive the warnings. To achieve this goal, the custom-built simulator utilised in previous chapters will be employed again. There are two studies in this chapter and each has two layouts namely *highway* and *urban* layouts. The highway layout is represented by a motorway scenario whilst the urban is represented by a oneway single carriageway. It is noted that a rigorous discussion on these scenarios and layouts can be found in Section 3.3.1 of Chapter 3.

The studies will have two versions of data traffic load, *moderate* and *heavy*, in the form of Periodic Warning Message (PWM). As used in previous chapters, 5 warning/sec represents moderate and 15 warning/sec heavy data traffic load. EDMs are, however, generated on-demand basis only when incidents occur. It is noteworthy that Section 5.4 of Chapter 5 discusses the operation of NETCODE using a state transition diagram. This diagram and related description explain how EDMs are prioritised by the proposed warning system ($State - 3$) and placed in a priority queue in order to be passed on to the next lower layer ($State - 11$).

The first study uses a free-flow road (freeway) as its simulation area. As vehicles generally move at a steady speed on this free-flow road, any form of unexpected abruption could potentially cause fatalities. This study takes the opportunity to explore the effectiveness of EDM dissemination in avoiding possible accidents. In doing so, the simulation is run with network densities 10, 20 and 30 vehicles. It is noted that in Chapters 4 and 7, network density is measured using the unit "vehicle/min" but in Chapter 6 and this current chapter the unit is just "vehicle". An explanation is presented to clarify this in Section 6.1.2 (Page 92).

In this study, vehicles are placed on the simulation area only once and allowed to commute around 10 miles with 70 mph and 1 mile with 30 mph velocity in two different experiments. When the vehicle located in front reaches exactly 10 mile distance in the motorway or 1 mile in the single carriageway, it is stopped abruptly. As soon as the vehicle gets stalled, it generates an EDM to warn the vehicles located around it. It is important to realise that in such circumstances only the witnessing vehicles have the knowledge of the incident but other following vehicles remain unaware of the event and keep moving towards a potential pile-up collision. It is also notable that as the incident takes place within a fraction of a second, even the drivers of the witnessing vehicles often cannot stop in time unless they have maintained

adequate stopping distance or have automatic braking technology. Thus, the effectiveness of EDM dissemination lies in how quickly the warning is disseminated to the vehicles who are actually in need of it. In doing so, a 2 sec threshold value is used and any EDM received after this threshold will not be considered "received".

The observation is made in this study as to how many witnessing and following vehicles receive the warnings with stopping instruction before colliding with the vehicles in front of them, as Equation 8.1 expresses. The Warning Generator (WG) of NETCODE (see Section 5.1.1 on page 74) is evaluated with three configurations. The first configuration sends only one EDM, the second sends two EDMs within an interval of 500 ms and the third sends three EDMs with a gap of 333 ms between the warnings. These three configurations pave the way to evaluate whether multiple EDMs for a single event help reach more of the expected recipient vehicles. Amongst the other warning systems, VSPCA uses priority-based dissemination but RBSM does not have this mechanism. A variant of RBSM with priority-based dissemination is also developed here to observe whether this improves the performance of this system. To complement the performance of EDMs, for all warning systems, effectiveness in identifying the stalled vehicle using PWMs is also observed and evaluated.

The second study involves two roundabout scenarios located in highway and urban layout each. This study takes the opportunity to explore the most common incident at a roundabout when vehicles fail to give way to the approaching vehicles from the right. Like the previous study, the simulation uses network densities of 10, 20 and 30 vehicles but this time on each side of the roundabout. The movement of vehicles is more complicated in this study and vehicles traverse the simulation area as described in Section 8.3.2. Normal movement is, however, broken for a randomly chosen vehicle (but same vehicle for all systems) that refuses to give way to a vehicle approaching from the right. At this point of the simulation, both vehicles stop at once and the deprived vehicle who was supposed to get the way generates the EDM to inform surrounding vehicles about this incident.

The observation is made in this study as to how EDMs are disseminated to cover all vehicles who expect it. These messages are disseminated not only to the following vehicles but also to other vehicles located on the first, second and third exits. The rest of the setup is the same as the previous study i.e. NETCODE generates 3 EDMs as described above and a variants of RBSM is used to explore its improved capability with priority-based dissemination. PWMs of all three warning systems are also evaluated and observed in this study.

## 8.6 The Study of EDM on the Free-flow Road

The study of the free-flow road is expressed by varying the network density against the percentage of vehicles reached while keeping other parameters fixed. Previously mentioned

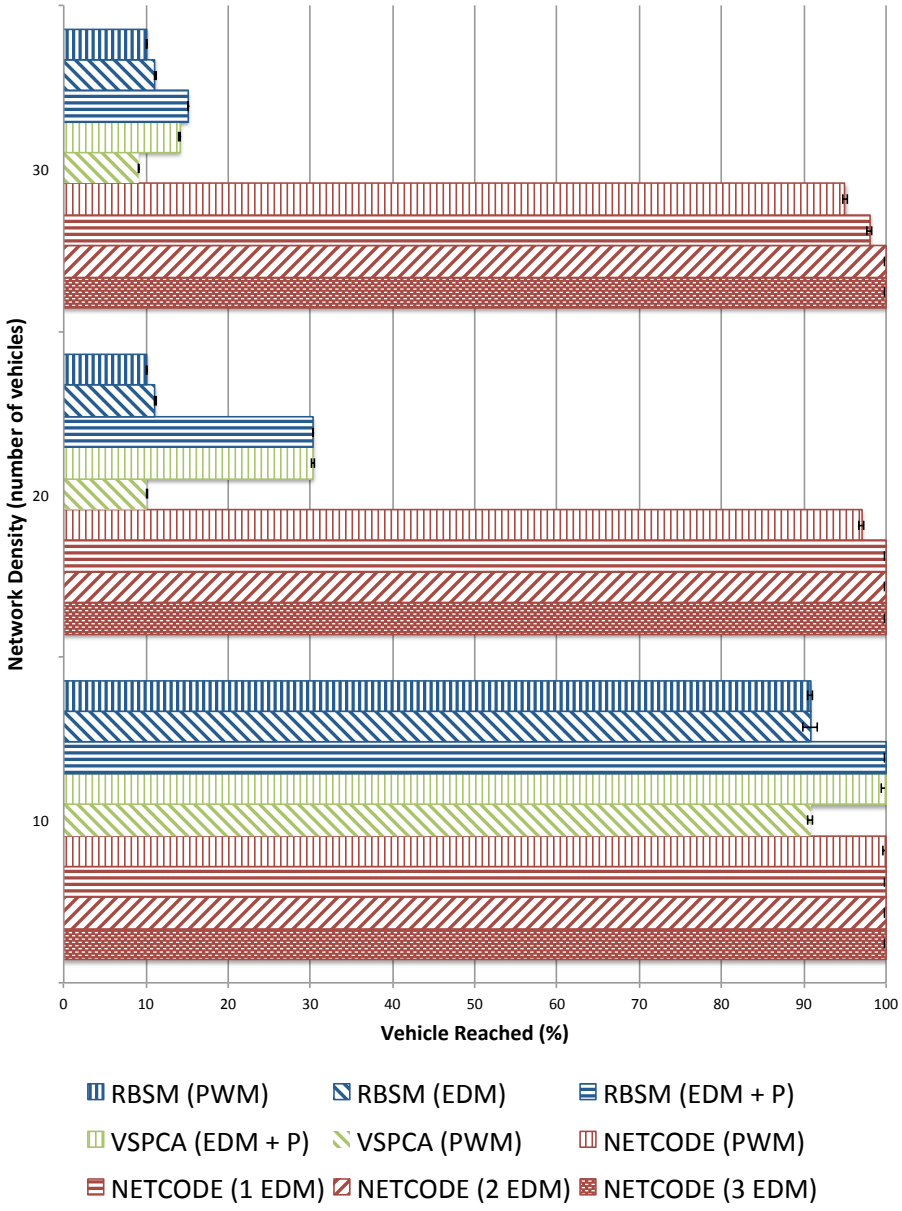



Figure 8.4: Percentage of vehicle reached by EDM and PWM on the free-flow road at 70 mph velocity (motorway) with moderate data traffic load.

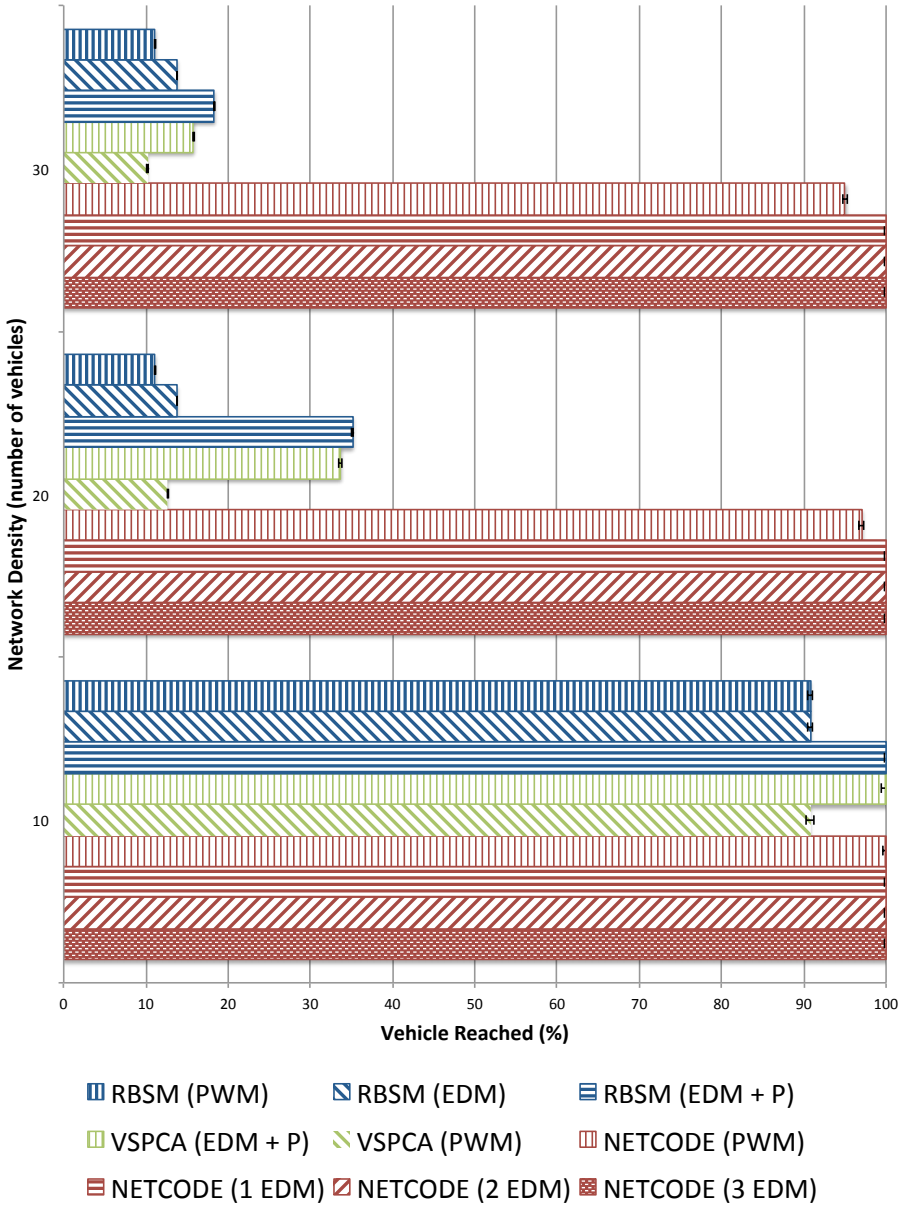



Figure 8.5: Percentage of vehicle reached by EDM and PWM on the free-flow road at 30 mph velocity (single carriageway) with moderate data traffic load.

network densities (10, 20 and 30 vehicles) are used in this study with a view to investigate the effectiveness of EDM dissemination by various warning systems in preventing collisions. Vehicles generally proceed at a steady velocity following other vehicles in front in this kind of scenario. A combination of driver discipline and control are essential to avoid incidents such as abrupt braking or follow-up collision that might potentially lead to pile-up collisions afterwards (see Section 3.3.2). Warning systems, however, try to reduce the possibility of such collisions with the help of technologies described in Section 3.1 of Chapter 3 instead of solely relying on human skills. The EDMs are key tool to accomplish this goal but needs to be delivered to the appropriate vehicles on time. This is evaluated by the current study using a combination of warning systems and their variants.

The study uses two data traffic load of PWMs with one providing 5 warning/sec whilst another releases 15 warning/sec in to the network. These two traffic loads, the former being moderate and the latter being heavy on to the network, give us the opportunity to observe the effectiveness of EDMs on the free-flow road from diverse perspectives. An average of 20 trials of each warning system is used to compute the metrics and prepare the graphs.

