Mitigation Strategies for Safety Applications in Vehicular Ad Hoc Networks Subjected to Jamming

A Dissertation
Presented in Partial Fulfillment of the Requirements for the
Degree of Doctor of Philosophy
with a
Major in Computer Science
in the
College of Graduate Studies
University of Idaho
by
Hani Eftikhar Alturkostani

Major Professor: Axel Krings, Ph.D.
Committee Members: Robert Rinker, Ph.D.; Jim Alves-Foss, Ph.D.; Ahmed Abdel-Rahim, Ph.D.
Department Administrator: Rick Sheldon, Ph.D.

April 2016

Authorization to Submit Dissertation

This dissertation of Hani Eftikhar Alturkostani, submitted for the degree of Doctor of Philosophy with a Major in Computer Science and titled "Mitigation Strategies for Safety Applications in Vehicular Ad Hoc Networks Subjected to Jamming," has been reviewed in final form. Permission, as indicated by the signatures and dates below, is now granted to submit final copies to the College of Graduate Studies for approval.

Major Professor: ______________________ ____________

Axel Krings, Ph.D. Date

Committee Members: ______________________ ____________

Robert Rinker, Ph.D. Date

______________________ ____________

Jim Alves-Foss, Ph.D. Date

______________________ ____________

Ahmed Abdel-Rahim, Ph.D. Date

Department

Administrator: ______________________ ____________

Rick Sheldon, Ph.D. Date

Abstract

The term Intelligent Transportation Systems (ITS) refers to the technologies, services, and applications that allow vehicles to communicate with each other (V2V) and also with fixed infrastructures (V2I) and (I2V). This collaborative communication forms a Vehicular Ad-Hoc Network (VANET) that enables the deployment of a wide range of useful applications to address some of transportation's most critical elements, such as mobility, environment, and safety. A key technology to facilitate such communication is called Dedicated Short Range Communications (DSRC), which operates in the 5.9 GHz band. One of the most important applications in ITS, furthermore, are DSRC Safety Applications, which aim to enhance safety and reduce traffic accidents. The reliability of any Safety Application is crucial; any disturbance, whether benign or malicious, could lead to catastrophic consequences like injury or loss of life. Wireless jamming is considered to be a serious threat to Safety Applications due to its simple implementation and severe impact on ongoing communications. In fact, wireless jamming is capable of blocking the communication between nodes entirely and creating a Wireless Denial of Service (WDoS) attack.

In this dissertation, we propose a new series of mitigation strategies for DSRC Safety Applications in VANETs to enhance their overall reliability in the presence of jamming attacks. These mitigation strategies are as follows: 1) an adaptive threshold-based agreement algorithm, 2) a detection algorithm that enables jamming-aware Safety Applications, and 3) a recovery strategy that uses dynamic transmission and power rates. Throughout this dissertation, we discuss these mitigation strategies and investigate their usefulness using mathematical models, simulations, and field experiments. Our test results show that the mitigation strategies will help to enhance the reliability of Safety Applications in the presence of wireless jamming. In addition, the techniques recommended by this dissertation are in line with current institutional and governmental standardization efforts and will not overwhelm the communication media.

Acknowledgements

I would like to express the deepest appreciation to my major professor, Axel Krings, for his exceptional guidance, patience, and caring as well as for providing me with an excellent atmosphere for doing research. Without his guidance and persistent help, writing this dissertation would not have been possible. I would also like to thank my committee members for their support and guidance: Dr. Ahmed Abdel-Rahim, Dr. Robert Rinker, and Dr. Jim Alves-Foss.

Moreover, I am thankful to the Institute of Public Administration in Saudi Arabia for funding my scholarship, and to the Idaho Global Entrepreneurial Mission (IGEM) for funding the test equipment and the field experiments.

Finally, I am deeply grateful to the University of Idaho's Computer Science faculty, staff, and students for how they have affected my life and studies and for providing me with an environment that enabled me to work.

Dedication

I would like to dedicate this dissertation to praising GOD and asking for his peace and blessing on all of those who contributed to completing this research and making it useful knowledge. Also, I would like to express a special feeling of deepest gratitude to my family for their support, patience, and encouragement toward the completion of this work.

My father, Eftikhar Alturkostani.
My mother, Niylah Khoja.
My wife, Noha Aziz.
My sons, Yazan and Yamen.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

ITS	Intelligent Transportation Systems
USDOT	United States Department of Transportation
V2V	Vehicle-to-Vehicle
V2I	Vehicle-to-Infrastructure
I2V	Infrastructure-to-Vehicle
DSRC	Dedicated Short Range Communication
WDoS	Wireless Denial of Service attack (WDoS)
NHTSA	National Highway Traffic Safety Administration
VANET	Vehicular ad hoc Networks
ECDSA	Elliptic Curve Digital Signature Algorithm
CA	Certificate Authority
IEEE	Institute of Electrical and Electronics Engineer
MAC	Media Access Control
BSM	Basic Safety Message
RSU	Road Side Unit
OBU	On-Board Unit
WSN	Wireless Sensor Networks
MANET	Mobile Ad-Hoc Networks
EEBL	Emergency Electronic Brake Lights
VSC-A	Vehicle Safety Communications - Applications
PDR	Packet Delivery Ratio
FCC	Federal Communication Commission
HV	Host Vehicle
RV	Remote Vehicle
WSMP	WAVE Short Message Protocol
IPv6	Internet Protocol Version 6
UDP	User Datagram Protocol
TCP	Transmission Control Protocol

WSM	WAVE Short Messages
WAVE	Wireless Access in Vehicular Environments
SAE	Society of Automotive Engineers
CCH	Control Channel
SCH	Service Channel
EIRP	Effective Isotropic Radiated Power
LLC	Logic Link Control
ASTM	American Society for Testing and Materials
DCF	Distributed Coordination Function
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DIFS	Distributed Inter-Frame Space
SIFS	Short Inter-frame Space
PIFS	PCF Inter-frame Space
PCF	Point Coordination Function
FCW	Forward Collision Warning
BSW	Blind Spot Warning
LCW	Lane Change Warning
DNPW	Do Not Pass Warning
IMA	Intersection Movement Assist
CLW	Control Loss Warning
ACM	À la Carte message
SNR	Signal-to-Noise Ratio
SJR	Signal-to-Jamming Ratio
LDCP	Low Density Parity Check
RSSI	Received Signal Strength Indicator
GPS	Global Positioning System
FSPL	Free Space Path Loss
PHY	Physical Layer
OFDM	Orthogonal Frequency Division Multiplexing
BPSK	Binary Phase Shift Keying
QPSK	Quadrature Phase Shift Keying

QAM	Quadrature Amplitude Modulation
WSA	WAVE Service Advertisement
MIPS	Microprocessor without Interlocked Pipeline Stages
SDRAM	Synchronous Dynamic Random-Access Memory
BER	Bit Error Rate
WLAN	Wireless Local Area Network
PCI	Peripheral Component Interconnect
PCAP	Packet Capture
RF	Radio Frequency
PVD	Probe Vehicle Data
PLCP	Physical Layer Convergence Protocol

CHAPTER 1

Introduction

Humans invented the wheel long ago and realized the benefits of hauling people and goods faster and more efficiently. Transportation has come a long way since that era; in fact, it has become one of the important systems that define our modern civilization. Whether we are driving cars, riding bicycles, or just walking, transportation impacts all of us in our everyday lives. This complex infrastructure of high-speed moving vehicles and roads comes with myriad challenges. These challenges can be categorized into three types: those that are related to mobility, those that are related to environment, and those that are related to safety. The safety of operating vehicles and the dangers associated with traveling on roads are of great concern.

According to the National Highway Traffic Safety Administration (NHTSA), there were 6.1 million police-reported crashes in 2014, and the number of fatalities from vehicle crashes accounted for 32,675 deaths in the U.S. in addition to 2.3 million injuries [1]. Governments and manufacturers alike have made efforts to reduce these fatalities and crashes, from enforcing strict rules and regulations to employing all available technologies to enhance safety.

Safety technologies, from passive mechanical features such as seat belts to computerized active measures, have improved as the available technologies advanced. The revolutionized communication technologies, however, have allowed a new collaborative safety system to be envisioned. This system will take advantage of wireless communication in order to expand the awareness and sensing capabilities of the technologies, services, and applications of Intelligent Transportation Systems (ITS). ITS are expected to improve the driving experience and aim to reduce the number of road accidents that occur. A technology that is at the core of ITS is wireless communication, specifically wireless vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. In an ITS, the group of communicating vehicles form a de-centralized network, referred to as a Vehicular Ad-Hoc Network (VANET).

Intelligent Transportation Systems provide a variety of useful applications. The most important of these, however, are the Safety Applications, which will help prevent collisions and increase driver awareness. It is estimated by the U.S. Department of Transportation (USDOT) that V2V applications based on Dedicated Short Range Communications (DSRC) can prevent up to 82% of all crashes in the United States that involve unimpaired drivers, potentially saving thousands of lives and billions of dollars [38]. Safety Applications rely on periodic Basic Safety Message (BSM) exchanges among vehicles and between vehicles and the infrastructure. The communication among vehicles and the infrastructure requires a solid underlying platform that consists of well-defined technologies in order to ensure safe, stable, and reliable system operation.

1.1 RESEARCH MOTIVATION AND OBJECTIVES

This dissertation focuses on the reliability of Safety Applications in ITS, which is of great concern, since Intelligent Transportation Systems are a part of a critical infrastructure. The wireless communication at the core of this technology, however, inherits the full spectrum of potential vulnerabilities and attacks, and any failure on its part may have catastrophic consequences like injury or loss of life. In particular, this work will focus on the mitigation of wireless jamming in VANETs, as jamming can disrupt Safety Applications to the point of rendering them useless.

In fact, Safety Applications can be manipulated by jamming in a way that may lead them to make wrong decisions and an increased level of hazards. Furthermore, any compromise, whether due to benign or malicious reasons, has the potential to undermine the public trust and acceptance of DSRC based on VANET technologies. Conventional security measures such as digital certificates, tamper-proof hardware, and network security schemes are not sufficient [49]. Therefore, it is paramount that mechanisms to increase reliability in the presence of faults are designed into the system rather than appended in an add-on fashion.

1.2 LITERATURE REVIEW

As mentioned earlier, VANETs can enable a wide range of applications that will be beneficial in reducing traffic accidents, enhancing mobility, and improving fuel efficiency. A number of challenges must be addressed before these applications are actually deployed, however. In this section, we will survey some challenges that are directly related to our research. In particular, we will discuss the challenges inherent in VANETs with regard to security and reliability.

Securing VANET communications and applications is fundamental. A lack of security, the use of improper techniques, or the undermining effects of pathological attacks will potentially have damaging consequences. For instance, these could incite a selfish behavior or, even worse, a disruption intended to cause crashes. The types of attacks that target vehicular networks can vary, but they are mostly been well-known and have been studied with great detail in [9, 11, 12, 54]. These attacks are:

Bogus information (forgery): In this type of attack, an attacker is capable of injecting and disseminating faulty information that impacts the decisions of other drivers within the context of the fault models that will be presented in Section 2.3. This attack involves generating value faults, e.g., transmissive symmetric or transmissive asymmetric faults. Producing value faults can be as simple as stimulating the sensors or internal equipment of the vehicle in order to mimic a nonexistent situation, e.g., tampering with on-board equipment at its source [54]. Alternatively, it can be as sophisticated as altering or fabricating the content of safety messages or positional information [13].

Several methods have been suggested to counter this type of attack. These methods can be categorized into either 1) using authentication and digital certificates [15, 16, 17, 14] or 2) using content verification [18, 50, 19, 53]. Agreement in VANET will be discussed in more details in Chapter 3, as the topic of agreement will be one of our major focuses in this research. Authentication and digital signatures in VANET have been thoroughly discussed in the IEEE 1609.2 standard [45], which suggests that messages be digitally signed by the sender in order to allow the receiver to verify that these messages have not been altered in any way. The digital signature implies that the sender is authorized to send the message. An asymmetric cryptographic algorithm is used for that purpose, which is the Elliptic Curve Digital Signature Algorithm (ECDSA), as mandated by the IEEE 1609.2. The authentication algorithm uses either 224-bit or 256-bit key lengths. Using ECDSA can be concerning, since the algorithm is considered to be processor-intensive. This is crucial, especially in dense environments where a receiver could receive up to thousands of BSMs every second. In [38] it was shown that signing or verifying a message with the 224-bit version of ECDSA takes about 60% to 80% as much processing time as using the 256-bit version. Thus, signing BSMs using the 224-bit key is favorable. In addition, the use of implicit certificates is a viable option to conserve resources.

ID disclosure (privacy violation): In this method of attack, an attacker may reveal a vehicle's identity and thus track its whereabouts and violate its privacy. According to the SAE J2735 standard [40], the identity of the vehicle, including the MAC address and the vehicle's ID, are temporary in order to ensure privacy. However, it is possible to link different identities with different locations in order to track a certain vehicle [20].

Several privacy schemes have been presented in the literature with the purpose of providing anonymity and un-linkability for both BSM messages and location information. Some schemes suggest the use of conditional privacy, in which only designated entities (e.g., law enforcement) are allowed to track certain vehicles in specific situations. We refer the reader to the following publications for a more in-depth overview of these issues [21, 22, 14, 23, 24, 25, 26].

Sybil Attack (impersonation): In this method of attack, the attacker pretends to be another vehicle by using a false identity, or they may send multiple messages from one node with multiple identities. This attack can be used to create an illusion of traffic congestion or to impersonate public safety vehicles. The sybil attack is regarded as a serious threat to VANETs and has been addressed in [33, 34, 54].

Several methods have been suggested as solutions to counter this attack. In [35], the authors have proposed a detection scheme based on the received signal strength variations, which allows the verification of the authenticity of nodes based their location. In [36], the authors suggest a similar approach via the introduction of the use of Road Side Units (RSUs) to collect the signal strengths and locations of vehicles.

A data-centric approach has been suggested by [37] in which an algorithm observes the behavior of a vehicle after sending a message.

Denial of Service (jamming): In this method of attack, the attacker targets the communication between nodes in order to completely or partially stop the service. This can be accomplished by emitting noise to interfere with legitimate communication or by flooding the media with bogus messages. This type of attack is referred to as jamming [11]. In addition, there are several types of jammers, including constant, random, and intelligent ones. The different types of jammers will be explained in more detail in Section 2.4. Methods to counter the effects of jamming have been extensively studied for wireless networks in general, including Wireless Sensor Networks (WSNs), Cognitive Radio Networks, and Mobile Ad-Hoc Networks (MANETs) [27, 28, 29, 30, 31, 32]. In Chapter Chapter 4, we will study some of these methods and their applicability in VANET environments.

We will focus on jamming and its impact on Safety Applications throughout this research. This is because of jamming's grave impact and ease of implementation in addition to the lack of proper protection mechanisms specifically for VANETs against jamming.

1.3 SUMMARY OF CONTRIBUTIONS

The major contributions of this dissertation are as follows:

1. An adaptive threshold-based agreement algorithm is presented that provides higher resilience in the presence of jamming. The performance of the new algorithm and its resilience against jamming are investigated using the Electronic Emergency Brake Lights (EEBL) Safety Application defined in the VSC-A project and the J2735 standard [40, 52]. The new algorithm outperforms its counterparts due to the nature of adaptively adjusting the voting thresholds. Whereas the observed improvements were modest, these improvements can be seen in the context of saving lives. In addition, we show that constant jamming can drastically decrease the decision quality for these threshold-based agreement algorithms.

2. A jamming detection algorithm is introduced to guide DSRC Safety Applications to a fail-safe mode. Specifically, we study the impact of a jamming type called a deceptive jammer on Basic Safety Messages (BSM) reception. The algorithm uses two different types of metrics: distance between vehicles and Packet Delivery Ratio (PDR). Furthermore, the algorithm uses predictions for distances and PDR when real information is not available due to BSM jamming. The field test results, using vehicles equipped with Arada LocoMate On Board Units (OBUs), show that the disruption of BSMs by deceptive jammers was significant. The results also show that a jamming-aware algorithm is capable of shifting DSRC Safety Applications to a fail-safe mode when jamming is detected.

3. A recovery strategy is introduced that uses higher BSM rates and adjusts transmission power and data rates[1] only when jamming is detected . In addition, we investigate the tradeoff between channel efficiency and reliability, since uncontrolled retransmission has the potential of saturating the media. Our results show that the recovery strategy helps Safety Applications to transition from fail-safe mode to operational mode earlier for several jammer types. In the context of safety critical applications, this will be especially helpful in avoiding accidents and saving lives.

1.4 DISSERTATION ORGANIZATION

In Chapter 2 we will give background information related to our work and to the ITS. The adaptive threshold-based algorithm will be discussed in details in Chapter 3. The design of jamming-aware Safety Applications in VANETs explained in Chapter 5. A novel recovery Strategy for DSRC Safety Applications subjected to jamming attacks will be introduced in Chapter 5. Finally, the conclusions and future work are presented in Chapter 6.

[1] Within the power ratings specified in FCC amendment [48]

CHAPTER 2
BACKGROUND

2.1 INTELLIGENT TRANSPORTATION SYSTEMS

The Federal Communication Commission (FCC) has licensed the use of the 5.850-5.925 GHz (5.9 GHz band) for the DSRC services [48]. Since it operates in a wireless environment, DSRC inherits the entire spectrum of vulnerabilities, e.g., signal manipulation, degradation or disruption. Given that ITS is part of a critical infrastructure, and the fact that any failure may result in loss of life, it is important to consider security and safety implications that might result from malicious act. A secondary consequence would be the loss of public trust in the technologies.

DSRC overall architecture is shown in Figure 2.1. A set of industry standards has been published to cover each layer of the architecture and to address proper interoperability, including [39, 40, 42, 44, 45, 46, 47]. Vehicles will be equipped with OBUs for inter-vehicular communication as well as communication with stationary RSUs. All vehicles will run Safety Applications and contribute by sending or receiving messages collaboratively. However, from a Safety Application point of view, we refer to the vehicle generating the alert as Remote Vehicle (RV), and the vehicle making the decision as Host Vehicle (HV).

To facilitate communications seven 10 MHz channels are used, i.e., one Control Channel (Channel 178) and six Service Channels (Channels 172, 174, 176, 180, 182 and 184), in addition to one 5 MHz channel held in reserve, as can be seen in Figure 2.2. Channel 172 is intended to be dedicated for V2V public safety communications, other channels are envisioned to be used for non-safety communication. Different channels have different power levels, which impacts the choice of a certain channel when designing Safety Applications.

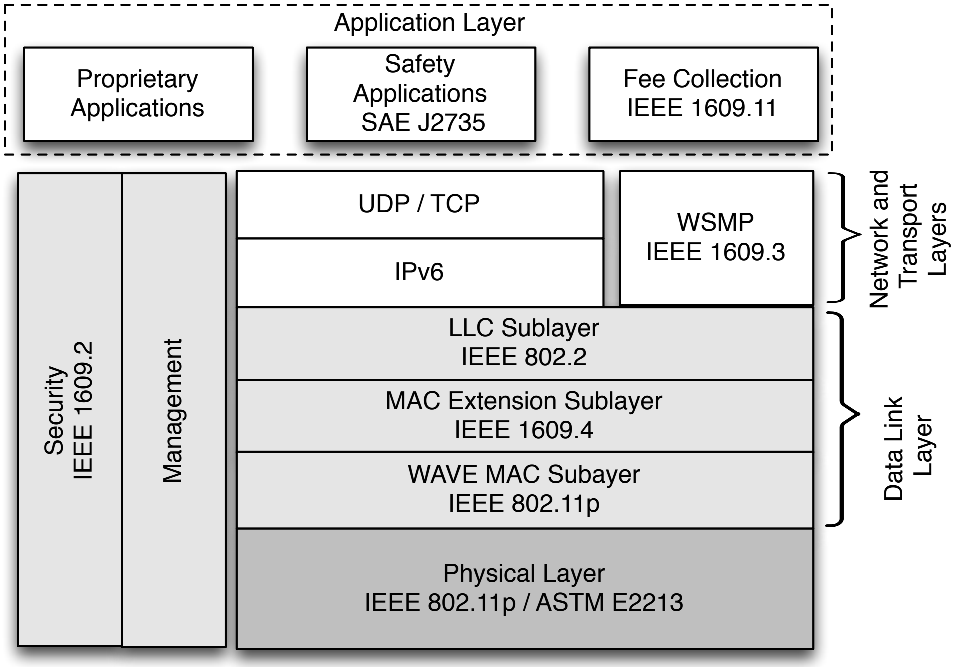
Application Layer
Proprietary Applications
Safety Applications SAE J2735
Fee Collection IEEE 1609.11
Security IEEE 1609.2
Management
UDP / TCP
IPv6
WSMP IEEE 1609.3
Network and Transport Layers
LLC Sublayer IEEE 802.2
MAC Extension Sublayer IEEE 1609.4
WAVE MAC Subayer IEEE 802.11p
Data Link Layer
Physical Layer IEEE 802.11p / ASTM E2213

Figure 2.1: Layered architecture for DSRC

2.1.1 *Power Levels*

Table 2.1 summarizes power levels for different DSRC channels. According to [48], the maximum Effective Isotropically Radiated Power (EIRP) will not exceed 30 W (44.8 dBm). The Effective Isotropic Radiated Power (EIRP) is the apparent power transmitted towards the receiver, assuming that the signal is radiated equally in all directions, we have

$$EIRP_{log} \quad = \quad P_T \quad - \quad L_c \quad + \quad G_a$$

where P_T is the transmission power in dBm, L_C is the signal loss in dB, and G_a is the antenna gain in dBi, relative to a isotropic reference antenna.

$$dBm \quad = \quad 10 log\left(\frac{outputpower}{1mW}\right)$$

Specific channel categories have additional limitations, under the ASTM-DSRC Standard [39], mainly:

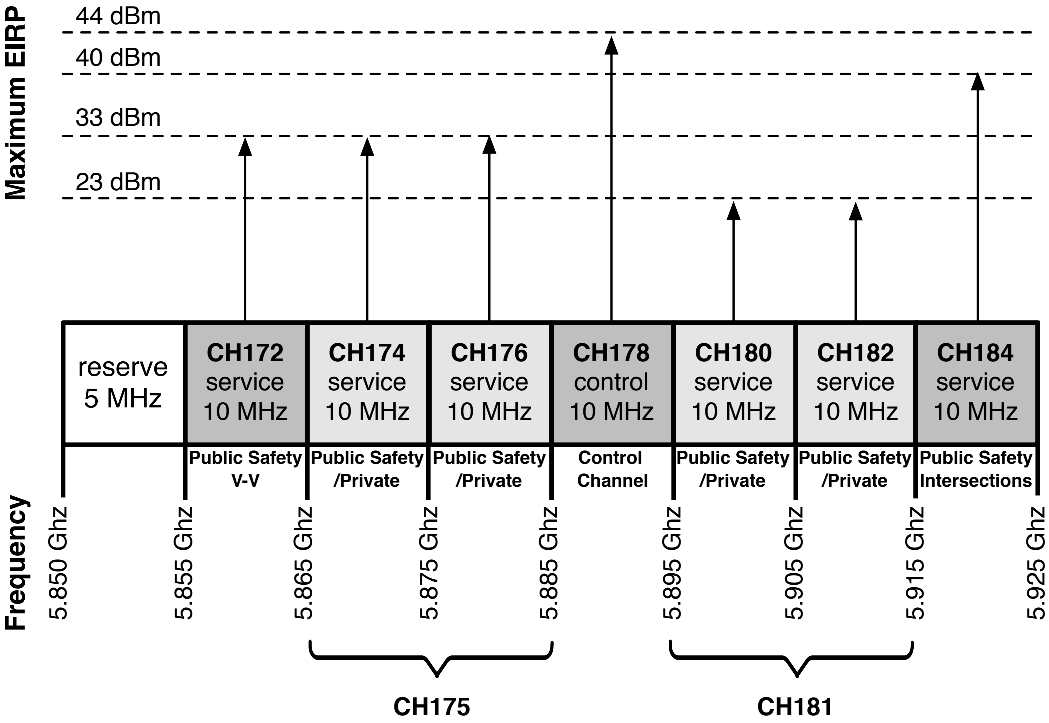

Figure 2.2: DSRC channels

- Public Safety and Private RSU installations operating in DSRC Channels 172, 174, 175 and 176 are used to implement small and medium range operations, RSU installation transmissions in DSRC Channels 172, 174, 176 shall not exceed 28.8 dBm antenna input power, and 33 dBm EIRP. RSU installation transmissions in DSRC Channel 175 shall not exceed 10 dBm antenna input power and 23 dBm EIRP.

- Public Safety RSU Installations transmission in DSRC Channel 178 shall not exceed 28.8 dBm antenna input power and 44.8 dBm EIRP. Private RSU installation transmission in DSRC Channel 178 shall not exceed 28.8 dBm antenna input power and 33 dBm EIRP.

- DSRC Channels 180, 181, and 182 are used to implement small zone operations. Public Safety and Private RSU installations in these DSRC channels shall not exceed 10 dBm antenna input power and 23 dBm EIRP. These installations shall use an antenna with a minimum 6 dBi gain. Interfering emissions from an RSU installation in these channels shall not exceed a maximum received power level of -76 dBm at 15 m from the installation being evaluated. The received power level is measured at 1.2 m above the ground with a 0 dBi antenna.

- Public Safety RSU and OBU operations in DSRC Channel 184 shall not exceed 28.8 dBm antenna input power and 40 dBm EIRP. Private RSU operations in DSRC Channel 184 shall not exceed 28.8 dBm antenna input power and 33 EIRP.

- Public Safety OBU operations in DSRC Channels 172, 174, and 176 shall not exceed 28.8 dBm antenna input power and 33 dBm EIRP. Public Safety OBU operations in DSRC Channel 175 shall not exceed 10 dBm antenna input power and 23 dBm EIRP.

- Public Safety OBU operations in Channel 178 shall not exceed 28.8 dBm antenna input power and 44.8 dBm EIRP.

- RSU and OBUs shall transmit only the power needed to communicate over the distance required by the application being supported.

2.1.2 *Medium Access Layer*

OBUs and RSUs form VANET, which use the IEEE 802.11p media access control (MAC) standard, which is an amendment to the IEEE 802.11 and 802.11a standards. This MAC protocol coordinates channel access for multiple devices. IEEE 802.11p adopts the IEEE 802.11 Distributed Coordination Function (DCF) [42], which allows different devices to contend for the channel using Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).

The concept of basic access method in DCF is depicted in Figure 2.3 Before an OBU is able to send a packet, the channel must be sensed idle for a period known as the Distributed Inter-Frame Space (DIFS). If the channel becomes busy during that period, the access to the channel is deferred. To reduce the probability of collisions as the result of more than one unit finding the channel idle, a random back-off is initiated, i.e., units defer access to the channel for extra randomly selected slots.

Table 2.1: DSRC peak power limits

CH	**Operation**	**Public Safety**		**Private**	
		Input Power (dBm)	EIRP (dBm)	Input Power (dBm)	EIRP (dBm)
172	RSU	28.8	33	28.8	33
	OBU	28.8	33	28.8	33
174	RSU	28.8	33	28.8	33
	OBU	28.8	33	28.8	33
175	RSU	10	23	10	23
	OBU	10	23	10	23
176	RSU	28.8	33	28.8	33
	OBU	28.8	33	28.8	33
178	RSU	28.8	44.8	28.8	33
	OBU	28.8	44.8	28.8	33
180	RSU	10	23	10	23
	OBU	n/a	n/a	n/a	n/a
181	RSU	10	23	10	23
	OBU	n/a	n/a	n/a	n/a
182	RSU	10	23	10	23
	OBU	n/a	n/a	n/a	n/a
184	RSU	28.8	40	28.8	33
	OBU	28.8	40	28.8	33

2.1.3 *Basic Safety Message*

According to the SAE J2735 standard [40], the BSM is used in a variety of DSRC Safety Applications to exchange safety data containing a vehicle's state. The BSM is typically broadcast at a transmission rate of 10 messages per second to surrounding vehicles. A BSM consists of two parts. The first part is required and contains data included in every BSM. The second part is optional and includes additional information for certain applications.