### 8.6.1 Data Traffic Load: *Moderate*

Figure 8.4 and 8.5 show that the performance of VSPCA and RBSM with regard to reaching expected vehicles is degraded sharply with the increase of network density in motorway (highway layout) and single carriageway (urban layout) scenarios respectively. It is due to the fact that increasing network density creates excessive contentions and collisions in the network that virtually isolates vehicles communicating with each other by introducing lengthy queuing delays longer than MTQD. It is also evident from the figures when network density is low (10 vehicles in this case), all warning systems demonstrate almost indistinguishable performance. Nevertheless, as network density increases NETCODE outperforms RBSM and VSPCA by a large margin. With 30 vehicles network density, when RBSM and VSPCA struggle to reach 15% expected vehicles in motorway scenario and below 20% in single carriageway scenario, NETCODE reaches more than 95% with a single EDM in motorway and take this performance to 100% when uses multiple EDMs in both scenarios. It is notable from the results observed here that warning systems perform slightly better in urban layout compared to highway. This is due to the reduced velocity of vehicles that gives warning systems a more effective window to deliver warning messages despite having similar queuing delays at the network layer. Besides, in order to complementing the results, PWMs are also observed in the evaluation to show how warning systems would have performed if there is no EDM and the simple application used in this thesis needs to identify the presence of a stalled vehicle in front. Results show that PWMs are always less effective compare to EDMs in identifying events like emergency stop or abrupt braking in the middle of a busy road.

It is important to realise from this study that priority-based VSPCA and the modified RBSM with priority-based delivery performs relatively better in 20 vehicle network density where both systems reach slightly more than 30% expected vehicles in motorway and 35% in single carriageway scenarios. In the least densely populated network, these two systems also match the performance of NETCODE by reaching 100% of expected vehicles. This clearly shows the strength of priority-based warning delivery and backs the claim made in the thesis statement that such an approach can potentially improve the performance.

### 8.6.2 Data Traffic Load: *Heavy*

The observation made in this section reveals that unlike the moderate counterpart, with heavy data traffic load warning systems, particularly NETCODE, in both motorway and single carriageway scenarios perform almost identically. Figure 8.6 and 8.7 show the performance of observed warning systems and identify that with a heavy data traffic load the performance of VSPCA and RBSM are nominally affected at 30 vehicle network density compared to the moderate counterpart of this study. This is unsurprising due to the fact that these two warning systems already suffered from long queuing delay larger than the *MTQD* even if the data traffic load is 5 warning/sec. When this load is increased to 15 warning/sec, naturally the isolation between vehicles continues and thus the performance remains same.

However, the most notable point in these results is the performance of NETCODE that is also affected by this excessive traffic load. At network density 10 and 20 in both motorway and single carriageway scenarios, NETCODE variants fail to achieve 100% performance and at 30 network density only reaches around 85% of the expected vehicles by sending a single EDM. This performance is improved to more than 90% by introducing multiple EDMs. This finding confirms the claim made in Section 8.2 that a small number of repeated messages can potentially improve performance. This study also shows that PWMs come short in reaching vehicles even with NETCODE. It is particularly notable at 30 vehicles network density in both motorway and single carriageway scenarios, NETCODE reaches only 70% of the total expected vehicles using PWMs; and RBSM and VSPCA stay within 10% of their performance level.

Overall, this observation once again confirms that the priority-based dissemination works better in delivering EDMs. In addition to NETCODE, RBSM with priority-based delivery and VSPCA, an inherently priority-based system, perform better than other variants and back the argument made in the thesis statement in regard to priority-based delivery further.

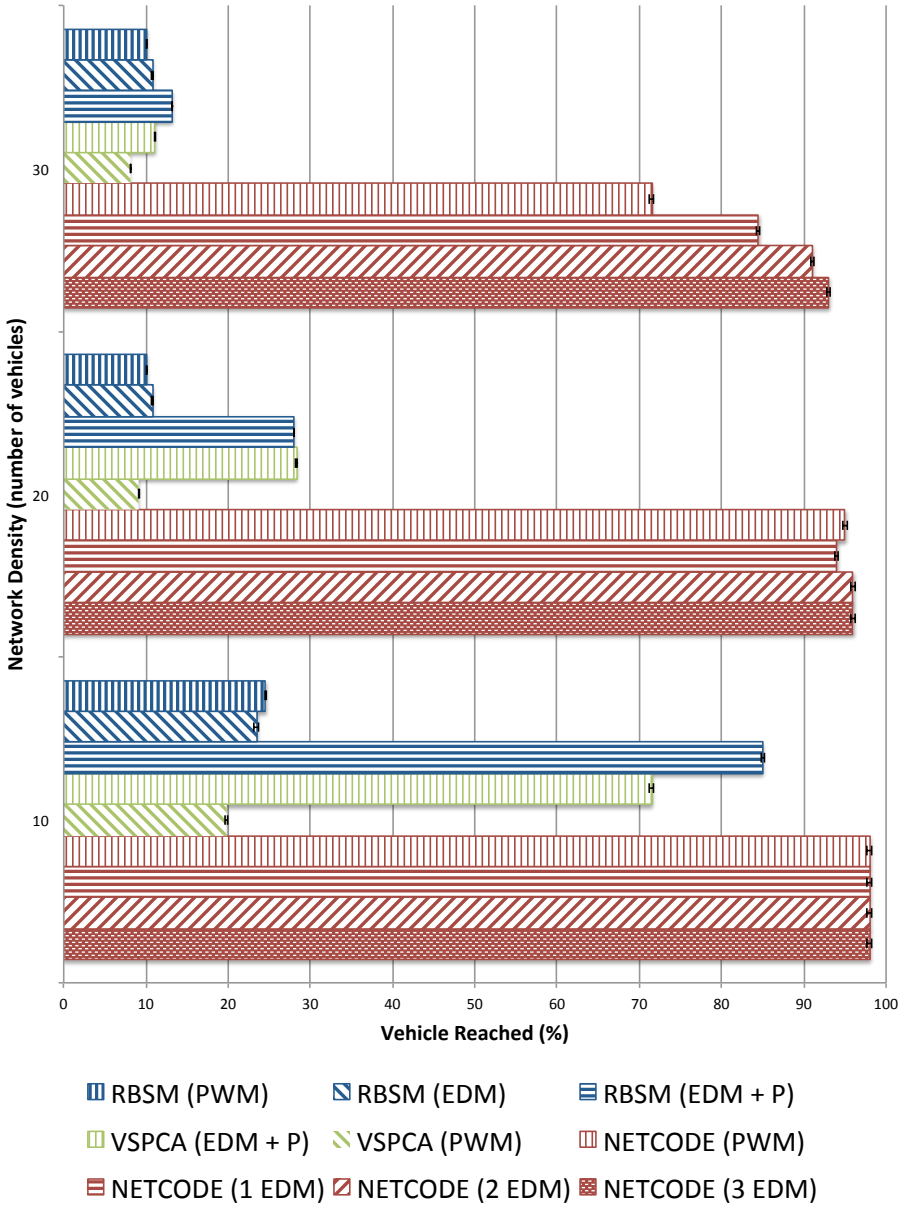



Figure 8.6: Percentage of vehicle reached by EDM and PWM on the free-flow road at 70 mph velocity (motorway) with heavy data traffic load.

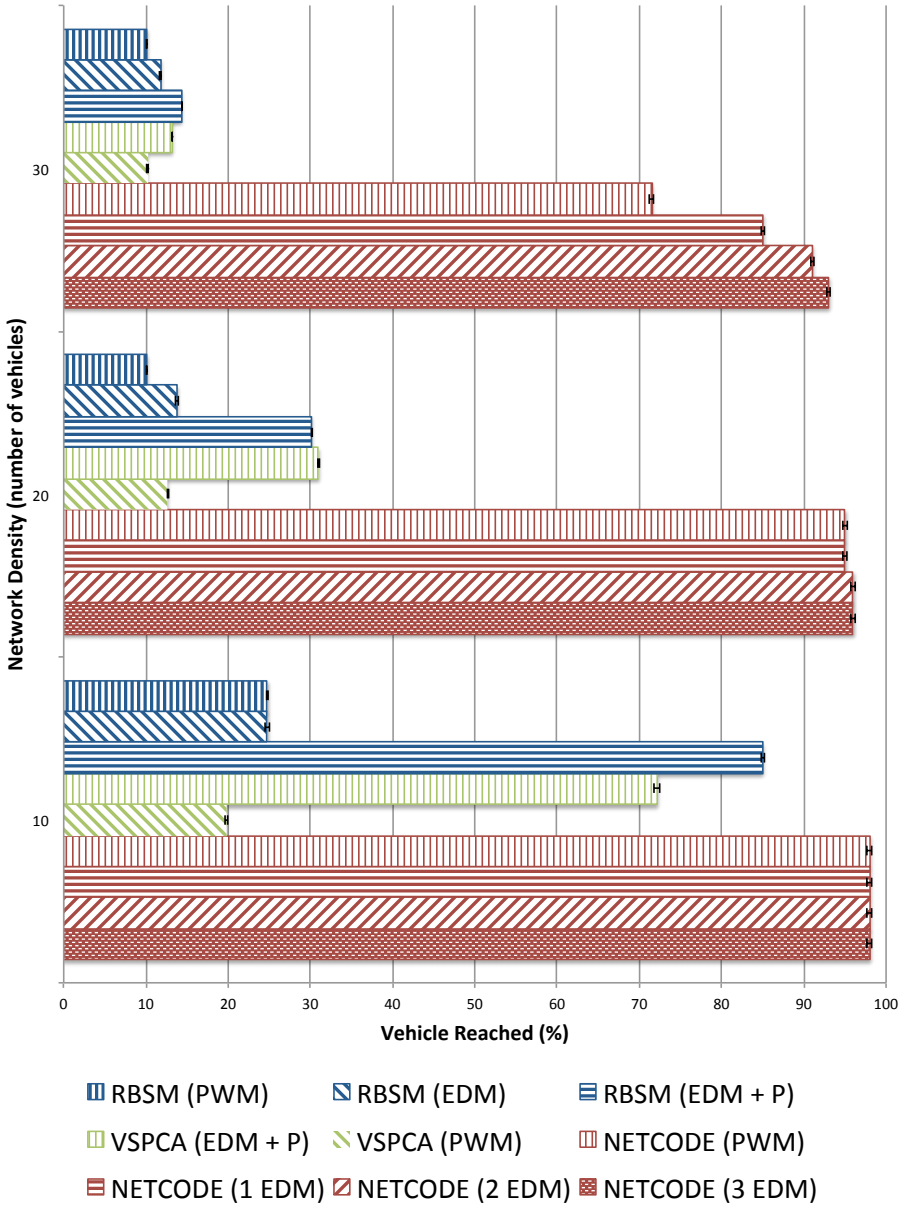



Figure 8.7: Percentage of vehicle reached by EDM and PWM on the free-flow road at 30 mph velocity (single carriageway) with heavy data traffic load.

## 8.7 The Study of EDM at the Roundabout

The study of the roundabout is expressed by varying the network density against the percentage of vehicles reached while keeping other parameters fixed. The network density is varied as 10, 20 and 30 vehicles whilst 5 warning/sec and 15 warning/sec data traffic load is considered moderate and heavy respectively, all as before. Finally, 20 trials are taken and averaged for each warning system to prepare the graphs.

### 8.7.1 Data Traffic Load: *Moderate*

Due to the fact that vehicles approach on a roundabout from multiple entrances, this scenario is more complicated compared to the free-flow roads. In event of an emergency stop on a roundabout, it is not always easy to warn all vehicles who are in a potential threat zone. On a free-flow road it is generally sufficient to inform the vehicles who are following the stopping vehicle from behind. However, on a roundabout, the situation is different as it is necessary to warn vehicles located at the back, on the left side as well as in front of the stopping vehicle. Because of the more complex positioning of the affected vehicle, warning systems often fail to deliver message to parties who are in need of it.

Figure 8.8 and 8.9 show that the performance of VSPCA and RBSM with regard to reaching expected vehicles is very poor at network densities of 20 and 30 vehicles in both highway (roundabout on motorway) and urban (roundabout on single carriageway) layouts. This performance, however, is not the most notable feature of this observation. If we compare this performance with what we observed earlier on the free-flow road in figure 8.4 and 8.5, we find that it does not deviate too much. Instead, it is NETCODE that demonstrates an interesting performance by coming short in reaching expected vehicles with PWMs compared to previous study. While using PWMs, in both highway and urban layouts at 20 and 30 vehicle network density NETCODE reaches less than 80 and 70 percent expected vehicles respectively. This performance is more than 15% short of what same system achieved on free-flow roads. This indicates that periodic warning messages are not sufficiently effective to inform potentially affected vehicles about an incident if it takes place at a location where vehicles approach the scene from multiple directions.