As can be seen in Table 2.2, the required part of the BSM message contains the following fields: *DSRC_MessageID* is the first value in the BSM message and is used to define the message type, and to inform the receiving application how to interpret the remaining bytes. *MsgCount* is used to sequence messages that were sent by the same sender with the same *DSRC_MessageID*. *TemporaryID* is used to identify the local vehicles that are interacting during an encounter. The value will periodically change to ensure the overall anonymity of the vehicle. *DSecond*

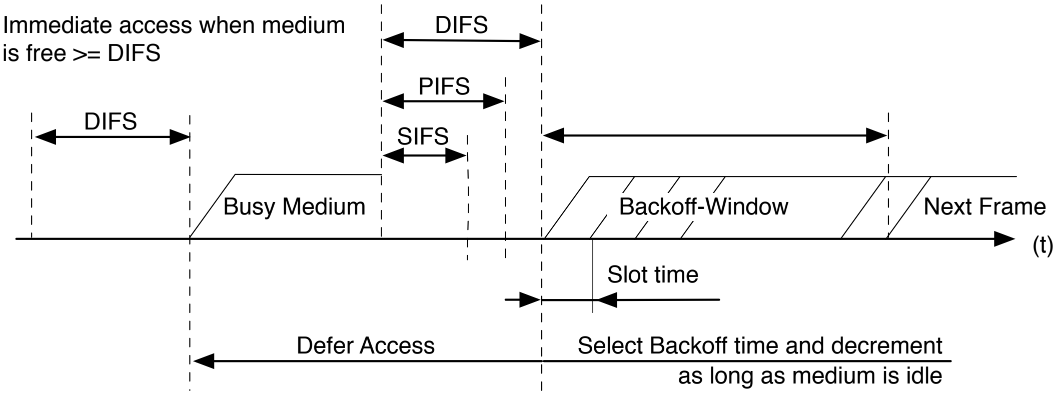
Immediate access when medium is free >= DIFS
DIFS
PIFS
SIFS
DIFS
Busy Medium
Backoff-Window
Next Frame
(t)
Slot time
Defer Access
Select Backoff time and decrement as long as medium is idle

Figure 2.3: Basic access method [43]

provides current timing information, and is a simple value consisting of integer values representing the milliseconds within a minute. *Latitude* and *Longitude* provide the geographic latitude and longitude of an object, expressed in $1/10^{th}$ integer micro degrees. *Elevation* represents the geographic position above or below the sea level. *PositionalAccuracy* consists of multiple parameters to represent the accuracy of the geographic position with respect to each axis. *TransmissionAndSpeed* expresses the current speed value in unsigned units of 0.02 meters per second combined with a value to represent vehicle's transmission state. *Heading* provides the current heading and the orientation of the vehicle. *SteeringwheelAngel* expresses the rate of change of the angel of the steering wheel in either direction. *AccelerationSet4Way* provides acceleration values in 3 orthogonal directions, in addition to yaw rotation rates. *BrakeSystemStatus* provides information about current brake system status, (brake usage, anti-lock brake status, auxiliary brake status), in addition to system control activity of the vehicle. Lastly, *VehicleSize* indicates the vehicle length and width.

2.2 SAFETY APPLICATIONS

A number of DSRC Safety Applications, envisioned to warn drivers of imminent dangers have been described in [52] and shown in Table 2.3. These applications use BSMs [40] to exchange information about the status of the vehicle, such as speed, GPS location, elevation, heading, acceleration and brake status. As mentioned

Table 2.2: Basic Safety Message BSM contents

– Part I, sent at all times				
Field	**Type**	**Name**	**Description**	**Size**
msgID	data element	DSRCmsgID	used in each message to define which type of message follows from the message set defined by the standard	1 Byte
msgCnt	data element	MsgCount	used to provide a sequence number within a stream of messages with the same DSRCmsgID and from the same sender	1 Bytes
id	data element	TemporaryID	used to as a means to identify the local vehicles that are interacting during an encounter, this value for a mobile OBU device will periodically change to ensure the anonymity of the vehicle	4 Bytes
secMark	data element	DSecond	used to represent the point in time when the message was generated, consisting of integer values from 0 to 60999 to represent the milliseconds within a minute	2 Bytes
– pos				
laat	data element	Latitude	represents the geographic latitude of an object, expressed in l/ loth integer micro degrees	4 Bytes
heading	data element	Longitude	represents the geographic longitude of an object, expressed in l/loth integer micro degrees.	4 Bytes
elev	data element	Elevation	represents the geographic position above or below the reference ellipsoid	2 Bytes
accuracy	data element	PositionalAccuracy	uses various parameters of quality to model the accuracy of the positional determination with respect to each given axis	4 Bytes
– motion				
speed	data frame	TransmissionAndSpeed	expresses the speed of the vehicle in unsigned units of 0.02 meters per seconds combine with 3 bit transmission state	2 Bytes
heading	data element	Heading	conveys current heading of the sending device, expressed in unsigned units of 0.0125 degrees from North	2 Bytes
angle	data element	SteeringWheelAngle	the angle of the steering wheel, expressed in a signed (to the right being positive) value with units of 1.5 degrees and occupying one byte	1 Byte
accelSet	data frame	AccelerationSet4Way	a set of acceleration values in 3 orthogonal directions of the vehicle and with yaw rotation rates, expressed as an octet set.	7 Bytes
– control				
brakes	data frame	BrakeSystemStatus	conveys a variety of information about the current brake and system control activity of the vehicle	2 Bytes
– basic				
size	data frame	VehicleSize	represents the vehicle length and vehicle width in a three byte value	3 Bytes
– Part II, sent as required				
safetyExt	data frame	VehicleSafetyExtention	used to send various additional details about the vehicle, such as Event Flags, Path History and PathPrediction	variable
statys	data frame	VehicleStatus	used to relate specific items of the vehicle's status, typically these are used in data event snapshots which are gathered and periodically reported to an RSU or as part of the BSM Part II content	variable

before, BSMs are generated periodically every 100 ms by each vehicle and broadcast in all directions.

Several high impact Safety Applications will be described using Figure 2.4.

Forward Collision Warning (FCW), depicted in Figure 2.4a), warns the driver of HV in case of an imminent rear-end collision with RV, driving ahead in the same lane and direction. FCW is useful in scenarios when approaching a vehicle that is decelerating or stopped.

The *Emergency Electronic Brake Lights* (EEBL) application, shown in Figure 2.4b), is a milder version of the FCW, which allows the driver of the HV to decelerate once receiving information from a RV that it is braking hard. This is most useful when the HV driver's line-of-sight is obstructed, e.g., by a large vehicle.

The *Do Not Pass Warning* (DNPW) in Figure 2.4c) warns to the driver of the HV during a passing maneuver attempt that another vehicle is traveling in the opposite direction.

The *Blind Spot Warning + Lane Change Warning* (BSW+LCW) Safety Application in Figure 2.4d) warns the driver of the HV attempting to change into a lane, which happens to be occupied by another vehicle traveling in the same direction, but is in its blind-spot.

The aforementioned DSRC Safety Applications rely all on the BSM messages from the RV. Should the HV not receive any or sufficiently frequent BSM messages, the application may not be reliable.

Table 2.3: Safety Applications and traffic accidents

	Crash Scenarios Safety Applications	**EEBL**	**FCW**	**BSW**	**DNPW**	**IMA**	**CLW**
1	Lead Vehicle Stopped		X				
2	Control Loss without Prior Vehicle Action						X
3	Vehicle(s) Turning at Non-Signalized Junctions					X	
4	Straight Crossing Paths at Non-Signalized Junctions					X	
5	Lead Vehicle Decelerating	X	X				
6	Vehicle(s) Changing Lanes - Same Direction			X	X		
7	Vehicle(s) Making Maneuver - Opposite Direction					X	

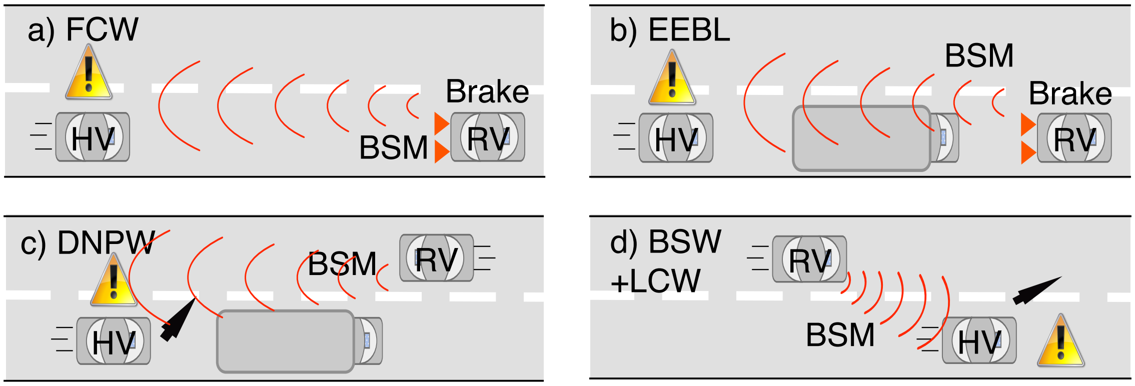

Figure 2.4: Safety Applications scenarios

2.2.1 *Safety Applications: Emergency Electronic Brake Lights*

The DSRC Safety Application selected for demonstration in this dissertation is the EEBL application. According to [40] and [52], when a vehicle brakes hard, the EEBL Safety Application communicates this event to surrounding vehicles via one or more BSMs. The Safety Application helps drivers following the vehicle emitting the event by generating an early notification that the lead vehicle is braking hard. This is especially useful if the driver's visibility is impaired, e.g., due to low visibility as the result of poor weather conditions or a vehicle in line of site. SAE J2735 standard [40] further states that it is assumed that the vehicle braking hard is equipped with a DSRC unit and that the message from the vehicle is received by the following vehicles, specifically vehicles in relevant positions. The following describes the flow of events. Upon hard braking, the lead vehicle sends a BSM with additional information about the hard braking event, such as a hard-braking event flag, deceleration, and brake pressure. The following vehicles receive and process the message and infer that the message is relevant, i.e., it refers to a similar heading in advance of the lead vehicle's path, where a hard braking event is taking place. The receiving vehicle warns the driver about the braking event and its severity.

2.3 FAULT MODELS

In the field of fault-tolerance, a *fault* is a physical defect, imperfection, or flaw that occurs in some hardware of software component [76]. This flaw can result in an *error*, which is the manifestation of the fault. An error on the other hand may result in the *failure* of a component or system. The relationship between fault, error and failure is shown in Figure 2.5 and is further described in [76] and [8].

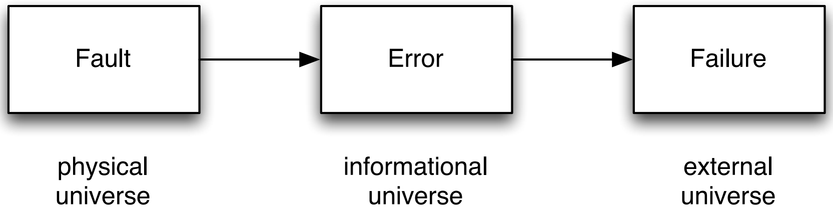

Figure 2.5: The relationship between fault, error and failure

One may say that "not all faults are created equal", as faults may exhibit different behaviors, which in turn may have different consequences for a system. The term *Fault Model* is generally used to describe taxonomies of faults. They help us understand the differences between faults based on their behavior, identify the potential impact on the system and guide us in identifying appropriate methods for dealing with faults or mixtures thereof.

In general, all faults can be categorized into either malicious or benign [5]. *Benign* faults are self-evident, globally diagnosable fault. A typical example of this fault type is a crash fault, e.g., the power supply of a router failed. Every entity in a system can see that the router is down.

Whereas benign faults are self-evident, *Malicious* faults are not. They may be perceived differently by different nodes in a redundant system. Malicious faults are also know as Byzantine faults [4, 3]. Byzantine faults are difficult to deal with and it has been shown that $N \geq 3m + 1$ nodes are needed to deal with m malicious faults [3].

Mixtures of faults have been considered in *hybrid fault models*. In [5] a mix of benign and malicious faults were considered. Later, malicious faults were partitioned into symmetric or asymmetric faults [6]. A *symmetric* fault implies that the same faulty value was received by all nodes, whereas an *asymmetric* fault has no restrictions on fault behavior and thus different nodes may receive different values. An asymmetric fault is the classic Byzantine fault in [3].

The faults model of [2], shown in Figure 2.6, further refined symmetric and asymmetric faults into *transmissive* and *omissive*. Specifically, a *Transmissive Symmetric* faults occur when the same erroneous value is delivered to all nodes. This fault is the symmetric fault in [6]. On the other hand, *Omissive Symmetric* faults are caused by the inability of the sender to deliver any value to any nodes. Thus no node received a value. The difference between benign faults and omissive symmetric faults is that the latter is not globally diagnosable, i.e., the receiving node does not know whether or not the omission was detected by all other receiving nodes.

Omissive and transmissive behavior of asymmetric faults is different. For instance, a sender may deliver a correct value to some nodes and no value at the other nodes, which in turn select a default value. This is called a *Strictly Omissive Asymmetric* fault. It should be noted that no faulty value was sent at all, but that the asymmetric behavior is due to the different values, as if a node had sent the correct value to some nodes and the default value to the others.

A *Transmissive Asymmetric* fault is the classic Byzantine fault, i.e., no restrictions are made on the values received by different nodes.

The fifth-fault hybrid fault model of [2] will be the basis for this research. Of special interest is the strictly omissive asymmetric fault, as it will be shown to be relevant in the case of jamming communication between vehicles.