The proposed warning system, however, makes up for its shortcomings with PWMs by achieving excellent performance using EDMs. The results show that priority-based EDM dissemination helps NETCODE reach nearly 100% expected vehicles. It is also notable that despite having priority-based dissemination approach enabled, VSPCA and RBSM variant could not come close to NETCODE?s performance. This behaviour can be explained with the knowledge of our previously observed results in Chapter 6 and 7 where it was shown that queuing delay larger than *MTQD* isolates vehicles from each other by preventing them from

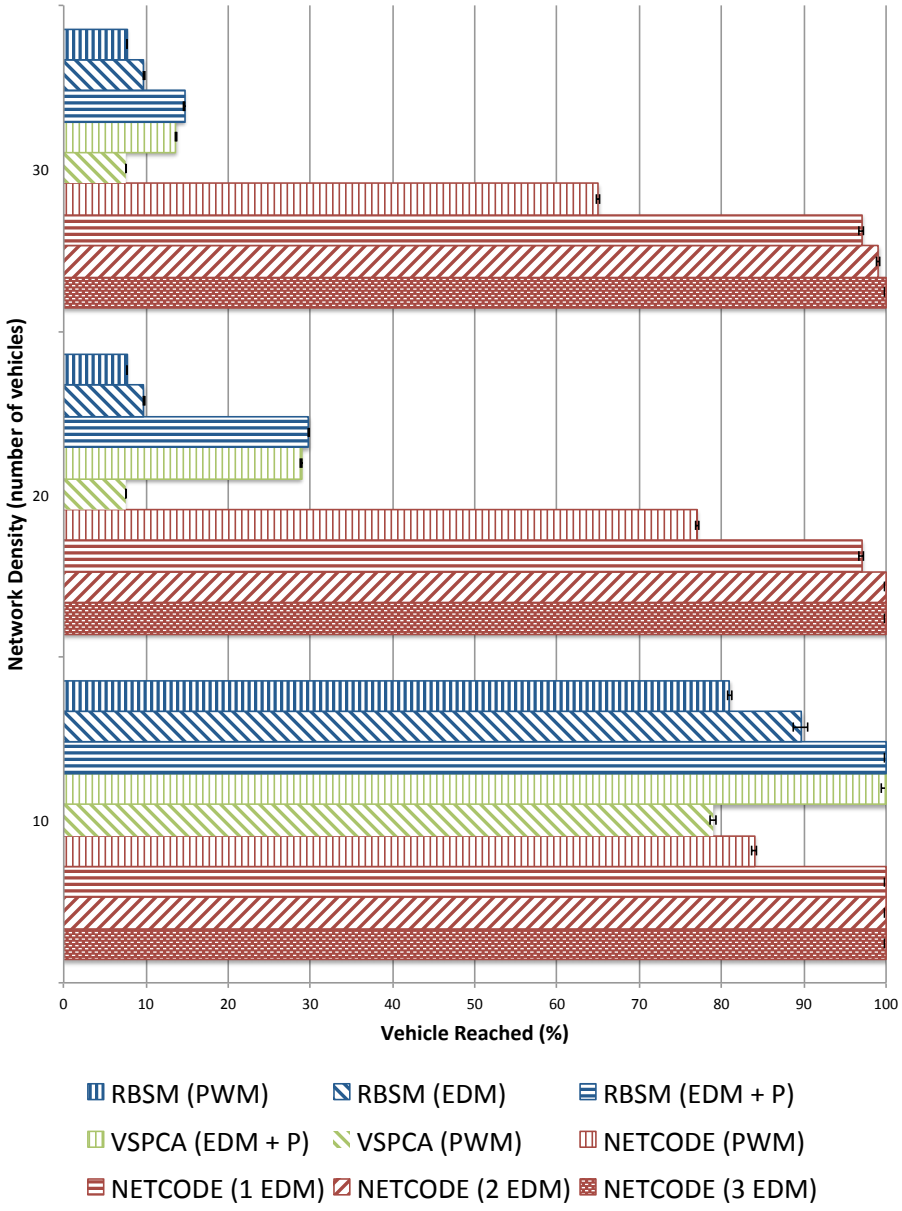



Figure 8.8: Percentage of vehicles reached by EDM and PWM at the roundabout at 70 mph velocity (motorway) with moderate data traffic load.

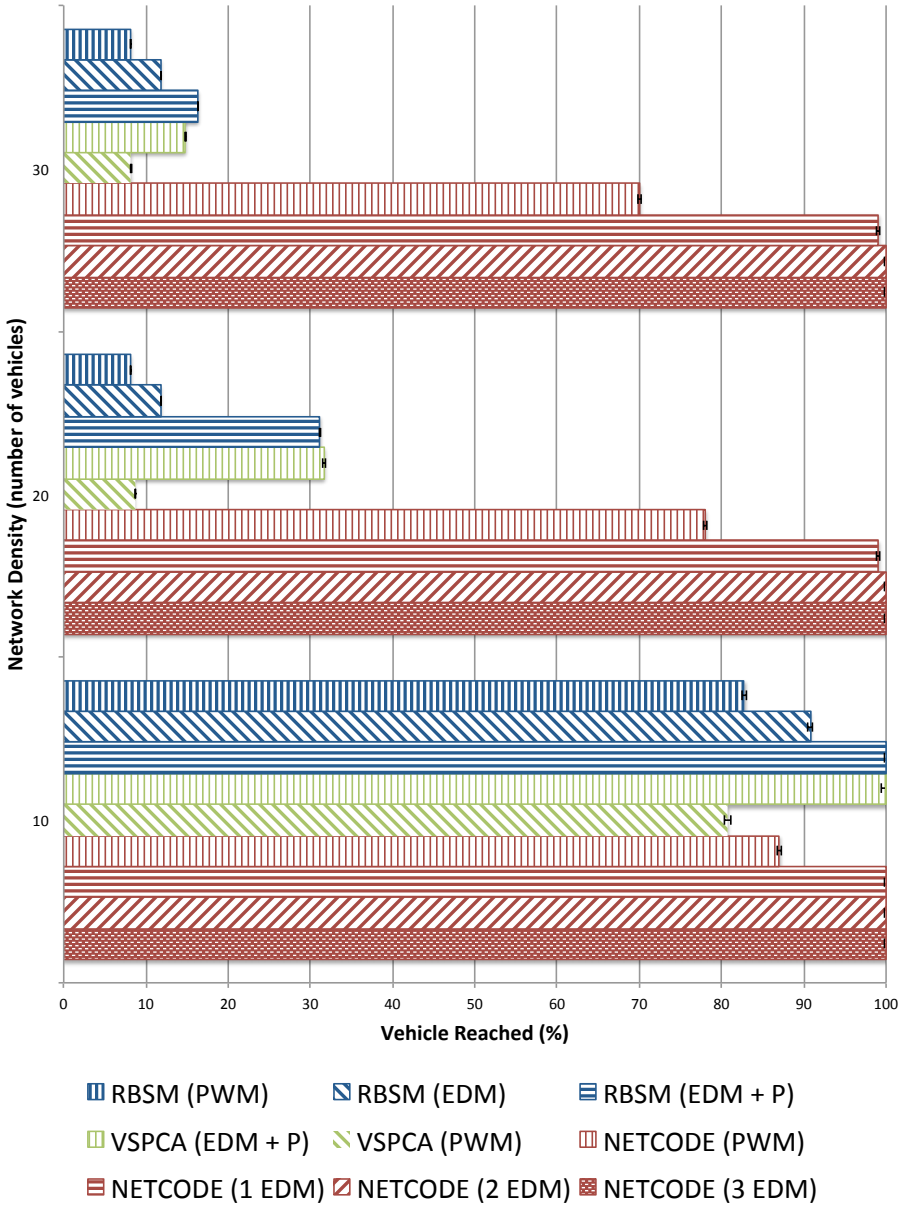



Figure 8.9: Percentage of vehicles reached by EDM and PWM at the roundabout at 30 mph velocity (single carriageway) with moderate data traffic load.

sending warnings. In such situation, EDMs cannot propagate even if they bypass all periodic warnings.

### 8.7.2 Data Traffic Load: *Heavy*

The study of the roundabout under heavy data traffic load puts all evaluated warning systems in the most challenging and harsh environment tested in this thesis. It is already shown earlier that roundabouts are complicated to deal with and in presence of a data traffic load of 15 warning/sec competition becomes quite extreme even at low network density.

Figure 8.10 and 8.11 show that all evaluated warning systems suffer reduced performance particularly at network densities of 20 to 30 vehicles. In the most dense motorway scenario, all versions of RBSM and VSPCA fall below 10% success in regard to reaching expected vehicles. At mid network density, the priority-based versions of these two warning systems achieve about 25% success. These systems perform slightly better in the urban single carriageway scenario but the additional coverage is not very significant.

NETCODE also faces the most difficult challenge in this study. Its PWMs are successful in reaching only 70% expected vehicles when the network density is 10 vehicles on the motorway. It, however, performs slightly better in urban single carriageway scenario. This performance gets further reduced to below 60% on the motorway and around 65% on the single carriageway when the network density is 30 vehicles. Unlike the previous evaluation, the use of EDMs by NETCODE cannot enhance the performance enough. A single EDM comes just short of covering 85% expected vehicles in the highest network density on both motorway and urban single carriageway whilst NETCODE fails to reach 100% expected vehicles in any network density even using three EDMs.

## 8.8 Summary of the Studies

The studies presented in this chapter fulfils the sixth research objective set in Chapter 1 of this thesis. As EDMs represent actual existing events as opposed to PWMs which are generated periodically and allowed to propagate even if there is no real threat, these studies find that priority-based warning dissemination improves the performance of the EDM dissemination; thus scrutinise this proposition by comparing performance of warning systems with and without priority. The outcome of these evaluations show that the time-sensitive EDMs can be delivered effectively if they are allowed to bypass the delivery queue that is mostly occupied by the PWMs.

These studies analyse the performance of the EDM dissemination with a variety of warning systems and confirm that in event of desperate need when PWMs fail to detect potential

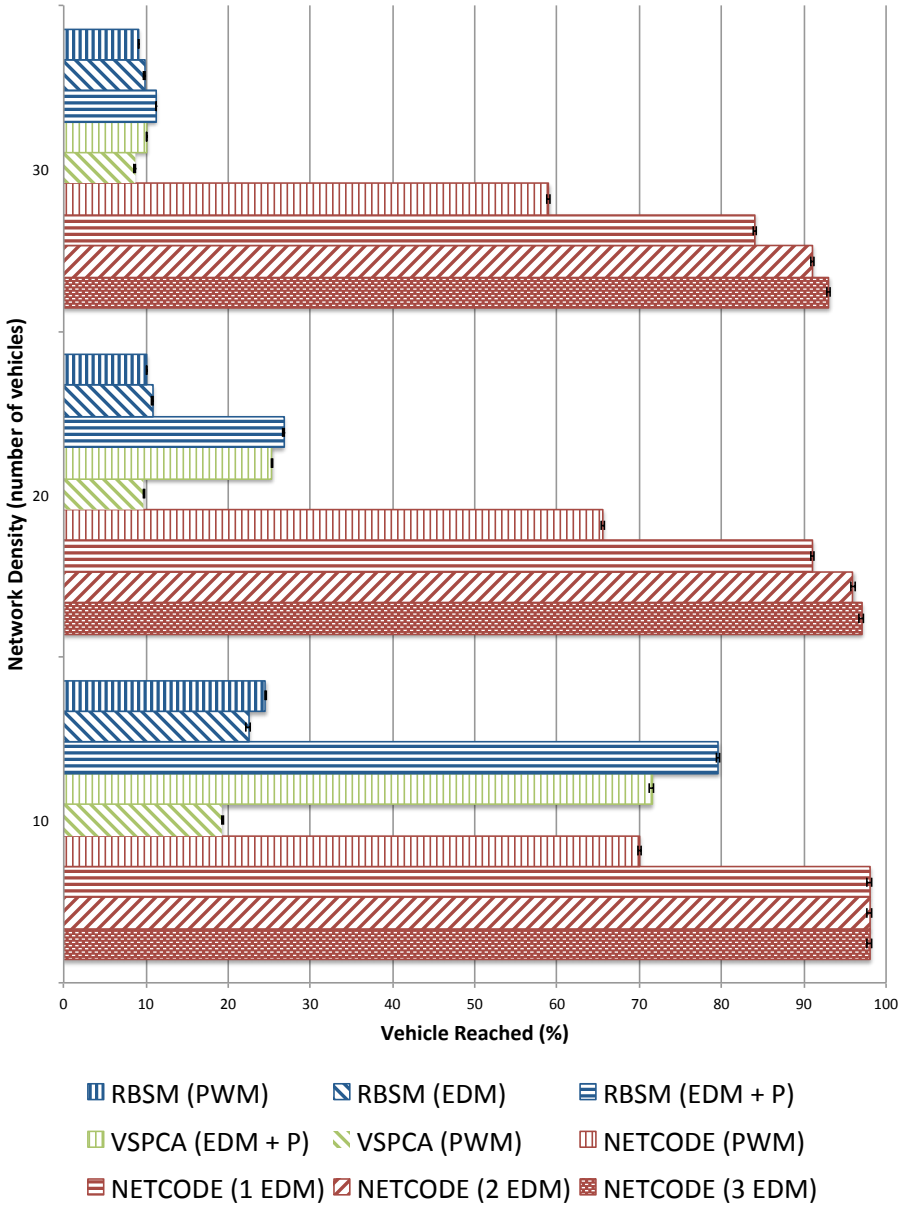



Figure 8.10: Percentage of vehicles reached by EDM and PWM at the roundabout at 70 mph velocity (motorway) with heavy data traffic load.