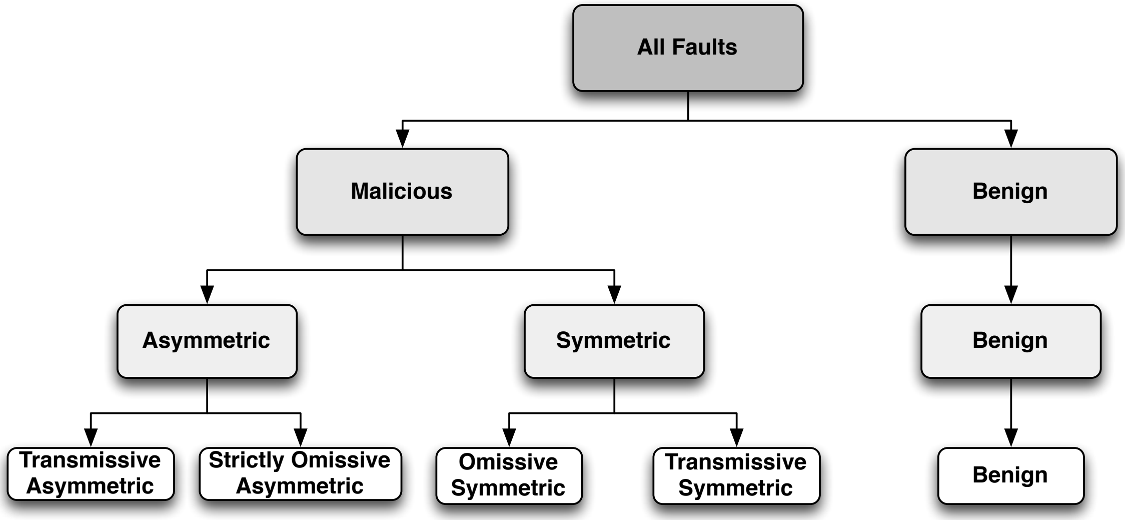

Figure 2.6: Fault taxonomy based on the hybrid fault model

2.4 MALICIOUS ATTACKS: WIRELESS JAMMING

Wireless jamming is a common attack in wireless communication, which can be launched using off-the-shelf equipment to interfere or block legitimate transmission by emitting radio signals that interfere with the communication. As a consequence, nodes are blocked and are no longer able to communicate with each other inside the jammed zone. Jamming can take several forms, commonly targeting the physical layer or creating a denial of service. The wireless medium is shared by nature, and the signals transmitted in this medium are susceptible to noise.

Jamming, which is the fault source addressed in this research, is the act of emitting radio signals that interfere with the intended communications. Different jammer types have been introduced and characterized in [51, 74], ranging from constant jammers, which constantly disrupt communication brute force, to intelligent jammers that are protocol-aware and able to target specific data or control packets.

It should be noted that usual jamming mitigation techniques, such as those based on spread spectrum, are not applicable in DSRC, as the channels are fixed in their spectrum and the safety channel, which is Channel 172, is dedicated to DSRC Safety Applications [39].

Several types of jammers have been defined, based on their behavior [51, 74]:

Constant Jammer: This type of jammer simply emits radio signals continuously (e.g. random noise), which interferes with the signal, i.e., it decreases the signal-to-noise ratio. The constant jammer has the most damaging impact, capable of causing large blind spots, since it can block communication entirely. However, it is relatively easy to detect, and is considered energy inefficient.

Random Jammer: This kind of jammer also operates at the physical layer, however unlike the constant jammer, it alternates between random periods of jamming and sleeping. This jammer type is more difficult to detect and consumes less energy.

Reactive Jammer: This jammer listens to the channel continuously and starts emitting noise once activity is sensed. It it difficult to detect, as it only operates during legitimate transmissions.

Deceptive Jammer: A deceptive jammer causes a Denial of Service (DoS) by not following MAC layer access rules. It continuously sends out bogus packets that appear to be legitimate, thus causing the channel to appear indefinitely busy for legitimate nodes. As opposed to the constant, random and reactive jammers, the deceptive jammer does not send noise, e.g., white noise or random bits, but validly formed packets.

Intelligent Jammer: This is a protocol-aware jammer that has the ability to analyze ongoing traffic. Thus, it can target only specific packets or packet types. Once a desired packet is sensed, the intelligent jammer can inject enough noise to corrupt these packets. This is the most sophisticated jammer and it is extremely difficult to detect [51].

Our focus in this research is on constant and deceptive jammers, which are considered the most disruptive as they indiscriminately affect all ongoing communication. In addition we will study the impact of those jammers on the communication of DSRC Safety Applications.

Some of the common metrics to identify jamming are as follows:

- *Packet Delivery Ratio* (PDR) is measured at the receiver and is the ratio of the number of packets sent to the number of packets correctly received during a time window.

- *Carrier Sensing Time* is measured at the transmitting node and measures the total waiting time before the medium becomes idle.

- *Signal Strength* is a measure of signal power at the receiver side, since signal power levels are affected by abnormal interference, e.g., jamming.

- *Signal-to-Noise Ratio* (SNR) is the ratio of signal and noise power levels.

- *Signal-to-Jamming Ratio (SJR)* is defined analogously as the SNR. Typically the SNR or SJR can be used to determine the packet error probability, which in turn can be used to determine the PDR.

2.5 RELIABILITY OF SAFETY APPLICATIONS

As indicated before, the ITS is a critical infrastructure, and any benign or malicious fault could have far-reaching consequences. Thus, reliability, security and survivability are of paramount importance. Failure of DSRC Safety Applications can have catastrophic consequences, e.g., injury or loss of life. At the core of DSRC Safety Applications is the reliability of BSMs, as they are the most important messages. Any attack or disruption of BSMs could cause failure of the Safety Applications.

Whereas standards such as the IEEE 1609.2 [45] address security mechanisms like authentication and encryption, they do not address willful disruption of communications due to jamming. Deterring jamming completely is most likely improbable [51]. However, minimizing its impact is achievable. This can be done by having detection mechanisms, which lead to situational-awareness in the presence of the jammer. Once jamming is confidently detected, the dependency on Safety Applications becomes unwise. Accordingly, our approach suggests jamming detection and consequent transition of the Safety Applications to a fail-safe mode. This could be achieved by notifying drivers that the applications are temporarily unavailable.

CHAPTER 3
Adaptive Threshold-Based Agreement Algorithm

Research has shown that threshold-based agreement methods effectively reduce the impact of value faults through validating events, by receiving BSM from multiple sources [49, 50]. Whereas previous work considered value faults, e.g., injection, data fabrication and sensor manipulation, it does not address the impact of omission faults and jamming.

This chapter investigates the impact of jamming on threshold-based agreement in VANETs. We show that jamming drastically reduces the correctness of the voted upon decision. We also consider the EEBL Safety Application, and demonstrate how jammer position and power affect the correctness of the decision. Furthermore we show how the number of vehicles impacts the correctness of decisions in the presence of jamming. Finally a new adaptive threshold algorithm is introduced that improves the resilience against jamming attacks compared to algorithms presented in previous research.

3.1 RELATED WORK

Schemes based on voting and information validation in VANET have been presented in [49, 50, 19, 53, 54]. The most relevant to the work presented here will be discussed in more detail.

In [49] the authors proposed four static agreement methods, which are based on voting schemes that enforce plausibility checks to reach a correct decision in the presence of value fault. The decision methods are *Freshest Message*, which take into account the most recent messages received, *Majority Wins*, which performs local voting over all received messages regarding a certain hazard, *Majority of Freshest X*, which is a combination of the previous two methods considering the recent *x* messages, and *Majority of Freshest X with Threshold*, which is an extension of the previous method in addition to a threshold check. Their work did not specifically take into account the choice of the number of messages.

In [50] agreement is accomplished by making the application wait for a number of BSMs before warning the driver, based on the decision method "majority of freshest messages with threshold" introduced by [49]. However their focus was on dynamic determination of the threshold. Choosing the value of the number of messages was established by dynamically choosing the threshold according to current neighborhood density within transmission range R. The dynamic methods have been further divided into *dynamic naive*, which chooses a threshold based on the number of one-hop neighbors at time t, *dynamic naive ahead*, which chooses a threshold based on the number of one-hop neighbors at time t ahead of the current vehicle, and *majority ahead*, where the threshold is determined by taking half of the number of one-hop neighbors plus one at time t ahead of the current vehicle. However, their work did not take into consideration omission faults.

In [53] the authors proposed a voting algorithm using the participation of vehicles to prevent malicious data manipulation, fabrication or modifying the functioning of a vehicle's On Board Equipment to carry out attacks. They take into consideration certain abuse cases such as false speeding, false congestion, false braking, false timing and position data and higher message frequency. Voting is based on a predetermined confidence value.

The work in this chapter considers the model of [49] and [50], which will be extended to consider the impact of jamming.

3.2 AGREEMENT IN VANET

In voting algorithms the selection of the correct threshold is essential. Selecting the threshold too low can increase the number of *false negatives*, i.e., the vote results in the faulty decision/value. Conversely, selecting the threshold too high results in high latency and exceeding safety time. The two methods for calculating the threshold have been discussed in the literature [49, 50] as static and dynamic thresholds. *Static* thresholds imply that the number of messages required for a decision is predetermined. The host vehicle waits for distinct number of messages regarding an event to be received. The decision to warn the driver or not is made by voting on what is being reported by the majority of vehicles. However, this method ignores variation in the neighborhood topology over time. As a result, the threshold might become insufficient in dense topologies, leading to premature decisions with high chance of false negatives. On the other hand, the threshold could become higher than required in sparse neighborhoods, which may also lead to undesired decision delay due to a lack of messages.

Dynamic threshold varies over time. Now the number of required messages is determined based on the number of vehicles in the surrounding neighborhood. However, the number of neighboring vehicles is taken without clear distinction of how the vehicles are positioned. This may lead to inaccurate threshold, because not all surrounding vehicles are witnessing the event. Even taking the number of vehicles ahead does not necessary grantee a correct threshold, because some ahead vehicles fall inside the transmission range, while being outside of the witnessing/detection area.

Jamming can impact the threshold selection. In the case of an event the subset of honest vehicles that detect the event will generate a true alert. However, due to jamming, one or more alerts may not be received by other vehicles. In fact, a malicious jammer may have a great advantage, e.g., by disrupting communication just after and event occurred. Furthermore this malicious event may have been coordinated with the jammer.

The general timing associated with threshold-based agreement is shown in Figure 3.1. The values associated with an event i, as they are extracted from BSM messages, are represented by the squares. These are the values received by the host vehicle running the DSRC Safety Application. Of special interest is the voting set, which contains the values received from the beginning of an event to the decision threshold. Again, the threshold is the number of message required before voting. This decision has to be made before time T_{safety}, which accounts for reaction and braking time.

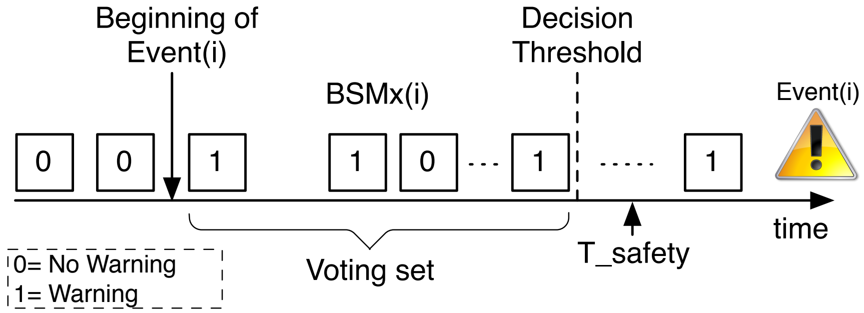

Figure 3.1: Threshold-based agreement using voting in VANET

In a pathological attack the coordinating adversaries would attempt to maximally stack faulty values into the voting sets. Then, as values from other vehicles that contradict the fault event arrive, a correct vote can be made once the number of correct values exceed the number of faulty values. An example of such pathological scenario is shown in Figure 3.2, where 35 faulty values were stacked into the voting set at time $t = 0$. Then correct messages arrive until the time by which the threshold is achieved. In the example the threshold was set to 75, which was met at $t = 0.6s$, and the voting set contained 35 faulty and 40 correct values. In the example, the voting value is of course decided when the 36^{th} correct value arrives.

Now assume a pathological malicious case where the time of an event is coordinated with the jammer. Just after the event and stacking of the voting set with false values, the jammer starts impairing communications of correct values. The scenario of Figure 3.2 now deteriorates to the scenario shown in Figure 3.3. Here the threshold would be set lower, as fewer message arrive, wrongly suggesting lower vehicle density. Voting at time $t = 0.8s$ now results in a false negative.

3.3 SYSTEM MODEL

The overall model associated with threshold-based agreement in VANET is based on the areal model used in [50] and will be explained using Figure 3.4 showing a single lane of traffic. Following and event i, e.g., stopped vehicle or approaching game, two distinct areas are considered, i.e., the detection and decision area. In the detection area, denoted by $D_{detect}(i)$, the driver of each Remote Vehicle RV_j, $1 < j < n$, either

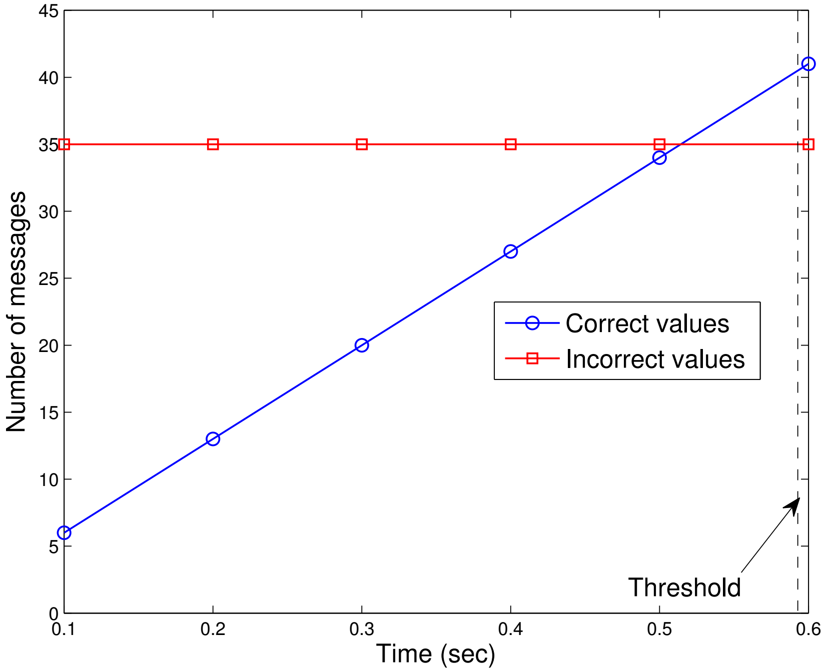

FIGURE 3.2: Reaching correct decision as correct values outvote incorrect values

has visual or autonomous sensing capabilities for detecting the hazard. The range of $D_{detect}(i)$ is bounded by the human vision and sensors capabilities, which in turn are subject to physiological and environmental conditions. In the decision area, denoted by $D_{decide}(i)$, each Host Vehicle HV_k, $1 < k < n'$, is distant from event i, but still within the transmission range R of RV_j. The group of vehicles RV_j located inside $D_{detect}(i)$ detect event i, e.g., the driver of the detecting vehicle brakes, thus triggering a $BSM_x(i)$ regarding event i, where x is a sequence number. $BSM_x(i)$ contains the information referred in Subsection 2.1.3, such as location, speed, deceleration rate and brake intensity (brake flag). $BSM_x(i)$ will be received by host vehicles HV_k inside $D_{decide}(i)$, as long as it is within the transmission range R of RV_j. Thus, after receiving $BSM_x(i)$, vehicle HV_k infers a hazard as long as it is relevant to its current position.