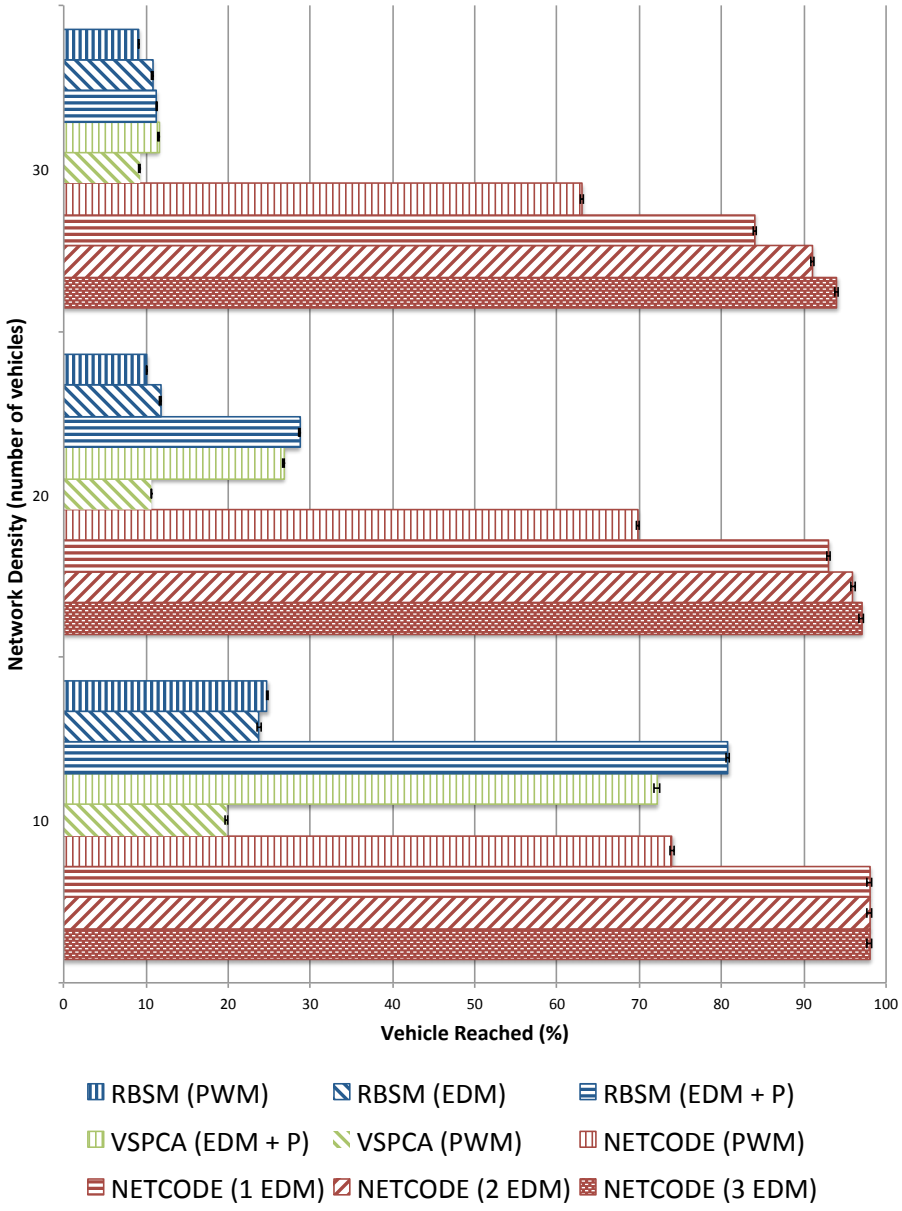



Figure 8.11: Percentage of vehicles reached by EDM and PWM at the roundabout at 30 mph velocity (single carriageway) with heavy data traffic load.

accidents, the proposed scheme with its priority-based EDM dissemination technique successfully reaches almost all expected vehicles when broadcast-based scheme struggle to cope with the growing network density and data traffic load.

The prospect of sending multiple EDMs for the same event is also evaluated in the studies presented in this chapter that confirm the enhancement of the dissemination performance further. The studies indicate that if multiple EDMs are sent in response to an incident, the reachability of NETCODE stays more than 95% even in the scenarios under stress caused by increasing numbers of vehicles and data traffic load.

## 8.9 Summary

This chapter analyses the performance of EDM dissemination by several accident warning systems. It backs the claim made in the thesis statement that priority-based warning dissemination can be effective, particularly in regard to EDMs. It also introduces the idea of using multiple EDMs in response to an event. Two studies are undertaken, one on a free-flow road and another at a roundabouts, to demonstrate that NETCODE disseminates EDMs more quickly and efficiently to the appropriate vehicles than the other warning systems. It also scrutinises the behaviour of PWM and EDM together and concludes that that the use of EDMs cannot be replaced by PWMs so that both types of warning are required to build a successful system.

# Chapter 9

# Conclusions and Future Work

This thesis addressed the problem of sending warning messages in a timely manner. In doing so, it has presented a data dissemination scheme built on a network coding principle, proposing a pair of encoding and decoding algorithms that forms the basis of a warning system capable of detecting potential accidents even in extreme circumstances when network density or data traffic load is so high that current broadcast schemes fail. The studies conducted in course of this research use simulation based approach for measuring performance of the proposed and the existing warning systems; but employ scenarios in a custom-built simulator designed to model realistic situations. The evaluations presented here have shown that the proposed scheme is fast enough to make timely delivery of the warning messages with a view to detecting potential accidents before those take place.

The evaluation presented in this thesis indicates that reduction in the number of transmissions helps reduce competition in the network significantly and allows vehicles to deliver warning messages more rapidly to their neighbours. It also demonstrates that knowledge of two-hop neighbourhood assists decoding coded message quickly without having to wait for further message to arrive. A number of evaluations also examine the relative performance of the proposed scheme when handling both PWMs and EDMs in diverse scenarios under stress caused by increasing numbers of vehicles and transmissions per vehicle. It finally concludes by confirming the thesis' primary contention that network coding helps reducing transmission queuing delay; thus pave the path for timely delivery of warning message, and the proposed scheme substantially outperformed existing schemes in detecting potential accidents.

The rest of the chapter is structured into three sections as follows: Section 9.1 reiterates the thesis statement and explains how it has been addressed in each chapter, Section 9.2 refers back to the problem and indicates how it has been addressed by showing the contributions, Section 9.3 discusses the potential routes this research can be advanced further and finally Section 9.4 concludes this thesis.

## 9.1 Thesis Statement

This section repeats the thesis statement from Section 1.1 and indicates how it has been addressed, with reference to the preceding chapters. The thesis statement is restated as follows:

The broadcast-based data dissemination in accident warning system is not suitable because this approach extends the warning delivery process as data traffic load or network density increases. It is shown in the earlier part of this thesis how broadcasting affects such systems by scrutinising the effect of network density and data traffic load on the network in the context of warning systems. Several performance evaluation studies argued that this problem can be solved with the help of full knowledge of the network or by reducing the traffic load. However, neither of these techniques are useful for accident warning system. The reason being, this cooperative system operates with the help of local knowledge and a regular flow of warning messages is necessary to keep neighbouring vehicles informed about the presence of the host vehicle and subsequently any potential incident that it might cause or be involved in.

Nevertheless, it is argued in this thesis that to overcome these limitations of the existing data dissemination schemes and make timely delivery of the warning message, network coding can play an important role. Therefore, this thesis asserts that:

**T1** The XOR-based network coding provides a potential solution on which a data dissemination scheme can be built, a solution that helps reduce the warning delivery time without restricting the regular flow of warning messages. This can be achieved by optimising the number of transmissions in the network. Being cooperative in nature, accident warning systems regularly disseminate warning messages that produce a warnings flow on the road. Intermediate vehicles in multi-hop VANET send these warnings to vehicles ahead or behind. While performing this operation, vehicles potentially can optimise the number of transmission by encoding a message coming from the behind with a message that arrived from the front and sending them together in one transmission.

**T2** Information about the two-hop neighbourhood can play a pivotal role in designing an encoding algorithm that picks packets in such an order so that receivers can decode them without requiring to wait for long. If a vehicle gets to know who are the neighbours of its neighbours, it can easily identify those who are not connected directly, a finding that potentially helps the vehicle portioning the network into two subsets, one in front and another at the rear. Members of those subsets are aware of the transmissions made within their subset but unaware of any transmission in the other subset. Being the linking node of those two subsets, when a vehicle encodes packets taking one from each, receiver vehicles easily decode it using the packet available at their disposal.

**T3** The performance of the warning delivery can be improved further in regard to event-driven messages if a priority queue is maintained at the network layer of each vehicle. This queue would authorise any event-driven message to bypass the periodic messages in the packet queue for expedited delivery.

To improve the performance of the accident warning system in context of making timely delivery, the claims made in the above thesis statement are achieved systematically through six objectives set in Section 1.2. The following part of this section describes how it has been achieved.

Chapter 3 addresses the RO1, i.e. the objective of identifying and gathering the requirements for an empirical warning system. It suggests a blue-print of a model warning system through a requirements survey and a methodical review of the existing warning systems. The studies conducted to achieve this objective identify that broadcast has been the most popular and effective data dissemination scheme employed for building warning systems in past. It, however, suspects some drawbacks that this scheme could possibly demonstrate and recommended a further investigation to know the extent of this problem up front.

Chapter 4 anatomises the existing warning systems operate with broadcast-based data dissemination schemes with a view to find the shortcomings (RO2). Three warning systems from three broad categories of broadcasts are picked to scrutinise their performances in this chapter. The studies conducted to achieve this objective find that although broadcast seems to be the most straightforward scheme for warning systems, existing approaches cannot handle excessive transmissions and often exhibit long transmission queuing delay while going through broad- cast storms. This behaviour leads to the collapse of the system for a considerable time.

Having identified the shortcomings of the broadcast based data dissemination schemes in course of achieving the previous objective, the RO3 has been accomplished in Chapter 5 that proposes, NETCODE, a new data dissemination scheme seeks to improve the performance of the accident warning systems in VANET. In doing so, network coding technique is employed to build a warning system. It presents a pair of encoding and decoding algorithms that work jointly towards achieving the goal of delivering warning messages in a timely manner. The development of NETCODE forms the basis of three evaluations conducted next in this thesis.

Chapter 6 addresses the RO4, i.e. the objective of evaluating the performance of the new scheme concerning transmissions related metrics. It finds that reduction in the number of transmissions using network coding helps reducing competitions in the network by minimising the number of collisions. This less competitive environment in return allows vehicles to quickly deliver warning messages to their neighbours (T1). It is anticipated at this stage that this improvement in delivery time can potentially impact in successful detection of potential accidents in real-life scenarios.

The RO5 has been accomplished in Chapter 7 that partially confirms the above anticipation by analysing the performance of the proposed scheme concerning periodic warning message as to how effectively they keep neighbouring vehicles informed about the presence of the host vehicle and how this information is materialised to detect potential accidents. It also shows that knowledge of one-hop neighbourhood assists decoding encoded message quickly without having to wait for further message to arrive (T2). The outcomes of this chapter find that network coding ultimately helps reducing transmission queuing delay; thus pave the path for timely delivery of warning message, and the proposed scheme substantially outperforms existing schemes in detecting potential accidents (T1). Therefore, this thesis moves one step closer to fulfilling the thesis statement.

Finally, Chapter 8 aims to achieve the RO6, i.e. the objective of analysing the performance of the EDM dissemination by the proposed scheme alongside period warnings. It establishes the claim made in the thesis statement that priority-based warning dissemination can be effective, particularly in regard to EDMs. The studies in this chapter find that when other broadcast-based systems fail to effectively distribute warning messages to prevent potential accidents, NETCODE achieves an outstanding success in surpassing their performances (T1). Besides, in event of desperate need when periodic message fails to detect potential accidents, the proposed scheme with its priority-based event-driven warning dissemination technique successfully detects almost all potential accidents (T3).

Having these objectives accomplished, this thesis concludes with the notion that XOR-based network coding is indeed a potential solution on which a data dissemination scheme can be built and the pair of encoding and decoding algorithm presented in Chapter 5 forms an accident warning systems better than available existing systems in the scenarios considered within the scope of this thesis.

## 9.2 Contributions

This thesis aims to solve the problem of delivering warning messages to neighbouring vehicles in a timely manner. In doing so, it has focused on the development and analysis of a warning system specifically designed to alleviate the problems stated above. In course of achieving this goal, the following contributions are made in this thesis:

1. **A Pair of Encoding and Decoding Algorithm:** This thesis presents an XOR-based data dissemination scheme and the heart of this scheme is a pair of encoding and decoding algorithm described in Chapter 5. These algorithms are the prime contribution of this thesis. They are based on an original idea developed in course of this research that if two-hop neighbourhood information is used to create a partition amongst commuting vehicles and subsequently encode two warnings amongst the respective sides,

the decoding process can be performed without having to wait for further warning arrival. This pair of algorithm uses this concept to divide participating vehicles into two sets and provides a way of employing network coding techniques to expedite data dissemination in a time sensitive system.

2. **NETwork COded DissEmination (NETCODE):** NETCODE can be seen as a standalone data dissemination scheme as well as a warning system that is comprised of both application and network layers. The conception of the system follows a methodical examination of requirements and a survey of existing systems. The design is capable of successfully disseminating periodic warning message at a relatively high rate and also of using priority-based event-driven messages in critical situations.

3. **An Evaluation Study of the 3 categories of Broadcast Schemes:** This thesis presents a performance analysis of three of systems representing three broad categories of broadcast namely limited-scope, flooding and single-hop. Their behaviour is analysed to understand the effect of broadcast storm on performance. In doing so, a more detailed simulation environment is used along with a city mobility model and a flow of vehicles that approximates that of a real city.

4. **A Comprehensive Requirements Survey:** VANET-based AWS design is a relatively new research area. As this new domain emerges, researchers from around the world propose contemporary ideas for building modern warning systems. In order to do so, it is needful to ascertain the system requirements, information to be exchanged, and protocols required for communication between vehicles. This thesis – with an aim to understand the requirements for building the system – conducts a survey on the requirements along with a review of existing proposals

## 9.3 Future Studies

This thesis leaves various open problems requiring further work. This section describes some potential future directions suggested by the work accomplished in this thesis.

**Security, Privacy & Trust**

The design and development of warning systems is a relatively new area having huge research opportunities to contribute in security, privacy and trust issues. Although the problem of designing efficient and effective warning systems has been widely studied, making such systems secure from potential threats has yet to be seriously addressed. Furthermore, the special nature of AWSs makes it necessary to develop a specific threat

model by anticipating potential adversaries, their motivations and likely modes of attack. The work accomplished in this thesis can be further extended to this direction. Appendix A provides more insights into this topic.

**Third & Fourth Degree Encoding**

The encoding algorithm presented in this thesis partitions the neighbours of the host vehicles into two subsets and applies XOR operation to the warnings taken from each side. This concept is motivated by the fact that roads are mostly straight and a host vehicle can slice them into two halves – front and rear. This method allows NETCODE sending two warnings in one transmission. This algorithm has the potential to include more warnings inside its coded packet by extending the degree of the coding operation. The proposed scheme can be extended particularly for junctions and roundabouts to handle more warnings in one transmission.

**Application Development**

The design of AWSs mostly involves network and link layer research, but this can be extended to application layer by providing added support to the underlying layers. For example, this thesis uses a simple application layer that generates PWMs and EDMs as per predefined configuration. This application can be modified to provide with supplementary support such as generating EDMs when a vehicle approach junctions or roundabouts, sending EDMs with special code informing following vehicles about road conditions and so on. Such uses of the application layer can potentially further enhance the performance of the warning system.

## 9.4 Summary and Conclusions

This thesis has addressed the problem of sending warning messages in a timely manner. In doing so, a network coding technique is employed in this thesis. The proposed NETwork COded DissEmination (NETCODE) is a VANET-based AWS responsible for generating and sending warnings to the vehicles on the road. The NETCODE offers an XOR-based data dissemination scheme that sends multiple warning in a single transmission and therefore, reduces the total number of transmissions required to send the same number of warnings that broadcast schemes send.

The evaluation presented in this thesis indicated that reduction in the number of transmissions helps reduce competition in the network significantly and this allows vehicles to deliver warning messages more rapidly to their neighbours. This thesis also examines the relative performance of NETCODE when handling both PWMs and EDMs in diverse scenarios under stress caused by increasing numbers of vehicles and transmissions per vehicle. This work

confirms the primary contention of the thesis that XOR-based network coding provides a potential solution on which a more efficient AWS data dissemination scheme can be built to reduce the delivery time without having to restrict the regular flow of warning messages.

# Appendices

# Appendix A

# Threats in Accident Warning Systems

It has been mentioned earlier in this thesis that Accident Warning Systems (AWSs) are developed for next generation vehicles and it is aimed to make the use of Vehicular Ad-hoc Networks (VANETs) to avoid potential collisions and spread safety notifications amongst nearby vehicles [58]. The problem of designing efficient and effective warning systems has been widely studied but making such systems secure from potential threats has yet to be seriously addressed.

Although security is seen as one of the important issues in general networking, it has largely been overlooked in the area of warning systems developed for vehicles. There is sometimes an implicit assumption that a separate security system designed for generic wireless networks can be added to an AWS [124]; however, such an approach is unlikely to be adequate because of the unique nature of both the safety system itself and the potential threats. For example, unlike most VANET applications that often handle confidential and sensitive data, warning systems are not generally concerned about data confidentiality. These systems willingly share data with other nodes so that they can operate cooperatively to prevent motor accidents. The special nature of AWSs makes it necessary to develop a specific threat model by anticipating potential adversaries, their motivations and likely modes of attack.

This appendix aims to describe and develop a threat model through an in-depth analysis of security, trust and privacy issues in AWSs and opens up future directions to contribute in this area. The offerings of this appendix are presented in a twofold aspect: firstly, it presents a survey of possible adversaries and potential attacks on AWSs; and, secondly, it develops a threat model by ranking adversaries based on the level of potential damage associated with their likely types of intrusion.

The remainder of the appendix is structured as follows: Section 2 presents an overview of the system; Sections 3 and 4 discuss adversaries and attacks respectively; Section 5 outlines potential challenges; and Section 6 presents the threat model before finally Section 7 concludes this appendix with a summary.

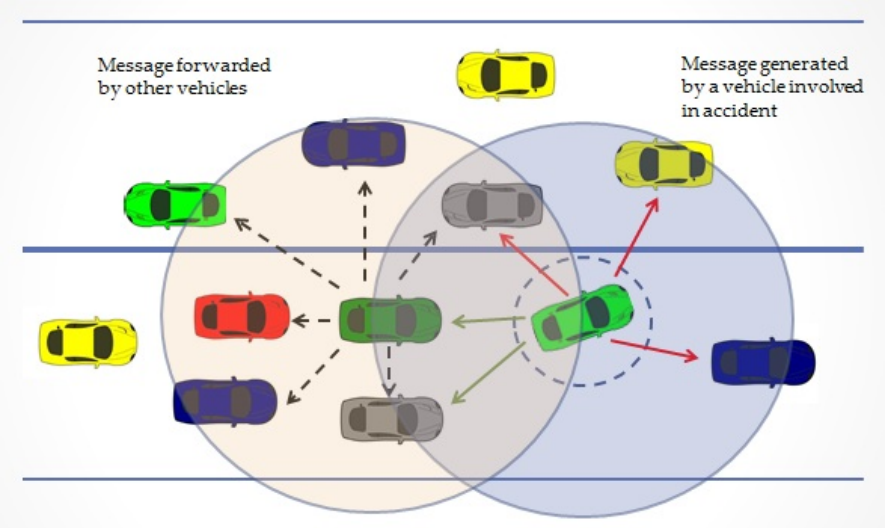



Figure A.1: The operation of an AWS in brief.

## A.1 Overview of the System

The design process of a threat model requires a preliminary requirement analysis and component level description of the system. Such a study is presented in Chapter 3 and in the publication [125]. The main conclusions of those studies are briefly summarised below.

**System Architecture and Requirements:** AWSs are collections of mobile nodes, each corresponding to a physical vehicle, whose purpose is to generate collision avoidance notifications that warn drivers before a potential accident takes place. These systems operate via a VANET with which they may be integrated to a greater or lesser degree.

For the purposes of system design, collisions may be classified into several generic types: follow-up, pile-up, intersection, lane-change, forward-collision and collisions with object, human or animal. In order to tackle these various hazards, an AWS will use its associated VANET to send messages to containing information about locations and velocities of vehicles. In order to generate such information, individual vehicles need to be equipped with various devices including GPS or similar receivers, sensors to gather important data such as speed, acceleration and deceleration, presence of other vehicles in close proximity and possibly On Board Units (OBUs) to allow drivers to enter warnings of less time-critical hazards manually.

**Message Pattern:** Information that vehicles exchange is not confidential but rather visible to and accessible by everyone so that it can be used to identify potential hazards to as wide a relevant audience as possible. There are generally four types of AWS message used to disseminate information. These are: Event Driven Message (EDM), Period Warning Message (PWM), Road Condition Notification (RCN) and Emergency call-up (ECU).

EDMs are sent in response to an emergency situation that has arisen suddenly and unexpect-

edly such as an accident, an abruptly stopped vehicle and so on. These messages are the highest priority variants in any AWS and need to reach the targeted audience in the shortest possible time. PWMs are also high priority and require to be disseminated quickly: vehicles send these to warn others about their presence. RCNs inform other vehicles about scenarios such damaged or slippery surfaces, localised weather hazards etc. and are treated as low priority notifications. ECU is used in some AWSs to summon police, ambulance or mechanics after an incident takes place.

**Interactions:** These messages are typically small and open in nature. Senders want every recipient to which information might be relevant to read it and messages are forwarded repeatedly over a specific region. Unfortunately this has the potential to allow attackers to manipulate content and spread false information across the network. By its nature an AWS depends on accurate content and manipulation introduces not only the threat of the system failing to work as intended but even worse, the possibility of it actually causing accidents that would otherwise not have occurred.

## A.2 Adversaries

Potential attackers can be categorised according to the damage they might cause. Following section divides them into three classes and describes how they are likely to operate in AWSs.

### First Degree Threat

This category includes adversaries whose objective primarily involves breaching normal practice for temporary personal driving advantage. The aim is not to cause physical harm to others or direct monetary gain.

**Dishonest Drivers:** These are potential adversaries who inject false information into the network with a view to gaining advantage over other vehicles. For example, one might create the illusion of congestion to encourage other drivers to avoid a route one wishes to use freely.

**Selfish Drivers:** AWSs are cooperative system and every vehicle must comply with this principle. In order to make the system a success, it is assumed that all vehicles will share information and forward it to others, if necessary. It is, however, possible that some drivers may refuse to comply with this norm by disabling the forwarding of warning message either completely or partially. The impact of this behaviour may or may not cause system failure depending on its prevalence in particular area.

**Pranksters:** These are likely to be amateur hackers interfering with the system for amusement and, possibly, notoriety. Attacks could be carried out from the roadside deliberately


Figure A.2: List of adversaries based on their degree of threat.

feeding misleading instructions to vehicles. Most such individuals are intent on inconvenience rather than serious damage but, given the nature of motor vehicles, there is a danger of unintended serious harm.

**On-board Passengers:** Warning systems are often equipped with an OBU that helps drivers entering warning and road condition notification manually. Although the intention is to allow drivers to report potential hazards, where data entry is insecure, it may be possible for passengers to inject false notification into the network either through carelessness or for amusement.

## Second Degree Threat

This category comprises adversaries that deliberately attack the system for monetary benefits but do not intend to cause physical harm. This includes misusing the system to rob others or trying to get personal information with a view to sell it.

**Robbers:** Accident warning systems warn other vehicles about potential collisions. In an unsecured system where vehicles react automatically to such warnings, it would be possible to inject false information to bring a target vehicle to a halt in order to facilitate a robbery.

**Sniffers:** Although the warnings that warning systems disseminate are public and do not contain any personal information, monitoring a target individual's movement, driving pattern and vehicle information without consent, is a privacy violation that could be used against the victim.

**Industrial Competitors:** The MAC address of IEEE 802.11 contains a manufacturer identity field. This could in principle be used by an intruder to defame competitors by falsely associating deliberately engineered problems with their systems.

**Watchers:** This kind of adversaries encompasses everyone from a government secret service operative to a tabloid newspaper journalist to a criminal group attempting to monitor someone's regular movements and activities. The nature of these adversaries is different than sniffers as they explicitly try to defame or watch someone for their monetary or personal gain.

### Third Degree Threat

This category comprises adversaries whose intention is to interfere with an AWS deliberately to cause harm to others.

**Malicious Attackers:** These attackers insert malicious information in the network or jam network channels to block information propagation in the network with a view to creating chaos for a variety of potential reasons such as affecting markets or creating diversions. Such an attack could easily lead to fatal accidents.

**Terrorist/Activists:** This group of adversaries can potentially manipulate data to create fatal accidents on motorways or in crowded city areas.

**Abductors:** An individual or a group who want to abduct someone can take advantage of this system. As drivers inject data regularly in the network, particularly in the form of periodic warning message, it leaves traces on their regular movement path. Abductors can make the use of those traces to predict someone's movement in advance to plot a physical attack in a planned and organised way.

**Crazy Pranksters:** For reasons previously mentioned, people pranking an AWS can cause physical injury or death even if unintentionally. Unfortunately there is reason to believe that some such individuals are capable of crossing the line into generating such outcomes deliberately for nihilistic pleasure.

## A.3 Attacks

In this section, a comprehensive survey is presented of the various types of attack that can be used to target AWSs. Later in this paper connections will be established between these attacks and previously described adversaries to build the threat model.

**Distributed Denial of Service (DDoS) Attack:** DDoS is a type of denial-of-service attack on networks that is triggered by first compromising a number of *slave* or *zombie* devices and

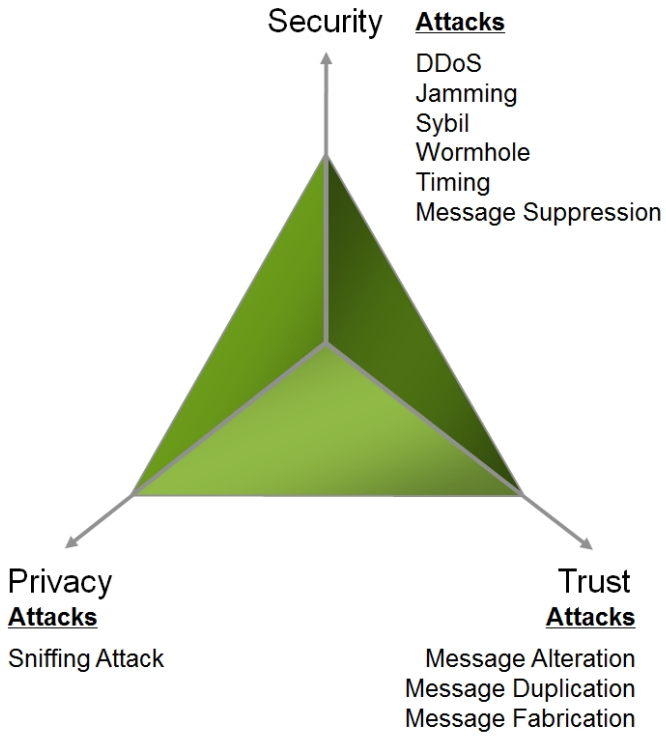



Figure A.3: Possible attacks associated with security, privacy and trust.

later using a trigger command to use their combined transmission power in an orchestrated flooding attack on some selected target [126]. The distributed nature of the attack makes it more difficult for the victim to block. Attacks of this type can make services unavailable during the course of the assault. The DDoS attack is considered one of the most dangerous attacks on networks [127].