When considering agreement, HV_k will accept BSM messages from different sources until a threshold of α has been received, or before reaching the maximum safety time for making a decision, which is the sum of reaction time T_{react} and required time for braking T_{brake}.

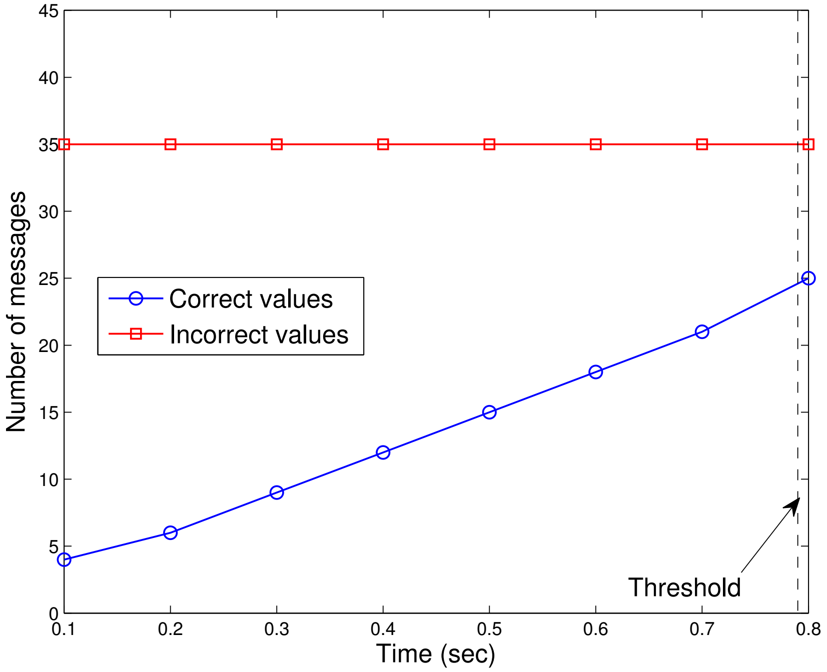

Figure 3.3: Reaching incorrect decision as incorrect values outvote correct values with support from jammer

3.3.1 *Attacker Model*

The attacker is assumed to be a constant jammer. It is stationary on the side of the road, targeting any HV_k in area $D_{decide}(i)$, as can be seen in Figure 3.5, where it is positioned to maximize its effect. As HV_k approaches the jammer, the impact of jamming becomes more severe, thereby increasing the packet error probability P_p. The distance of HV_k to the jammer has great impact on P_p.

Three different jammer positions have been examined in Figure 3.5. Positions A, B, and C are at the beginning, middle, and far-end of the decision area respectively. Our focus is on position A, as it gives the advantage to the jammer by being closer to HV_k at the time of event i. This increases P_p, thus decreasing the Packet Delivery Ratio at $D_{decide}(i)$ compared to the other two positions. The impact of the jamming power on the packet delivery ratio for the different positions is shown in Figure 3.6.

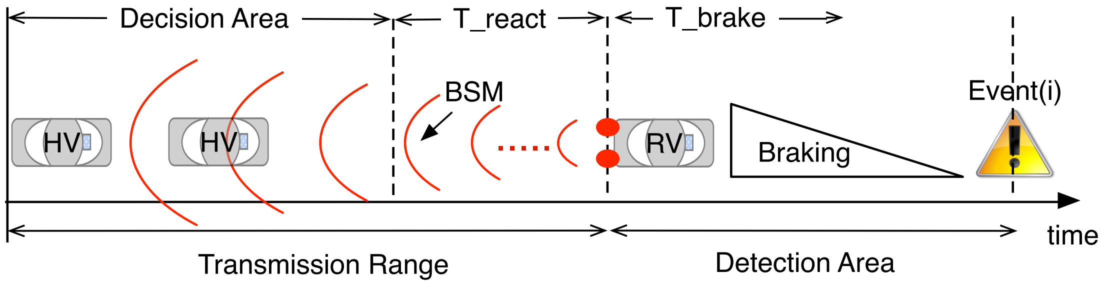

Figure 3.4: System model for EEBL Safety Application

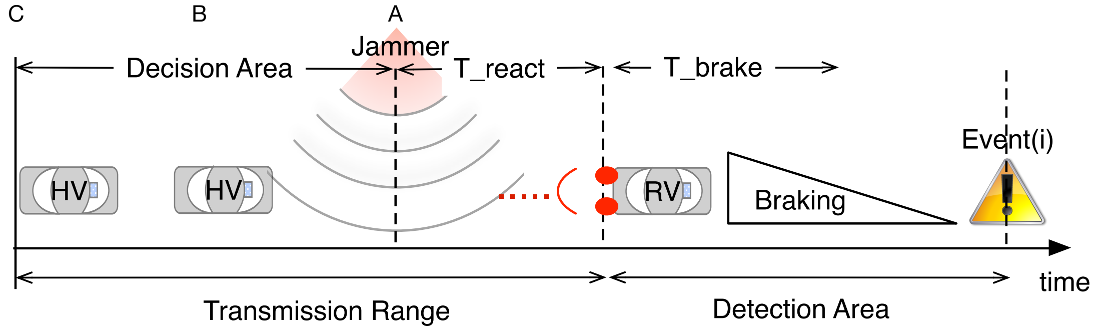

Figure 3.5: Attacker model for EEBL Safety Application

3.4 ADAPTIVE THRESHOLD ALGORITHM

We next present an adaptive threshold algorithm which has improved performance over those introduced in [49, 50]. The algorithm shown in Figure 3.7 allows HV_k to choose a threshold value $\alpha(t)$, defined below, based on the number of vehicles in the detection area $D_{detect}(i)$ at time t and before reaching T_{safety}. When HV_k receives a BSM message it first checks the location for relevance. If it is relevant to HV_k's current position and has not been recognized as a previous event, it checks the content for hazard inference, e.g., in the case of EEBL Safety Application it checks the brake flag. If a new hazard has been detected by HV_k, the algorithm initializes a new event location $i+1$, calculates T_{safety} based on HV's current speed and location, and further increases the RV count by one. The algorithm also proceeds with incrementing the warning counter and the total count of received BSM regarding the event by one, and the current time is checked against T_{safety}. If T_{safety} has been reached, a prompt decision must be made. Otherwise it checks whether it

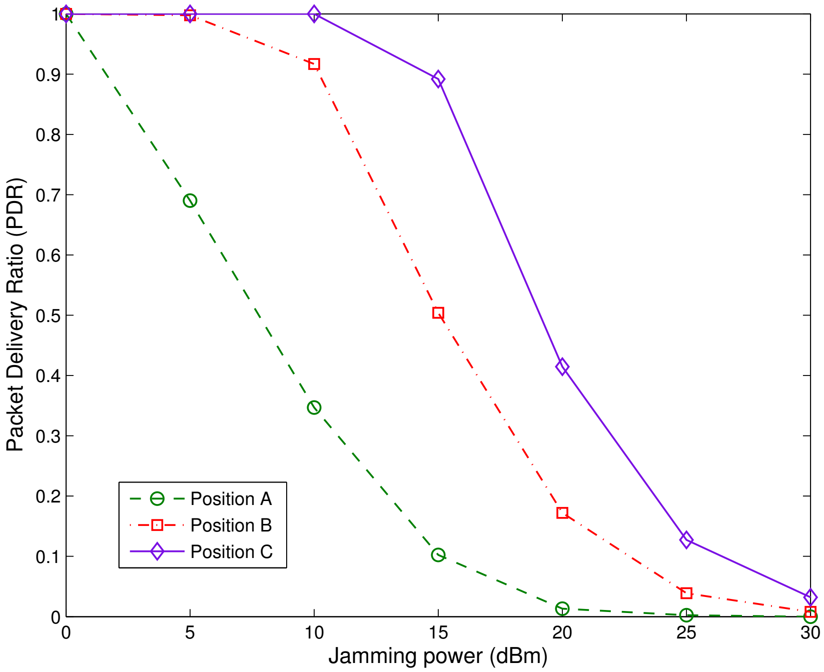

FIGURE 3.6: The impact of jammer position on the PDR in $D_{decide}(i)$

has received enough BSM messages to reach threshold $\alpha(t)$. If the check is true it initiates voting and makes a decision. The process is repeated in case there is still time to T_{safety} or the threshold has not yet met. Threshold $\alpha(t)$ is determined at time t based on the number of vehicles in $D_{detect}(i)$ by

$$\alpha(t) = P(\lambda) \times N(D_{detect(i)}(t)) \tag{3.1}$$

where $P(\lambda)$ is a percentage of the recent BSM arrival rate λ, and $N(D_{detect(i)}(t))$ is the number of vehicles in the detection area for event i at time t.

3.5 SIMULATION DETAILS

To test the algorithm presented in Section 3.4, we used a Matlab model consisting of two stages. The first stage involves generating traffic movement, where as the second stage calculates transmission and agreement. In this section we will describe the

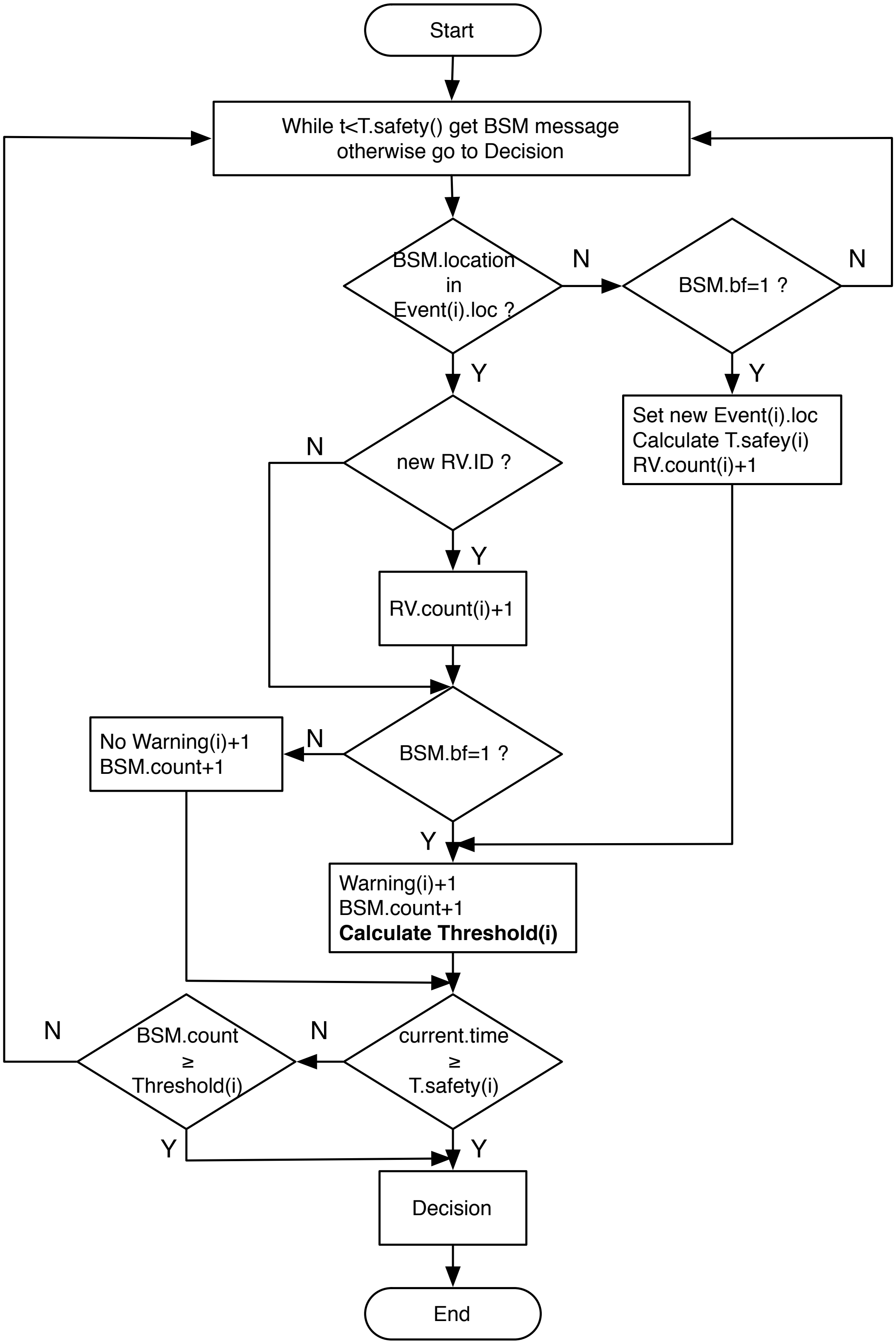

Figure 3.7: Adaptive threshold algorithm

simulation methodology, which involves, constant jammer model, mobility model (car following model) and MatLab functions.

3.5.1 *Constant Jammer Model*

The constant jammer can be modeled based on model provided in [63, 51]. The Signal-to-Jamming ratio (SJR) is calculated as follows,

$$SJR = \frac{P_t G_{tr} G_{rt} R_{jr}^2 L_j B_j}{P_j G_{jr} G_{rj} R_{tr}^2 L_r B_r} \tag{3.2}$$

where, the subscript j refers to the jammer, and r to the receiver and t to the transmitter. P_x is the transmission power of vehicle x, G_{xy} is the antenna gain from vehicle x to y, R_{xy} is the distance between vehicles x to y, L_r is the communication link's signal loss, L_j is the jamming signal loss and B_x is the vehicle's x bandwidth.

Considering, that the gains, the signal loss and the bandwidth for both transmitter and receiver are equal, Equation 3.2 can be simplified as

$$SJR = \frac{P_t R_{jr}^2}{P_j R_{tr}^2} \tag{3.3}$$

Note that DSRC uses Phase Shift Keying (PSK), we obtain the energy per bit and the Bit Error Rate (BER) for both 3 Mbps and 6 Mbps as

$$\frac{E_b}{N_0} = SJR \times \frac{B}{R} \tag{3.4}$$

where E_b/N_0 is the energy per bit to noise power spectral density ratio, B is the channel bandwidth in Hz, and R is the data rate in $bits/s$ [71]. The BER is now computed by

$$BER = \frac{1}{2} erfc\left(\sqrt{\frac{E_b}{N_0}}\right) \tag{3.5}$$

where *erfc* is the complementary error function. Finally, the packet error probability is

$$P_p = 1 - (1 - BER)^N \tag{3.6}$$

where N is the packet length in bits.

3.5.2 *Mobility Model: Car Following Model*

Traffic movement characteristics in our model are based on the Car-Following model [55], which is a *microscopic* traffic flow model. A microscopic traffic flow model represents microscopic properties like the position and velocity of single vehicles. The reason we chose a microscopic model is its ability to evaluates properties of the vehicles dynamics such as velocity and position of each vehicle. In contrast *macroscopic* traffic flow models evaluate traffic flow characteristics such as density, and mean speed of a the whole traffic stream.

For simplicity we used the first General-Motors car-following model [55], which assumes that the sensitivity of the driver is a constant α in any given situation.

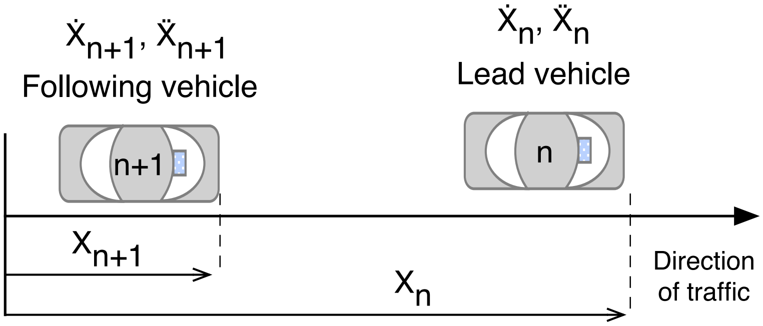

Figure 3.8: The Car-Following model

First the speed $\dot{X}_n$ and distance X_n of the lead vehicle are calculated using the equations 3.7 and 3.8

$$\dot{X}_n\,(t+T) = \dot{X}_n(t)\left[\frac{\ddot{X}_n\,(t) + \ddot{X}_n\,(t+T)}{2}\right]T \tag{3.7}$$

$$X_n\,(t+T) = X_n(t) + \dot{X}_n(t)T + \left[\frac{\ddot{X}_n(t) + \ddot{X}_n(t+T)}{2}\right]\left[\frac{T^2}{2}\right] \tag{3.8}$$

In equation 3.9 the acceleration $\dot{X}_{n+1}$ of the following vehicle is calculated, where ΔT is the reaction time and α is the sensitivity.

$$\ddot{X}_{n+1}\,(t+\Delta t) = \alpha\left[\dot{X}_n\,(t) - \dot{X}_{n+1}\,(t)\right] \tag{3.9}$$

As shown in Figure 3.8, a lead vehicle n and a following vehicle $n+1$ are initially stopped at time $t = 0$. Since the vehicle is initially stopped, the speed can be expressed as $\dot{X}_n(0) = 0$, and the distance from the starting point is $X_n(0) = 0$. We start by defining the behavior of the lead vehicle n, which implies the acceleration, the desired maximum speed and deceleration rate of the vehicle. Vehicle n is set to accelerate at a constant rate of $\ddot{X}_n$, until it reaches its maximum speed, and eventually brake at a certain point and start to decelerate. The values for the lead vehicle's acceleration (and deceleration) $\ddot{X}_n$ are preassigned over a certain period of time.

Using Equation 3.7, now we can calculate the speed of the lead vehicle n at time $(t+T)$, where T is the increment in time.

The position of the lead vehicle, i.e., distance from starting point, at time $(t+T)$ can be calculated using Equation 3.8.

Now, since we have the acceleration and speed of the lead vehicle, we can calculate the following vehicle's acceleration, which is denoted by $\ddot{X}_{n+1}$ using Equation 3.9, where Δt is the reaction time, and α is the sensitivity parameter. In our experiment we have selected $\Delta t = 1$ second, and $\alpha = 0.5$. These values are selected based on the suggested reaction times and sensitivity values provided in [55]. Therefore, the acceleration (and deceleration) of the following vehicle can be predicted for time $(t+T)$, and the speed $\dot{X}_{n+1}$, and the distance X_{n+1} of the following vehicles can be calculated using Equations 3.7 and 3.8.

3.5.3 *MatLab Functions*

Using the MatLab code provided in Section A.1, we have automated the car following model to generate mobility for N following vehicles in one lane. The *mobility function*, first calculates the speed and distance for the lead vehicle based on the parameters defined by the user, i.e., the time increment T, the overall time for the simulation *max_time*, the rates for *acceleration* and the *deceleration*, the maximum speed *max_speed* and braking times *Tbrake_start* and *Tbrake_end*. Once the acceleration/decoration and distances for lead vehicle movement are calculated and placed in a matrix, the mobility function will proceed with predicting the movement for the following vehicles. The mobility function returns a matrix that contains the exact speed, acceleration and position and relative distances for all vehicles for the entire simulation time.

The communication between vehicles and transmission of BSMs is calculated using the *transmission function* described in Section A.2. The output of the mobility function is used as an input for the transmission function. The PDR will be calculated for specific or group of vehicles can be obtained based on the distance between the vehicles and the BER. Note that this function, assumes normal transmission conditions without the presence of the jammer.

For jamming scenarios, we use the functions described in Section A.3 and A.4. The impact of jamming is calculated based on the model presented in Subsection 3.5.1.

Finally, the *agreement function* described in Section A.5 uses the concepts of the agreement algorithm discussed in Section 3.4. The function utilizes the mobility and transmission functions as inputs, and returns the the percentage of false negatives based on the number of faulty decisions for the static, dynamic and adaptive thresholds.

3.6 PERFORMANCE EVALUATION

As was introduced in Section 3.5, the performance of the new adaptive threshold algorithm was compared against the algorithms in [49, 50] using a two-stage model, i.e., the "car following mobility model" of [55] as input to Matlab, which calculated the false negative rates based on the jamming and communication model of [64]. The evaluation was for the EEBL application in a single lane road attacked by a jammer with specifications equal to an OBU. Further assumptions were that BSM messages cannot be forged and that transmission errors due to collisions are negligible due to the overall low traffic density. The simulation parameters were set according to Table 4.1.

Figure 3.9 shows the effect of jamming on the decision making process for the new adaptive threshold algorithm, the static threshold algorithm of [49] with thresholds 10 and 20, and the dynamic algorithm of [50]. Jamming power ranged from 5 dBm to 30 dBm; 0 dBm represents the case without jamming. The traffic density

Table 3.1: Simulation parameters

Simulation software	Matlab
Simulation duration	120 *sec*
Transmission range	300 *m*
Number of vehicles	5-55 vehicle/*km*
Vehicle speed	15 *m/sec*
Reaction time	1 *sec*
BSM generation	every 100 *msec*
Effective bandwidth	8.3 MHz
Data rate	6 Mbps
Transmitter power	20 dBm
Jammer power	5-30 dBm

was fixed at 45 vehicles/km. It can be seen that all algorithms are very sensitive to the impact of jamming. However, the dynamic and the adaptive algorithms show the highest resistance against this impact, with modest advantage of up to 5% to the adaptive algorithm.

One may ask the question about the usefulness of the algorithms if they are so affected by jamming. The answer however is that if the impact of jamming is high, jamming detection can be used to steer the application to a fail-safe mode. That is, if jamming is detected the application can alert the driver about the unavailability of the application. It is the lower powered jamming that is harder to detect, and that is the range in which the algorithms are most useful. The false negative rates at 0 dBm are due to vehicles in the decision area, specially those at the back end, that fall outside of the transmission range of some vehicles at the very front of the detection area. However, vehicles at the backend of the decision area would still receive alert messages, but not enough to reach the static threshold, hence resulting in high false negative. Figure 3.10 shows the effect of vehicle density on different threshold algorithms with jamming power fixed to 10 dBm. When traffic is sparse the chances of making faulty decisions is the highest. This is due to larger inter-vehicle spacing, and thus vehicles in the decision area are more affected by jamming. This is because of the jammer's proximity to the host vehicle in comparison to other remote vehicles in the detection area. The result is that the number of messages being received by the host vehicle is insufficient, which in consequence results in higher

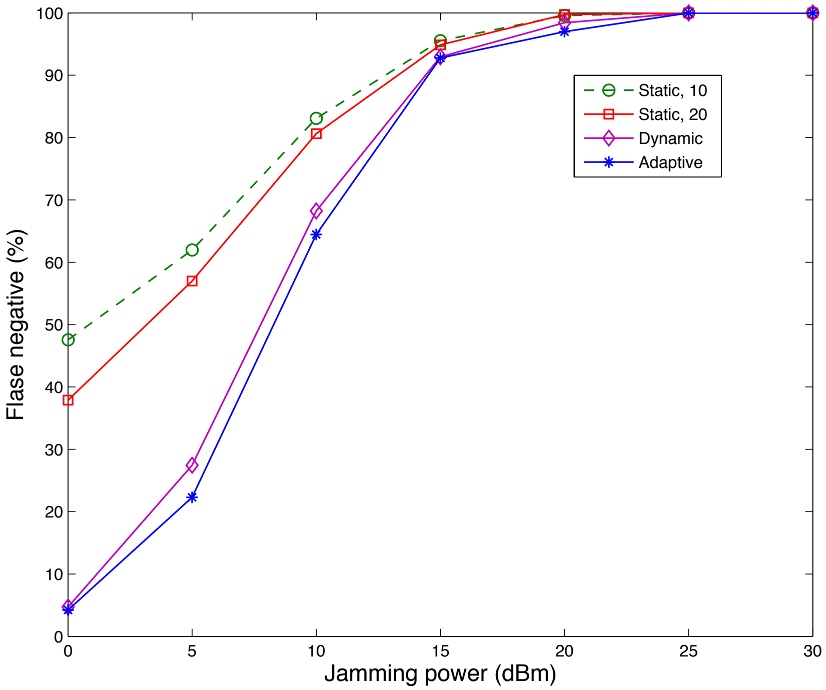

Figure 3.9: The effect of jamming power on threshold algorithms

false negative rates. As the traffic becomes more dense, the decisions improve even in the presence of moderate jamming. The adaptive algorithm performs modestly better in all situations, i.e., up to 4%. As in the discussion of the previous figure, the high false negative rate in the presence of jamming highlights the need for jammer detection. It should be noted that the false negative rate at a vehicle density of 45 vehicles/km also appears in Figure 3.9 for 10 dBm jamming power.

3.7 Conclusions

DSRC Safety Application reliability was investigated in ITS subject to benign and malicious faults. In order to minimize faulty decisions made by DSRC Safety Applications about events, e.g., detection of – and reaction to hazards, agreement has been found to improve detection of fault event notification, such as warnings or revocation thereof. This chapter investigated the impact of jamming on threshold-based agreement algorithms, such as static, dynamic, and adaptive algorithms. It

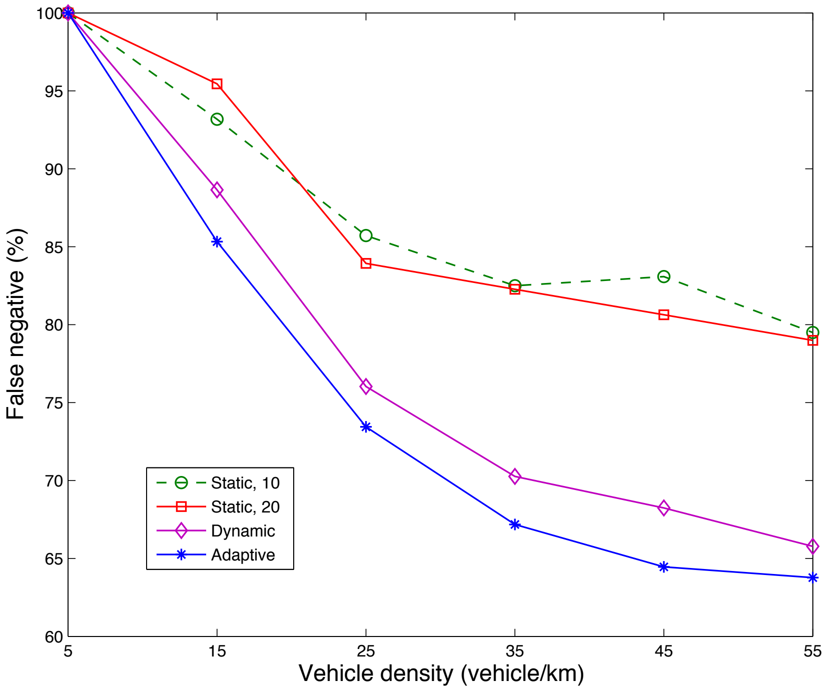

FIGURE 3.10: The effect of vehicle densities on agreement algorithms

was shown that constant jamming can drastically decrease the decision quality for these threshold-based agreement algorithms. A new adaptive threshold algorithm was presented that provides higher resilience against jamming.