**Jamming Attack:** Wireless networks are built upon a shared medium that allows potential adversaries to launch attacks easily. A jamming attack is a denial-of-service attack aimed at disabling this medium. For example an attacker may use a jamming device that emits a powerful RF signal to block a wireless channel so that legitimate users cannot get access [128, 21]. There are several jamming attack models such as constant jammer, deceptive jammer, dom jammer, reactive jammer and so on [129]. In an AWS an attack of this type would make vehicle information unavailable to other nodes. In a scenario where vehicles come to rely on AWSs to trigger automatic avoidance measures, this could easily result in collisions and serious harm.

**Sybil Attack:** This attack mode was first formally defined by [130] as the sending of message from one node with multiple spoofed identities. In a VANET ([131]) this amounts to a vehicle maliciously fabricating different identities to mislead others and generate false information. It is observed and argued that without a centralized authority, this attack is always possible and may go undetected [130, 132].

**Wormhole Attack:** This is an attack on various types of networks and considered one of the most difficult to counter [133]. According to [134], in a wormhole attack, a private tunnel is used to deliver apparently locally-originating packets to a remote destination. In this way a distant node can be made to appear at a location where it does not exist in reality. A wormhole attack can be performed even if the network provides confidentiality and authenticity.

**Sniffing Attack:** The aim here is simply to snoop on a target individual by collecting private information from the network [135]. There are several variants including content sniffing, phishing, location sniffing, identity sniffing etc. It has potential to create great threat on lives and properties should victims privacy is compromised.

**Timing Attack:** This attack particularly targets real-time applications. The attacker interferes with a legitimate message to engineer a deliberate delay [136]. Real-time applications that are time dependent can then be made to fail. This kind of attack is very difficult to detect as the attacker acts like a normal node.

**Message Attacks:** Message attacks are a group of attacks involving message alteration, duplication, fabrication and suppression. These have been identified as threats for VANETs in the literature [137] and target the relaying networks. In alteration, important information is altered during relay but in such a way that it still looks legitimate. In duplication a message is replicated by a relay to gain specific objectives. In fabrication, a message is generated that looks like it has been legitimately relayed rather than sourced by its creator. Finally, in suppression a relay simply discards a message it is supposed to forward allowing an attacker to block information from reaching intended recipients.

## A.4 Potential Challenges

AWS differ from other applications that might be expected to run on top of VANETs. They exhibit open behaviour where data must be visible and information about physical locations needs to be exchanged [29, 59]. Because of this special nature, defending against threats presents some important challenges.

**Cooperative Systems:** By its nature, an AWS is a cooperative distributed system operating locally with no centralised control. The basic conception relies on every node acting in a manner that is honest, helpful and cooperative because each is reliant for its safety on the received data. However, in practice adversaries can prey on a system organised in this way to achieve unethical and illegal benefits. It is easy to trigger attacks by using suitably prepared intruder vehicles to inject false or fabricated data into the network. A potential solution to this problem would be the use of an existing trust system, but that may create tension with a desire to preserve the personal privacy of the drivers.

**Trust vs Privacy:** Trust and privacy always have a somewhat uneasy relationship that becomes especially complicated in AWSs. Nodes depend on received data for important and safety critical decision-making and they need to know that such data is coming from a legitimate source. While a trust mechanism, by endorsing data, would remove many potential threats, in this situation, given the inherent location tracking, it would also compromise privacy and open drivers to snooping and even criminal targeting.

**Non-confidential System:** In an AWS the aim is to disseminate data to all vehicles who might be affected by the content. As a result, the source is not usually aware of the relevant audience and cannot use secure channels. This makes it easier for attackers to alter or fabricate data and disseminate false information that looks legitimate.

**Decentralised Nature:** The openness issue might be addressed if vehicles are provided with certificates issued by a trusted central authority. In this case only messages signed by their sources are to be trusted. However, the biggest challenge to doing this is the decentralised nature of the AWS which may not have access to a backbone network and thence a central server.

On consideration it can be seen that the above challenges are interconnected nature. As decentralised AWSs are cooperative system, they need to verify trust. Verifying trust, however, affects personal privacy that can be compromised because of the openness of the system. Nonetheless, the problem of openness is difficult to address unless the system is turned into a central authority controlled system.

## A.5 The Threat Model

Potential adversaries and possible attacks have already been discussed along with different challenges that AWSs create because of their openness and cooperative behaviour. These considerations provide sufficient context for designing a realistic generic threat model for an AWS. Figure A.4 combines that information with a view to identify relationships between adversaries and attacks; and presents the threat model along with a discussion on possible countermeasure to safeguard the system from those attacks.

The threat model is built in such a way that it divides the adversaries in the first place. This division provides clear understanding on the possible attackers who retain the maximum potential to make the system vulnerable. It also shows who often go undetected without leaving any trace of the system being misused. These adversaries have the potential to trigger attacks targeting security, privacy and trust aspects of the system that has also been shown in the model.

In order to protect AWSs from these attacks, the most suitable way is to look at the at-

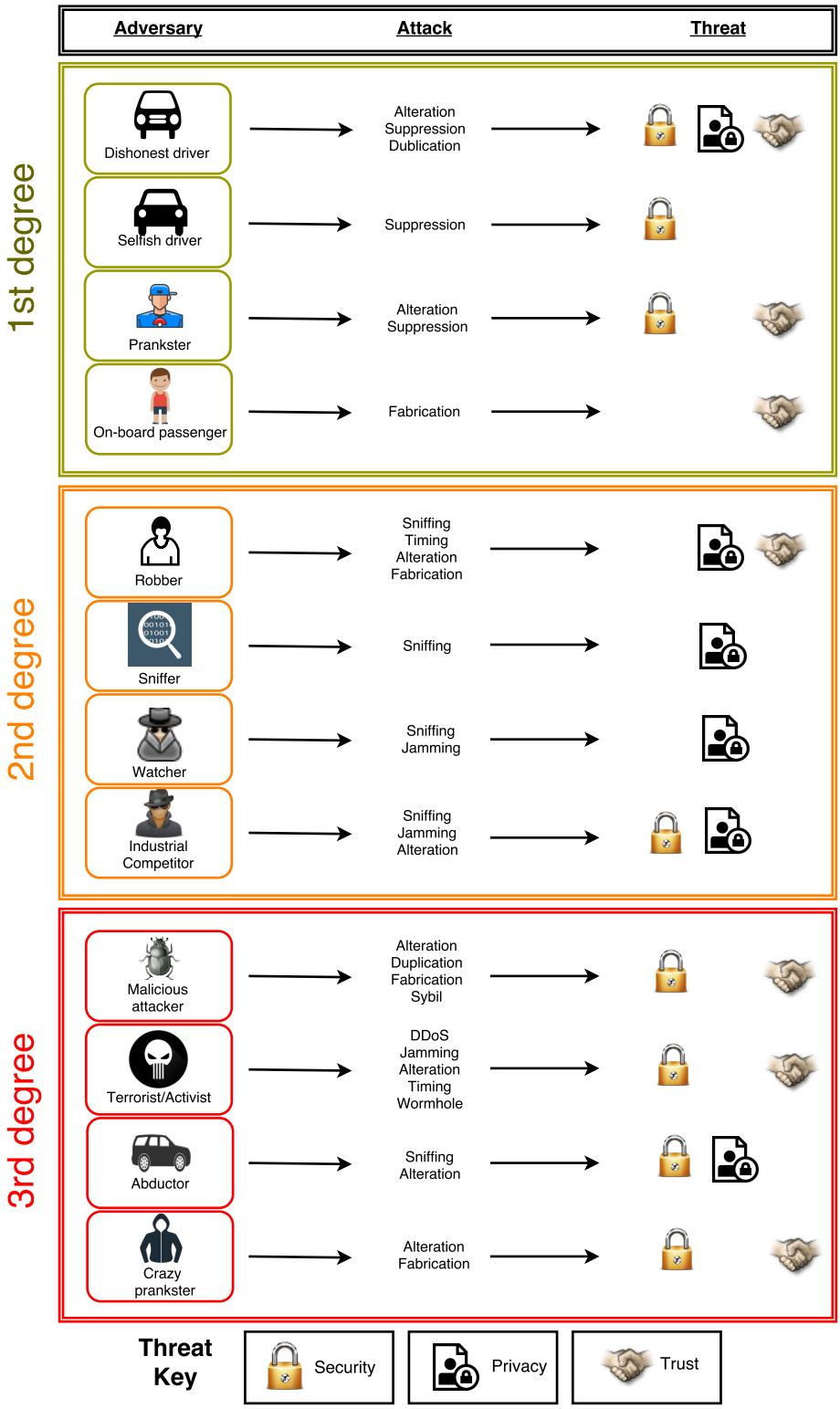



Figure A.4: The *Threat Model* developed as a part of this thesis but not used in its core contribution.

tack from the aspects they are targeting in the system. For example, dishonest-drivers and pranksters would be likely to use data-related attacks because the main objective is to fool people to gain temporary personal benefit or pleasure. Robbers and abductors would try to stop people in the middle of their way by giving false warning whilst terrorist and malicious attackers would create chaos by injecting malicious information. These behaviours indicate that the attacks would possibly make the use of trust issues and therefore, to protect AWSs from such attacks, establishment of trust system acts as a solution [136].

There are a number of approaches that help establishing trust such as key-based [138], reputation-based [139] and so on. These approaches, however, would require identifying the person involved in communication. As ASWs willingly and openly disseminate its location, revealing identify can cause severe threat. A potential solution to this problem would be using privacy-friendly trust system that recently became a prime research topic in trust [140].

A trust system is, however, of little help in combating warning suppression attacks by both dishonest-drivers and selfish-drivers; and sometimes crazy pranksters. Selfish-node detection mechanism of Mobile Ad-hoc Networks can be introduced in VANET to fight against these adversaries [141]. Besides, security enforcement through monitoring vehicle communication behaviour offers partial solution to this problem. Another useful corrective measure that might help combat some threats would be OBUs that give drivers the opportunity to counter information discovered to be false. This might also help protect against long-term message alteration message and to cancel out accidental warnings.

## A.6 Summary

This appendix presents a threat model for warning systems and aims to open up new directions associated with security, privacy and trust issues of the next generation vehicles. The main contribution of this work is the identification of potential adversaries that might make warning systems vulnerable, the categorisation of such adversaries based on their degree of threat and their likely attacks they might mount to achieve their objectives. In future, this model can be used to show right paths in building trust systems and privacy friendly routing in NETCODE or newly developed warning systems. Such solutions will be essential before warning systems can safely be deployed in the field.

# Bibliography

[1] C. Fragouli, J.-Y. L. Boudec, and J. Widmer, "Network coding: an instant primer," *ACM SIGCOMM Computer Communication Review*, vol. 36, no. 1, pp. 63–68, January 2006.

[2] T. Ho and D. Lun, *Network Coding: An Introduction*. Cambridge University Press, April 2008.

[3] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard, and J. Crowcroft, "XORs in the Air: Practical Wireless Network Coding," in *Proceedings of ACM SIGCOMM*, Pisa, Italy, June 2008, pp. 497–510.

[4] BBC, "Britain's scariest roads revealed," The British Broadcasting Corporation, Tech. Rep., November 2009.

[5] C. Campolo and A. Molinaro, "Data Rate Selection in WBSS-based IEEE 802.11p/WAVE Vehicular Ad Hoc Networks," in *Proceedings of Nets4Cars*, 2010, pp. 412–416.

[6] N. Komoda and R. W. Goudy, "The standardization activities in iso/tc204/wg14 vehicle/roadway warning and control systems." in *Proceedings of Steps Forward, Intelligent Transport Systems World Congress.*, vol. 5, Yokohama, Japan., November 1996.

[7] S. E. Shladover, "Intelligent solutions Next generation warning and control systems." *ISO Focus*, October 2009.

[8] J.-C. Chen and T. Zhang, *IP-Based Next-Generation Wireless Networks*. John Wiley & Sons John Wiley & Sons, 2004.

[9] DVSA, "Highways Agency warns tailgaters that 'only a fool breaks the 2-second rule'," Driver and Vehicle Standards Agency, Tech. Rep., 22 May 2014.

[10] RSA-Ireland, "Driving safely in traffic - the two second rule," URL: http://www.rotr.ie/rules-for-driving/, Road Safety Authority, Republic of Ireland, Tech. Rep., 2014, correct as of 13 December 2015.

[11] DMV-NY, "Chapter 8: Defensive Driving," The New York State Department of Motor Vehicles, URL: http://dmv.ny.gov/about-dmv/chapter-8-defensive-driving, 2015, correct as of 13 December 2015.

[12] R. Johnson and J. H. Brown, *The Twentieth Century Biographical Dictionary of Notable Americans*. The Biographical Soceity, 1904.

[13] A. K. Sen, "Sir J.C. Bose and Radio Science," *IEEE MTT-S International Microwave Symposium Digest*, vol. 1, pp. 557–560, June 1997.