The performance of the new adaptive threshold algorithm and its resilience against jamming were investigated using the Electronic Emergency Brake Lights Safety Application defined in the VSC-A project and J2735 standard. The new algorithm was shown to outperform its counterpart, due to adaptively adjusting the voting thresholds. Whereas the observed improvements were by modest 2-5%, these improvement should be seen in the context of saving lives. While threshold-based agreement algorithms in VANETs are effective in the presence of faulty nodes or low power jamming, they deteriorate as the jamming power increases. Specifically, the observations of the false negative rates when the EEBL application was subjected to jamming with higher power levels suggest the need for jamming detection in order to transition the application to a fail-safe state.

CHAPTER 4
On the Design of Jamming-Aware Safety Applications in VANETs

In this chapter, we propose a new jamming-aware algorithm for DSRC Safety Application design for VANET that increases reliability using jamming detection and consequent fail-safe behavior, without any alteration of existing protocols and standards. The impact of deceptive jamming on data rates and the impact of the jammer's data rate were studied using actual field measurements. Finally, we show the operation of the jamming-aware algorithm using field data.

4.1 RELATED WORK

There are many papers that discuss the topic of jamming detection in wireless networks, including wireless sensor networks (WSN), mobile ad hoc networks (MANET) and 802.11, however little research discusses detection schemes designed specifically for VANETs, which impose different requirements as will be explained in Subsection 4.1.2. Besides their application domain, e.g., WSN, MANET or VANET, research efforts can be partitioned into jamming prevention and jamming detection. A general overview of jamming attacks in wireless networks based on jamming prevention and jamming detection is given in [51].

4.1.1 *General Wireless Networks*

Prevention:

Some typical mechanisms for jamming prevention are Frequency Hopping, Channel Surfing, Spread Spectrum, and Spatial Retreats [56, 57]. Frequency Hopping, Channel Surfing, and Spread Spectrum operate at the physical layer and are not effective in VANETs, because the channels are pre-assigned and fixed in their spectrum according to the ASTM E2213-03 standard [58]. Thus, any mechanisms that require modifications on the physical layer would imply deviating from the existing WAVE standards. Spatial retreat helps mitigate jamming by moving nodes outside the affected area. However, in VANET this is generally not applicable as the geometry of the roads are fixed. Diverting traffic to use other roads is at a much higher level of granularity.

Other research uses directional antennas [59], or coding such as Low Density Parity Check (LDPC) [60], or redundant encoding [61]. Directional antennas take advantage of sectored or smart antennas, which produces more focused beams between transmitter and receiver. This will increase the antenna gain and potentially overpower jamming signals. However, in VANETs antennas are omni-directional, uniformly emitting power in all directions to broadcast to surrounding vehicles [52].

Detection:

Jamming detection methods vary according to the different types of jammers, e.g., constant, deceptive, reactive, random and intelligent. Some of these methods depend on metrics such as Signal Strength, Carrier Sensing Time or Packet Delivery Ratio, which may be measured or averaged from the network over time. Jamming is detected once a significant deviation from normal behavior is sensed. A single metric is not enough to confidently differentiate jamming situations from other normal situations, where deviations in performance could be due to network conditions such as congestion or failure at the sender side [74]. Thus, to increase the jamming detection probability, [74] proposed schemes that combine metrics, namely by combining signal strength with packet delivery ratio, or combining location information with the packet delivery ratio. These two methods were used in consistency checks, and effectively increased the probability for detecting the presence of a jammer. Whereas this work addresses general wireless networks, the overall idea also applies to VANETS. We will leverage this general strategy in our jamming-aware algorithm by also using multiple metrics.

In [62] an approach was presented where individual nodes maintained lists of observed communication behavior. These lists were consequently exchanged with neighboring nodes in order to determine abnormal behavior, e.g., jamming. However, such an approach is not suitable in the fast-changing topology of VANET. In fact, any detection mechanism intended for VANET needs to 1) adapt quickly to topology changes, and 2) detect jamming in a timely manner. These two requirements eliminate detection methods that require multi-hop data exchanges among nodes.

4.1.2 *Related VANET Research*

The impact of jamming on DSRC has been investigated at different levels. Since our interest is in DSRC Safety Applications, we focus our attention at the Safety Application level. Specifically, we focus on solutions that conform to the existing standards, rather than consider mechanisms that go beyond these standards. Diverse solutions are proposed in the literature. In [63] the impact of constant, random, and intelligent jamming on DSRC Safety Applications is shown for homogeneous channel behavior, where signal-to-jamming ratios were the basis for packet error probabilities. Different redundancy schemes are introduced in an attempt to increase resilience against jamming. This is extended in [64] to consider the impact of jamming on different data, and the effect of channel power in [65]. While these approaches appear to be effective, the redundancy consumes additional bandwidth, thereby limiting use by other DSRC applications. Furthermore, the research did not not deal with challenges such as MAC layer efficiency, processor utilization, channel congestion and fail-safe operation of the Safety Applications.

In [66], the authors demonstrate that constant, periodic and reactive jamming could cover certain areas in which its effect is temporary and vanishes as vehicles traverse through the plagued region. Once jamming levels reach certain thresholds, communication is no longer possible. This implies that jamming-unaware applications will not work anymore once certain jamming thresholds are exceeded. It is therefore crucial to have efficient jamming detection, e.g., a jamming state. This makes it possible to switch the Safety Application to a fail-safe state. Alternatively, a more refined state model may be used, allowing different states, based on the severity or possible impact of jamming, e.g., considering the criticality of the Safety Applications.

A solution for VANET based on Correlation Coefficient, by measuring dependance among periods of error and correct reception times, is proposed in [67].

The method only considers reactive jamming, i.e., the jammer transmits only after sensing legitimate activity. The approach uses only the Error Probability as a metric, which is not sufficient to conclude jamming [74].

Jamming in platoons is addressed in [68], where a simple algorithm for real-time detection in VANET based on so-called beacons is given. However, this approach is for the specific case of platoons of vehicles only.

The authors in [69] propose a solution to detect jamming based on the PDR and its rate of change. However, depending on PDR alone is not sufficient as the change in PDR can be a result of factors other than jamming, e.g., poor link quality due to large distance between sender and receiver [74].

In [70] it is argued that detection methods that depend on metrics such as Received Signal Strength Indicator (RSSI), relative position, or PDR, could reveal the presence of jamming as long as there are messages being received. Thus, when the PDR drops to 0% these metrics may no longer be available. Hence, jamming detection strategies that depend on receiving these metrics may simply fail.

To counter this effect, our proposed solution uses path prediction to infer future locations using messages received prior to entering a jammed zone. Thus it can estimate future distances and PDR based on normal, prior, behavior as will be explained next.

4.2 DESIGN CONCEPTS

Jamming detection, which will be the basis of the proposed jamming-aware algorithm, is based on the concept of consistency checks of relevant metrics [74]. By combining several metrics, the efficiency of detecting jamming increases. The detection algorithm leverages the use of two metrics, i.e., distance and PDR, which can be derived from information available in BSMs. The distance metric reveals important information regarding the expected link quality. In the case of jamming, when no BSMs are received, the distance is no longer available. Thus, the jamming-aware algorithm uses path prediction. In our algorithm, PDR is used to represent link quality.

The new jamming-aware algorithm is based on the concept of consistency check [74]. Consistency checks using several metrics provide higher detection probability than detection schemes that depend only on one metric. The diversity of the selected metrics helps differentiate between jamming and deteriorating communication due to benign effects such as signal fading. Our consistency checks use PDR and the distance between RV and HV, based on GPS coordinates embedded within the BSMs. We extend the principle of consistency check by incorporating path prediction based on prior received GPS coordinates. Prediction is important when vehicles travel inside a jammed zone, as they will no longer be able to communicate via BSMs. In this case the HV will no longer receive location data from the RV.

4.2.1 *Location Prediction*

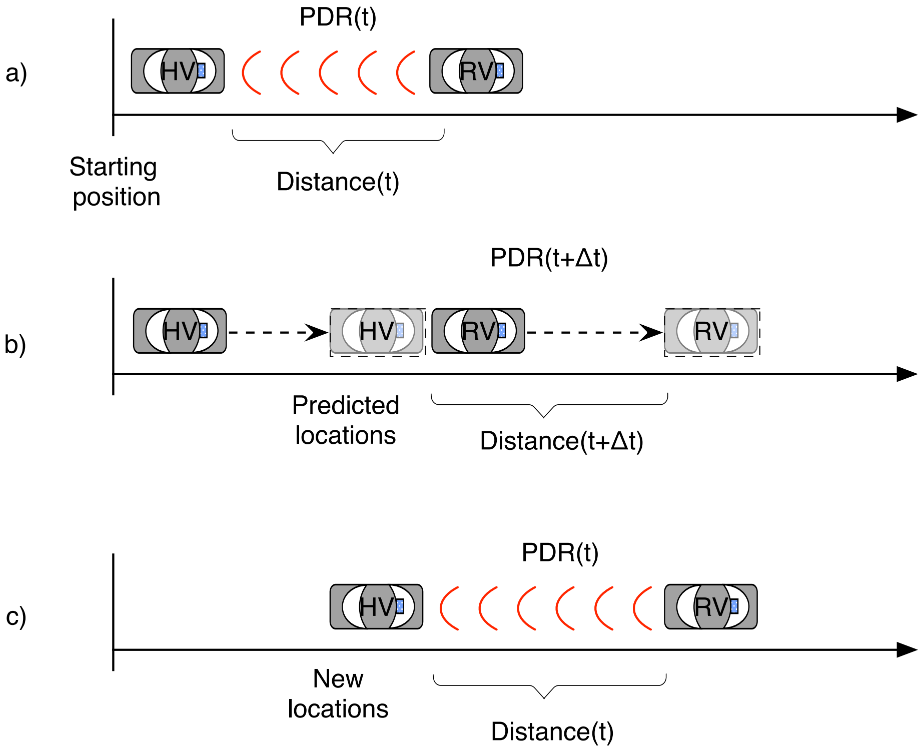

FIGURE 4.1: Jamming-aware scenario

Prediction is explained in Figure 4.1, where we assume both vehicles equipped with On-Board Units (OBUs) are traveling in a single lane. In normal operational conditions, when no jamming is present, the HV receives a BSM from the RV at time t, which contains information such as vehicle ID, type, location, speed, heading, and acceleration. Each received message reflects the status of the RV at the time the message was generated. The HV also generates a similar set of information regarding its current status. Thus, the HV will be able to calculate the current distance, $Distance(t)$. In addition, each received BSM will contribute to the calculation of the $PDR(t)$. This is shown in Figure 4.1a.

The HV will be able to estimate the future distance between both vehicles and the expected PDR, i.e., $Distance(t + \Delta t)$ and $PDR(t + \Delta t)$, shown in Figure 4.1b. As time progresses, the two vehicles will relocate, as shown in Figure 4.1c, and new BSMs will be sent from the RV inferring actual movement. The estimated values can be compared against the actual values, and any discrepancies reveal abnormality. The actual path prediction is described in Annex C-8 of SAE J2735 Standard [40].

4.2.2 *PDR Estimation*

PDR estimation is the second metric for consistency checks. For simplicity, a line-of-sight link budget can be used to estimate the link quality. The major losses result from free space path loss, which can be quantified as

$$FSPL_{dB} = 10 \log_{10} \left(\frac{4\pi d f}{c} \right)^2 \tag{4.1}$$

where $FSPL_{dB}$ is the free space path loss in dB, d is the distance between the transmitter and receiver in meters, f is the channel frequency in Hz, and c is the speed of light [71].

The received power can be expressed as the difference between gains and losses

$$P_{RX} = P_{TX} + G_{TX} + G_{RX} - FSPL_{dB} \tag{4.2}$$

where P_{RX} is received power in dBm, P_{TX} is the transmitter output power in dBm, G_{TX} is the transmitter antenna gain in dBi, and G_{RX} is the receiver antenna gain in dBi [71].

The signal-to-noise ratio is then calculated by

$$SNR_{dB} = 10log_{10}\frac{P_{signal}}{P_{noise}} = P_{RX} - P_{noise} \tag{4.3}$$

where SNR is the signal-to-noise ratio in dB, and P_{noise} is the noise power in dB.

Considering that DSRC uses Phase Shift Keying (PSK), we obtain the energy per bit and the Bit Error Rate (BER) for both 3 Mbps and 6 Mbps as

$$\frac{E_b}{N_0} = SNR \times \frac{B}{R} \tag{4.4}$$

where E_b/N_0 is the energy per bit to noise power spectral density ratio, B is the channel bandwidth in Hz, and R is the data rate in $bits/s$ [71]. The BER is now computed by

$$BER = \frac{1}{2}erfc\left(\sqrt{\frac{E_b}{N_0}}\right) \tag{4.5}$$

where *erfc* is the complementary error function.

Finally, the packet error rate is

$$P_p = 1 - (1 - BER)^N \tag{4.6}$$

where N is the packet length in bits. The PDR follows directly from the P_p.

4.3 JAMMING-AWARE ALGORITHM

The jamming-aware algorithm shown in Figure 4.2 is executed on all vehicles, but is described here from the viewpoint of the HV. Starting at time t equal to the current time, if no BSM message is received during a time interval Δt, the algorithm updates $t = t + \Delta t$ and starts over. In case a BSM message is received during Δt, it updates the status of the RV. This status consists of information contained in the received BSM, most importantly the RV's location (latitude, longitude and elevation), speed and heading. Given this location information, the distance between the two vehicles is calculated. Furthermore the PDR is determined. This is possible since the expected BSM packet rate is known to be 100ms. Thus the PDR is equal to the fraction of BSMs received during a predetermined window. If the value of the flag is not equal to 1, i.e, the flag is 0, the algorithm has received its first BSM from RV and proceeds to predict the future $Distance(t + \Delta t)$, and $PDR(t + \Delta t)$. It will then update the current time t and change the flag to $flag = 1$, which represents an acknowledgement of the existence of the RV. Then the algorithm proceeds to wait for another BSM.