[14] J. Gans, S. King, and J. Wright, *Handbook of Telecommunications Economics (Volume 2): Technology Evolution and the Internet*. Elsevier, 2005, vol. 2, ch. 7 (Wireless Communication), pp. 243–285.

[15] C. S. R. Murthy and B. S. Manoj, *Ad Hoc Wireless Networks: Architectures and Protocols*. Pearson Education, May 2004.

[16] G. Watson, "System of Communication," American Patent US 2 495 682 A, 1932.

[17] A. Goldsmith, *Wireless Communications*. Cambridge University Press, 2005.

[18] M. Mouly and M.-B. Pautet, *The Gsm System for Mobile Communications*. Telecom Pub, 1992.

[19] H. Labiod, A. Hossam, and C. D. Santis, *Wi-Fi, Bluetooth, Zigbee and Wimax*. Springer, 2007.

[20] T. Krag and S. Bettrich, *Wireless Mesh Networking*. OReilly Wireless Devcenter, 2004.

[21] A. D. Wood, J. A. Stankovic, and S. H. Son, "JAM: A Jammed-Area Mapping Service for Sensor Networks," in *Proceedings of 24th IEEE Real-Time Systems Symposium*, 2003, pp. 286–297.

[22] K.-S. Hong and L. Choi, "Dag-based multipath routing for mobile sensor networks," in *Proceedings of International Conference on ICT Convergence (ICIT)*, Seoul, Korea, September 2011.

[23] P. Nicopolitidis, M. S. Obaidat, G. I. Papadimitriou, and A. S. Pomportsis, *Wireless Networks*. Wiley, 2013.

[24] J. Schiller, *Mobile Communications*, 2nd ed. Addison Wesley, 2003.

[25] C. E. Perkins, *Ad Hoc Networking*. Addison Wesley, 2001.

[26] A. Boukerche, H. Oliveira, E. Nakamura, and A. Loureiro, "Vehicular Ad Hoc Networks: A New Challenge for Localization-Based Systems," *Computer Communications (Elsevier)*, vol. 31, no. 12, pp. 2838–2849, 2008.

[27] "FCC Allocates Spectrum in 5.9 GHz Range for Intelligent Transportation System Uses," Published as a News Release by Federal Communications Commission, Washington, D.C. 20554., 1999.

[28] "Cars Talking and Hearing in Harmony' - a Smart Move for ETSI! Newly published ETSI Harmonized Standard enables market placement of radio equipment for road safety and traffic management," Published as a Press Release by European Telecommunications Standards Institute (ETSI), Sophia Antipolis, France., 2008.

[29] T. Nadeem, P. Shankar, and L. Iftode, "A Comparative Study of Data Dissemination Models for VANETs," in *Proceedings of IEEE Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services*, San Jose, CA, USA, 2006, pp. 1–10.

[30] S. Yousefi, M. Siadat, and M. M. Fathy, "Vehicular Ad Hoc Networks (VANETs): Challenges and Perspective," in *Proceedings of the 6th Intermational Coference on ITS Telecommunications*, 2006, pp. 761–766.

[31] S. Y. Wang, "Predicting the Lifetime of Repairable Unicast Routing Paths in Vehicle-Formed Mobile Ad Hoc Networks on Highways," in *Proceedings of the 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, Barcelona, Spain, September 2004.

[32] ——, "On the intermittence of routing paths in vehicle formed mobile ad hoc networks on highways," in *Proceedings of the 7th International IEEE Conference on Intelligent Transportation Systems*, October 2004.

[33] J. Harri and C. Bonnet, "A Lower Bound for Vehicles Trajectory Duration," in *Proceedings of IEEE Vehicular Technology Conference*, 2006.

[34] M. M. Artimy, W. Robertson, and W. Phillips, "Connectivity in InterVehicle Ad Hoc Networks," in *Proceedings of the Canadian Conference on Electrical and Computer Engineering (CCGEI)*, Niagara Falls, Canada., 2004.

[35] M. M. Artimy, W. Robertson, and W. J. Phillips, "Connectivity with Static Tranlsmission Range in Vehicular Ad Hoc Networks," in *Proceedings of the 3rd Annual Communication Networks and Services Research Conference (CNSR)*, Halifax, Canada, May 2005.

[36] J. J. Blum, A. Eskaindarian, and L. Hoffman, "Challenges of Intervehicle Ad Hoc Networks," *IEEE Transaction on Intelligent Transportation Systems*, vol. 5, no. 4, pp. 347–351, December 2004.

[37] V. Kumar, S. Mishra, and N. Chand, "Applications of VANETs: Present & Future," *Communications and Network*, pp. 12–15, 2013.

[38] *IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks*, IEEE 802 Working Groups Std., 2012.

[39] P. Brenner, "A Technical Tutorial on the IEEE 802.11 Protocol," Breezecom, Tech. Rep., 1997.

[40] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network Information Flow," *IEEE Transaction on Information Theory*, vol. 46, no. 4, pp. 1204–1216, July 2000.

[41] J. Widmer and J.-Y. L. Boudec, "Network coding for efficient communication in extreme networks," in *Proceedings of ACM SIGCOMM workshop on Delay-tolerant networking*, 2005, pp. 284–291.

[42] H. Seferoglu and A. Markopoulou, "Network Coding-Aware Queue Management for TCP Flows Over Coded Wireless Networks," *IEEE/ACM Transactions on Networking*, vol. 22, no. 4, pp. 1297–1310, September 2013.

[43] A. A. Hamra, C. Barakat, and T. Turletti, "Network coding for wireless mesh networks: a case study," in *Proceedings of International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Buffalo-Niagara Falls, USA, 2006.

[44] S. Katti, D. Katabi, H. Balakrishnan, and M. Medard, "Symbol-level network coding for wireless mesh networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 4, pp. 401–412, October 2008.

[45] S. Omiwade, R. Zheng, and C. Hua, "Practical Localized Network Coding in Wireless Mesh Networks," in *Proceedings of 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, San Francisco, CA, USA, 2008, pp. 332–340.

[46] D. Silva and F. R. Kschischang, "On metrics for error correction in network coding," *IEEE Transactions on Information Theory*, vol. 55, no. 12, pp. 5479–5490, 2009.

[47] M. Gadouleau and Z. Yan, "Packing and covering properties of subspace codes for error control in random linear network coding," *IEEE Transactions on Information Theory*, vol. 56, no. 5, pp. 2097–2108, May 2010.

[48] Z. Zhang, "Theory and applications of network error correction coding," *Proceedings of the IEEE*, vol. 99, no. 3, pp. 406–420, March 2011.

[49] C. Gkantsidis, J. Miller, and P. Rodriguez, "Comprehensive view of a live network coding P2P system," in *Proceedings of ACM SIGCOMM*, 2006, pp. 177–188.

[50] B. Li and D. Niu, "Random Network Coding in Peer-to-Peer Networks: From Theory to Practice," *Proceedings of the IEEE*, vol. 99, no. 3, pp. 513–523, March 2011.

[51] M. Yang and Y. Yang, "Applying Network Coding to Peer-to-Peer File Sharing," *IEEE Transactions on Computers*, vol. 63, no. 8, pp. 1938–1950, April 2013.

[52] D. S. Lun, N. Ratnakar, R. Koetter, M. Medard, E. Ahmed, and H. Lee, "Achieving Minumum-Cost Multicast: A Decentralized Approach Based on Network Coding," in *Proceedings of INFOCOM*, vol. 3, Miami, USA, March 2005, pp. 1607–1617.

[53] S. Deb, M. Medard, and C. Choute, "Algebraic Gossip: A Network Coding Approach to Optimal Multiple Rumor Mongering," *IEEE Transactions on Information Theory*, pp. 1–22, 2006.

[54] D. Mosk-Aoyama and D. Shah, "Information Dissemination via Network Coding," in *Proceedings of Information Theory*, Seattle, WA, USA, July 2006, pp. 1748–1752.

[55] C. Fragouli, J. Widmer, and J.-Y. L. Boudec, "A Network Coding Approach to Engery Efficient Broadcasting: from theory to practice," in *Proceedings of INFOCOM*, Barcelona, Spain, April 2006, pp. 1–11.

[56] L. Li, R. Ramjee, M. Buddhikot, and S. Miller, "Network Coding-Based Broadcast in Mobile Ad hoc Networks," in *Proceedings of INFOCOM*, Anchorage, Alaska, USA, May 2007, pp. 1739–1747.

[57] K. A. Agha, N. Kadi, and I. Stojmenovic, "Fountain Codes with XOR of Encoded Packets for Broadcasting and source independent backbone in Multi-hop Networks using Network Coding," in *Proceedings of Vehicular Technology Conference*, Barcelona, Spain, 2009, pp. 1–5.

[58] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular Ad Hoc network," *Journal of Network and Computer Applications*, pp. 1–13, 2013.

[59] F. J. Martinez, J.-C. Cano, C. T. Calafate, and P. Manzoni, "A VANET Solution to Prevent Car Accident," in *Proceedings of Jornadas de Paralelismo*, Spain, 2007.

[60] Y. Liu, U. Ozguner, and E. Ekici, "Performance Evaluation of Intersection Warning System using a Vehicle Traffic and Wireless Simulator," in *Proceedings of IEEE Intelligent Vehicles Symposium*, Las Vegas, NV, USA, June 2005, pp. 171–176.

[61] J. Yang, J. Wang, and B. Liu, "An Intersection Collision Warning System Using Wi-Fi Smartphones in VANET," in *Proceedings of IEEE Global Telecommunications Conference*, Houston, TX, USA, December 2011, pp. 1–5.

[62] C. J. Merlin and W. B. Heinzelman, "A study of Safety Applications in Vehicular Networks," in *Proceedings of IEEE International Conference on Mobile Adhoc and Sensor Systems*, Washington, DC, USA, November 2005.

[63] C.-L. Huang, Y. P. Fallah, R. Sengupta, and H. Krishnan, "Adaptive Intervehicle Communication Control for Cooperative Safety Systems," *IEEE Networks*, vol. Vol. 24, Issue 1, pp. 20–25, January-February 2010.

[64] N. F. Abdullah, A. Doufexi, and R. J. Piechocki, "Car-to-Car Safety Broadcast with Interference using Raptor Codes," in *Proceedings of IEEE 73rd Vehicular Technology Conference*, Budapest, Hungary, May 2011.

[65] A. Sebastian, M. Tang, Y. Feng, and M. Looi, "A Multicast Routing Scheme for Efficient Safety Message Dissemination," in *Proceedings of IEEE Wireless Communication and Networking Conference (WCNC)*, Sydney, Australia, 2010.

[66] R. Prasad and M. Ruggieri, *Applied satellite navigation - using GPS, GALILEO and augmentation systems*. ARTECH House Publishers, 2005.

[67] EVP-Europe, "A Beginner's Guide to GNSS in Europe," International Federation of Air Traffic Controllers' Associations, Tech. Rep., 1999.

[68] C. J. Hegarty and E. Chatre, "Evolution of the Global Navigation SatelliteSystem (GNSS)," *Proceedings of the IEEE*, pp. 1902–1917, December 2008.

[69] NOAA, "GPS Accuracy," National Coordination Office for Space-Based Positioning, Navigation, and Timing, URL: http://www.gps.gov/systems/gps/performance/accuracy, Tech. Rep., 2013.

[70] ——, "GPS Modernization," National Coordination Office for Space-Based Positioning, Navigation, and Timing, URL: http://www.gps.gov/systems/gps/modernization, Tech. Rep., 2013.

[71] B. Harvey, *The Rebirth of the Russian Space Program*. Springer, 2007, ch. Military programs.

[72] RISS, "Glonass-K: A prospective satellite of the current GLONASS system," Reshetnev Information Satellite Systems, Tech. Rep., 2007.

[73] ESA, "What is Galileo?" European Space Agency, Tech. Rep., December 2015.

[74] J. Laukkonen, "A Collision Avoidance System May Reduce the Likelihood of a Serious Accident," About.com (Car Tech), Tech. Rep., 2013.

[75] Leipzig, "Lane keeping assist: Steering wheel vibrates to warn the driver if the car leaves its lane unintentionally," Mercedes-Benz Cars, Tech. Rep., 2008.

[76] M. Petracca, P. Pagano, R. Pelliccia, M. Ghibaudi, C. Salvadori, and C. Nastasi, *On-Board Unit Hardware and Software Design for Vehicular Ad-Hoc Networks*. IGI Global, 2013.

[77] J. M. D. Fuentes, A. I. Gonzlez-Tablas, and A. Ribagorda, *Overview of Security Issues in Vehicular Ad-hoc Networks*. IGI Global, 2011.

[78] "LKW-MAUT Electronic Toll Collection System for Germany," 2013, uRL: http://www.roadtraffic-technology.com/projects/lkw-maut/lkw-maut3.html.

[79] L. Yang, J. Guo, and Y. Wu, "Piggyback Cooperative Repetition for Reliable Broadcasting of Safety Messages in VANETs," in *Proceedings of 6th IEEE Consumer Communications and Networking Conference*, Las Vegas, NV, USA, 2009.

[80] M. Li, W. Lou, and K. Zeng, "OppCast: Opportunistic Broadcast of Warning Messages in VANETs with Unreliable Links," in *Proceedings of IEEE 6th International Conference on Mobile Adhoc and Sensor Systems*, October 2009, pp. 534–543.

[81] J. J. Haas and Y.-C. Hu, "Communication Requirements for Crash Avoidance," in *Proceedings of 7th ACM International Workshop on VehiculAr InterNETworking (ACM VANET)*, Chicago, IL, USA, September 2010, pp. 1–10.

[82] Q. Yu and D. Liu, "Disseminate Warning Message in VANETs Based on Predicting the Interval of Vehicles," in *Proceedings of the 5th International Conference on Frontier of Computer Science and Technology*, Changchun, China, 2010, pp. 559–564.

[83] F. Martinez, M. Fogue, M. Coll, J.-C. Cano, C. Calafate, and P. Manzoni, "Evaluating the Impact of a Novel Warning Message Dissemination Scheme for VANETs Using Real City Maps," in *Proceedings of International IFIP TC 6 Networking Conference*, Chennai, India, May 2010, pp. 265–276.

[84] H. Kim, "An Efficient Alert Broadcasting Scheme Considering Various Densities in VANET," in *Proceedings of Springer Communications in Computer and Information Science (CCIS) Conference*, 2010, pp. 631–638.

[85] R. Namritha and K. Karuppanan, "Opportunistic Dissemination of Emergency Message using VANET on Urban Roads," in *Proceedings of IEEE International Conference on Recent Trends in Information Technology*, Chennai, India, June 2011, pp. 172–177.

[86] H.-S. Kim, S.-S. Jang, H.-C. Cha, and T.-Y. Byun, "A Relay Vehicle Selection Scheme for Delivery of Emergency Message Considering Density and Trajectory of Moving Vehicles for VANET," in *Proceedings of Springer Communications in Computer and Information Science (CCIS) Conference*, 2011, pp. 257–266.

[87] Y. Li and W. Wang, "Geo-Dissemination in Vehicular Ad Hoc Networks," in *Proceedings of IEEE Ad-hoc and Sensor Networking Symposium*, 2012.

[88] A. Amoroso, G. Marfia, M. Roccetti, and G. Pau, "To Live and Drive in L.A.: Measurements from a Real Intervehicular Accident Alert Test," in *Proceedings of IEEE Workshop on Wireless Vehicular Communications and Networks*, 2012, pp. 328–332.

[89] S. Kumar, L. Shi, N. Ahmed, S. Gil, D. Katabi, and D. Rus, "CarSpeak: A Content-Centric Network for Autonomous Driving," in *Proceedings of ACM SIGCOMM*, Helsinki, Finland, August 2012, pp. 259–270.

[90] H. Samet, "Octree Approximation and Compression Methods," in *Proceedings of the 1st International Symposium on 3D Data Processing Visualization and Transmission*, 2002.

[91] Oxford, *The New Shorter Oxford English Dictionary (pp 2632)*. Clarendon Press, 1993.

[92] S. O. Al-Humoud, L. M. Mackenzie, and W. Vanderbauwhede, "Dynamic counter-based broadcast in MANETs," in *Proceedings of the 4th ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks*, Canary Islands, Spain, 2009, pp. 84–88.

[93] P. Mohapatra, C. Ghu, and J. Li, "Group Communications in Mobile Ad Hoc Networks," *IEEE Computer*, vol. 37, pp. 52–59, February 2004.

[94] R. Chen, W. Jin, and A. Regan, "Broadcasting in Vehicular Networks: Issues and Approaches," *IEEE Networks*, vol. 24(1), pp. 20–25, January–February 2010.

[95] T.A. Ramrekha and C. Politis, "A hybrid adaptive routing protocol for extreme emergency ad hoc communication," in *Proceedings of 19th International Conference on Computer Communications and Networks*, Zurich, Switzerland, August 2010.

[96] A. Dahiya and R. Chauhan, "A Comparative study of MANET and VANET Environment," *Journal of Computing*, vol. 2, pp. pp 87–92, 2010.

[97] S. Y. Wang, "Predicting the lifetime of repairable unicast routing paths in vehicle-formed mobile ad hoc networks on highways," in *Proceedings of the 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, Barcelona, Spain, September 2004.

[98] W. Brad and C. Tracy, "Comparison of Broadcasting Techniques for Mobile Ad hoc Network," in *Proceedings of the 3rd ACM International Symposium on Mobile ad hoc Networking and Computing (Mobihoc)*, Lausanne, Switzerland, 2002.

[99] S. O. Al-Humoud, "The Dynamic Counter-Based Broadcast for Mobile Ad hoc Networks," Ph.D. dissertation, University of Glasgow, Glasgow, United Kingdom, 2011.

[100] P. Wei and L. Xi-Cheng, "On The Reduction of Broadcast Redundancy in Mobile Ad hoc Networks," in *Proceedings of the First Annual Workshop on Mobile and Ad Hoc Networking and Computing*, Boston, MA, USA, 2000.

[101] T. Yu-Chee, N. Sze-Yao, and S. En-Yu, "Adaptive Approaches to Relieving Broadcast Storms in a Wireless Multihop Mobile Ad hoc Network," *IEEE Transactions on Computers*, vol. 52, pp. 545–557, 2003.

[102] Z. Hao and J. Zhong-Ping, "Performance Analysis of Broadcasting Schemes in Mobile Ad hoc Networks," *IEEE Communications Letters*, vol. 8, pp. 718–720, 2004.

[103] S.-Y. Ni, Y.-C. Tseng, Y.-S. Chen, and J.-P. Sheu, "The Broadcast Storm Problem in a Mobile Ad Hoc Network," in *Proceedings of ACM MOBICOM*, Seattle, Washington, USA, 1999, pp. 151–162.

[104] J.-M. Choi, J. So, and Y.-B. Ko, "Numerical Analysis of IEEE 802.11 Broadcast Scheme in Multihop Wireless Ad-hoc Networks," *Information Networking. Convergence in Broadband and Mobile Networking Lecture Notes in Computer Science*, vol. 3391, pp. 1–10, 2005.

[105] Y.-C. Tseng, S.-Y. Ni, Y.-S. Chen, and J.-P. Sheu, "The Broadcast Storm Problem in a Mobile Ad-hoc Network," *Wireless Networks*, vol. 8, pp. 153–167, 2002.

[106] N. Wisitpongphan, O. K. Tonguz, J. S. Parikh, P. Mudalige, F. Bai, and V. Sadekar, "Broadcast Storm Mitigation Techniques in Vehicular Ad Hoc Networks," *IEEE Wireless Communications*, pp. 84–94, 2007.

[107] F. J. Martinez, C.-K. Toh, J.-C. Cano, and C. T. Calafate, "A Street Broadcast Reduction Scheme (SBR) to Mitigate the Broadcast Storm Problem in VANETs," in *Proceedings of Wirelss Pers. Communication*, 2011.

[108] USC, "The Network Simulator – ns-2," The University of Southern California, Tech. Rep., November 2011.

[109] Riverbed, "Riverbed Modeler: The fastest discrete event-simulation engine for analyzing and designing communication networks," Riverbed Application and Network Performance Management Solutions, Tech. Rep., 2015.

[110] OpenSim, "OMNeT++ 5.0b3 released," OpenSim Ltd, Tech. Rep., December 2015.

[111] S. Mao, *Fundamentals of Communication Networks: Principles and Practice*. Academic Press (AP), 2010, ch. Chapter 8 – Fundamentals of communication networks, pp. 201–234.

[112] C. Sommer, R. German, and F. Dressler, "Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis," *IEEE Transactions on Mobile Computing*, vol. 10, no. 1, pp. 3–15, January 2011.

[113] S. Kurkowski, T. Camp, and M. Colagrosso, "MANET Simulation Studies: The IncrediblesMANET Simulation Studies: The Incredibles," *ACM SIGMOBILE Mobile Computing and Communications ...ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 9, no. 4, 2005.

[114] M. Ciampa, *CWNA Guide to Wireless LANs*. Cengage Learning, 2013.

[115] F. Martinez, C.-K. Toh, J.-C. Cano, and C. Calafate, "Realistic Radio Propagation Models (RPMs) for VANET Simulations," in *Proceedings of the Wireless Communications and Networking Conference (WCNC)*, Budapest, Hungary, April 2009, pp. 1–6.

[116] C. Sommer, D. Eckhoff, R. German, and F. Dressler, "A computationally inexpensive empirical model of IEEE 802.11p radio shadowing in urban environments," in *Proceedings of the Eighth International Conference on Wireless On-Demand Network Systems and Services (WONS)*, Bardonecchia, Italy, 2011, pp. 84–90.

[117] M. Boban, T. Vinhoza, M. Ferreira, and J. Barros, "Impact of Vehicles as Obstacles in Vehicular Ad Hoc Networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 1, pp. 15–28, 2011.

[118] A. Mahajan, N. Potnis, K. Gopalan, and A. Wang, "Modeling vanet deployment in urban settings," in *Proceedings of the 10th ACM Symposium on Modeling, Analysis, and Simulation of Wireless and Mobile Systems*, Crete Island, Greece, 2007, pp. 551–558.

[119] T. Camp, J. Boleng, , and V. Davies, "A survey of mobility models for ad hoc network research," *Wireless Communication and Mobile Computing Special Issue on Mobile Ad Hoc Networking: Research, Trends and Applications.*, pp. 483–502, 2002.

[120] M. Musolesi and C. Mascolo, "Mobility Models for Systems Evaluation: A Survey," Dartmouth College (USA) and University of Cambridge (UK), Tech. Rep., 2011.

[121] V. Gupta and M. K. Rohil, "Information Embedding in IEEE 802.11 Beacon Frame," in *Proceedings of National Conference on Communication Technologies and its impact on Next Generation Computing (CTNGC)*, 2012.

[122] T. A. Berson, "Differential Cryptanalysis Mod 232 with Applications to MD5Differential Cryptanalysis Mod 2 to th power 32 with Applications to MD5," *EUROCRYPT*, pp. 71–80, 1992.

[123] DoT, "The Highway Code," Department for Transport, Tech. Rep., October 2015.

[124] P. Papadimitratos, L. Buttyan, H. Holczer, and S. E., "Secure vehicular communication systems: Design and architecture," *IEEE Communications*, vol. 46, pp. 100–109, 2008.

[125] N. M. Chowdhury, L. M. Mackenzie, and C. Perkins, "Requirement Analysis for Building Practical Accident Warning Systems based on Vehicular Ad-hoc Networks," in *11th IEEE/IFIP Annual Conference on Wireless On-demand Network Systems and Services (WONS)*. Obergurgl, Austria: IEEE, 2014, pp. 81–88.

[126] V. Paxson, "An analysis of using reflectors for distributed denial-of-service attacks," *Computer Communication Review*, vol. 31 (3), July 2001.

[127] L. Garber, "Denial-of-service attacks rip the internet," *Computer Magazin*, July 2000.

[128] W. Xu, T. Wood, W. Trappe, and Y. Zhang, "Channel surfing and spatial retreats: defenses against wireless denial of service." in *Proceedings of ACM workshop on Wireless Security*, 2004, pp. 80–89.

[129] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of Service Attacks in Wireless Networks: The Case of Jammers," *IEEE Communications Surveys and Tutorials*, vol. 13 (2), pp. 245–257, 2011.

[130] J. Douceur, "The sybil attack," in *Proceedings of the first International Workshop on Peer-to-Peer Systems*, 2002.

[131] C. Chen, X. Wang, W. Han, and B. Zang, "A Robust Detection of the Sybil Attack in Urban VANETs," in *Proceedings of the 29th IEEE International Conference on Distributed Computing Systems Workshops*, 2009.

[132] G. Guette and B. Ducourthial, "On the Sybil attack detection in VANET," in *Proceedings of IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems*, 2007.

[133] S. M. Safi, A. Movaghar, and M. Mohammadizadeh, "A Novel Approach for Avoiding Wormhole Attacks in VANET," in *Proceedings of First Asian Himalayas International Conference on Internet*, 2009.

[134] Y.-C. Hu and D. Johnson, "Wormhole Attacks in Wireless Networks," *IEEE Journal on Selected Areas in Communications*, vol. 24 (2), pp. 370–380, 2006.

[135] B. S. Thakur and S. Chaudhary, "Content sniffing attack detection in client and server side: A survey," *International Journal of Advanced Computer Research*, vol. 2 (10), pp. pp 7 – 10, 2013.

[136] I. A. Sumra, H. Hasbullah, J. lail, and R. Masood-ur, "Trust and Trusted Computing in VANET," *Computer Science Journa*, vol. 1 (1), pp. 29–51, 2011.

[137] B. Parno and A. Perrig, "Challenges in securing vechicular networks," in *In the proceedings of ACM SIGCOMM*, 2005.

[138] J.-J. Wang, J.-P. Li, Y.-F. Li, and J. Peng, "Review of Key-Based Dynamic Trust Authorization Mechanism," in *Proceedings of International Conference on Wavelet Active Media Technology and Information Processing (ICWAMTIP)*, Chengdu, China, 2012, pp. 263–267.

[139] A. Bradai, W. Ben-Ameur, and H. Afifi, "Byzantine resistant reputation-based trust management," in *Proceedings of the 9th International Conference Conference on Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom)*, Austin, TX, USA, 2013, pp. 269–278.

[140] S. Ries, M. Fischlin, L. Martucci, and M. Muhlhauser, "Learning Whom to Trust in a Privacy-Friendly Way," in *Proceedings of 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Changsha, China, 2011, pp. 214–225.

[141] H. Deng, R. Xu, J. Li, and F. Zhang, "Agent-based cooperative anomaly detection for wireless ad hoc networks," in *Proceedings of the 12th International Conference on Parallel and Distributed Systems*, 2006.