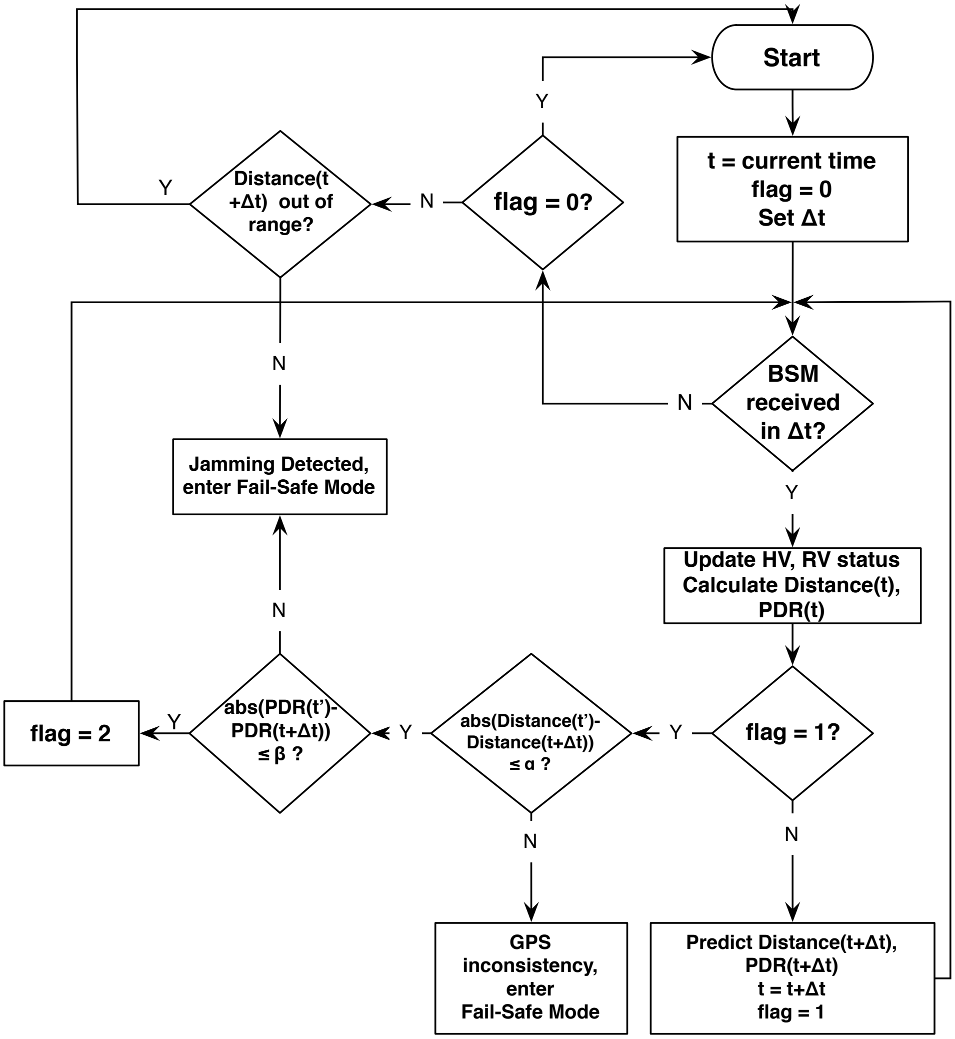
Start
t = current time
flag = 0
Set Δt
Y
flag = 0?
N
Distance(t +Δt) out of range?
Y
N
Jamming Detected, enter Fail-Safe Mode
N
BSM received in Δt?
N
Y
Update HV, RV status
Calculate Distance(t), PDR(t)
flag = 1?
Y
N
abs(Distance(t')- Distance(t+Δt)) ≤ α ?
Y
N
abs(PDR(t')- PDR(t+Δt)) ≤ β ?
Y
N
flag = 2
GPS inconsistency, enter Fail-Safe Mode
Predict Distance(t+Δt), PDR(t+Δt)
t = t+Δt
flag = 1

Figure 4.2: Jamming-aware algorithm

The algorithm contains a flag, initialized to $flag = 0$, that helps determine its state. When a new BSM is received, the new status information as well as the predicted status are available. Since now the flag is 1, the algorithm proceeds to compare the current distance between the RV and HV with the distance calculated from the prediction. If these distances are inconsistent, e.g., the GPS is malfunctioning or malicious data was injected, the system enters a fail-safe mode. In Figure 4.2 the consistency check is computed as $|Distance(t') - Distance(t + \Delta t)|$, where $Distance(t')$ is the actually measured distance according to GPS coordinates at time $t' = t + \Delta t$, and $Distance(t + \Delta t)$ is the predicted distance. To account for deviations in GPS accuracy the tolerance factor α was introduced.

Otherwise the algorithm proceeds to the PDR check, comparing the PDR calculated for the window with the predicted PDR. The prediction of the PDR could be based on the expected link quality from Subsection 4.2.2, or based on previously measured behavior, as will be explained in Section 4.4. If the calculated PDR is inconsistent with the predicted PDR, jamming is assumed and the system will enter a fail-safe mode. The notation for the calculated versus predicted PDR is analogous to that used for distances above, i.e., $|PDR(t') - PDR(t + \Delta t)|$, where $PDR(t')$ is the calculated PDR at time $t' = t + \Delta t$, and $PDR(t + \Delta t)$ is the predicted PDR. A tolerance of β accounts for deviations in PDR values.

Inconsistency beyond tolerance α or β indicate significant changes in distances and PDR that cannot be the result of GPS inaccuracy or normal signal fading. Should both consistency checks pass, the algorithm assumes normal operation, sets the flag value to 2, and resumes receiving BSMs.

If no new BSM is received after successfully receiving at least one BSM, the algorithm checks to see if the predicted distance is out of range. If the RV is out of HV's range, the algorithm starts over. Otherwise we conclude that jamming has occurred and fail-safe mode will be entered.

Finally, it should be noted that in cases where the sending OBU fails in a benign way, the algorithm will detect inconsistency and also guide the Safety Application to the fail-safe mode, indicating that the application should no longer be trusted.

4.4 PERFORMANCE EVALUATION

The impact of jamming on vehicle communications and the performance of the jamming-aware algorithm were evaluated in a field test. For this purpose an HV and RV were equipped with OBUs, specifically LocoMate Classic OBUs from Arada Systems [73]. An additional LocoMate Classic OBU was configured to be a deceptive jammer capable of operating at different data rates by reprogramming the OBU. Specifically, the jamming OBU sent out a constant stream of bogus packets, violating the distributed coordination function (DCF) of the IEEE 802.11p protocol, which blocked other OBUs from accessing the media. The exact parameters for the field test below are shown in Table 4.1.

Table 4.1: Field test parameters

OBU	Arada Systems LocoMate Classic
Vehicle speed	15.6 m/s
Test range	straight 2-lane road
Test range length	1.35 km
Jammer position	600m from starting point
BSM rate	10 BSM/s (a BSM every 100ms)
Channel	Safety Channel 172
Effective bandwidth	8.3 MHz
Transmitter power	18 dBm
Data rate	3 and 6 Mbps
Jammer power	18 dBm
Jammer data rates	3, 6, and 12 Mbps

4.4.1 *Normal PDR*

The estimates of the PDR of communication between the RV and HV in the absence of jamming is used by the jamming-aware algorithm to predict future behavior. To see how realistic such estimates are, a field test was conducted in open space. Specifically, to obtain the PDR during normal (non-jamming) operation, communication was logged over the entire OBU communication range, where BSMs were collected at the HV as the RV increased its distance. The results of the measured PDR (the field test) and the calculated PDR (see Subsection 4.2.2) are shown in Figure 4.3 and

Figure 4.4. One can observe in the figures that the experiment is in line with the calculated estimates.

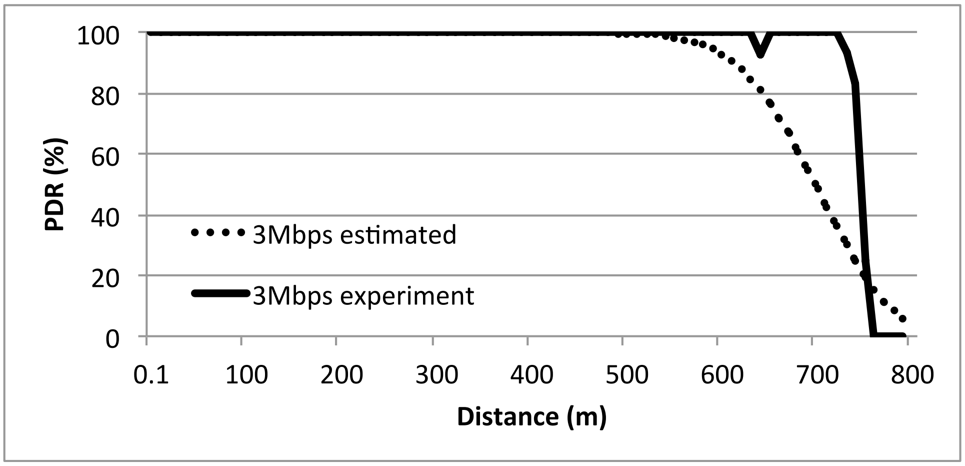

Figure 4.3: Estimated and actual PDR for 3Mbps

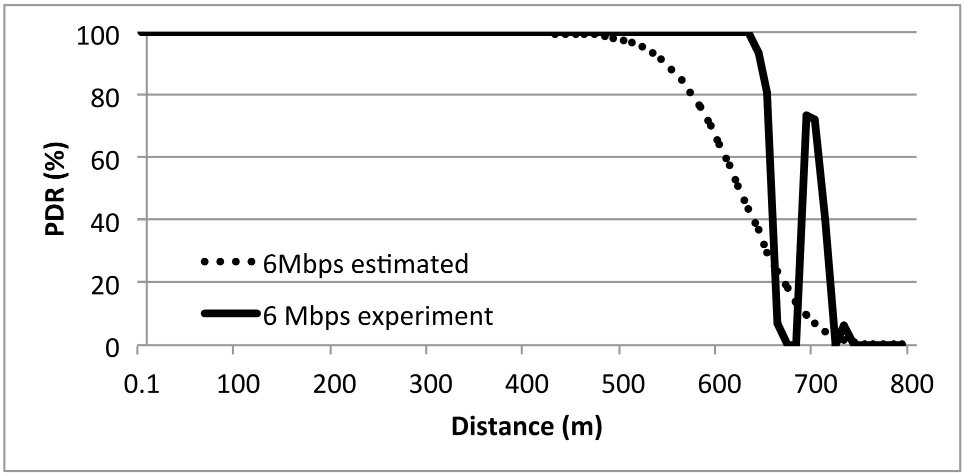

Figure 4.4: Estimated and actual PDR for 6Mbps

4.4.2 *The Impact of Jamming on PDR*

The experiment to measure the impact of jamming on the PDR consisted of two cars (RV followed by the HV) driving on a straight 2-lane road, passing a deceptive jammer located in a parked vehicle on the roadside. During the tests BSMs were logged by the OBU in the HV for data rates of 3 and 6 Mbps as they were subjected to deceptive jamming with rates of 3, 6, and 12 Mbps. It should be noted that data rates of 12 Mbps were shown to be unsuitable for BSM communication in the presence of jamming in [63, 64, 65].

Figure 4.5 shows the PDR for 3 Mbps BSM communication for different jamming rates for a typical test scenario. As the HV and RV approached the jammer stationed at 600m, the HV could not receive BSMs around 375-425m. The impact of the jammer dropped off at around 750-800m. The transmission rate of the jammer had only modest impact on the PDR. However, for this kind of jammer we could not establish a pattern for these small differences during several experiments.

The result from a typical experiment with a data rate of 6 Mbps is shown in Figure 4.6. Again the PDR is only modestly affected by the rate of the deceptive jammer. An interesting situation can be seen for the experiment with the 3 Mbps deceptive jammer. Here, after the HV was jammed, it could briefly receive messages from the RV again around 475m. The reason for this was that a small truck passed the test vehicles and positioned itself briefly between the vehicles and the jammer, thus reducing the impact of deceptive jamming.

In summary, the field test revealed that the data rates of the deceptive jammer only modestly affected transmissions. The same could be observed over different tests about how transmissions of different data rates were affected. Whereas the overall impact of jamming was very high, we could not establish a clear pattern in the differences of the impact for different data rates of the jammer and vehicles. This is in contrast to constant jamming, where the impact of jamming drastically decreases PDRs for higher data rates [63].

4.4.3 *Jamming-aware Algorithm Evaluation*

The results from the evaluation of the jamming-aware algorithm for the 3Mbps field test data of the previous subsection are shown in Figure 4.7. The algorithm successfully detected jamming once the PDR drop was detected by the consistency check based on distance and PDR. No inconsistency of distances were observed by the algorithm. Thus, in this specific field experiment only one of the two detection mechanisms was sufficient, as no GPS inconsistencies were injected. However, the PDR inconsistency was detected.

4.5 FIELD EXPERIMENT AND EQUIPMENT DETAILS

In this section we will elaborate more on the equipment used to perform the field experiment described previously in Section 4.4. We will also shed light on the overall test environment and the commands used to perform the experiment.

For the experiment purpose, we used the Arada LocoMate OBUs [73]. The units are shown in Figure 4.8, and they are primarily used to enable wireless connectivity between OBUs or between OBUs and RSUs in vehicular environments. The LocoMate OBU operates within the physical specification of the FCC amendment and the ASTM E2213 standard [39, 48]. Also, it provides safety and data services to the vehicle users by communicating BSMs per the SAE J2735 standard [40]. For location information, the OBU has integrated GPS device with RF antenna, which provide the longitude and latitude for the vehicle.

Figure 4.9 shows the device and its connectivity. According to the manufacturer's user manual [73], the OBU utilizes MIPS processor clocked at 680MHz and a flash memory of 16MB in addition to an SDRAM of 64MB. It has a Gigabit Ethernet Interface and Atheros AR5414 based WLAN Mini PCI. During the tests, we used portable power supplies, and the GPS antenna was placed on the top of the vehicle. The devices themselves were held outside the vehicle with upward antenna orientation.

The overall testing area is shown in Figure 4.10, with a total distance of 1350 m. Here, three distinct marked positions were of our interest, the starting point at 0 m, the jammer position at 600 m, and finally the end point at 1350 m.

A total number of three OBUs were used, one acting as HV and the other one as an RV, as for the third was used as a stationary deceptive jammer. The experiment was performed in several runs, with each run set to different parameters. In each run a Packet Capture File (.pcap) was stored for further analysis.

Next, we describe each of the experiments along with the commands used to operate the OBUs. In the *first experiment*, the purpose was to measure the normal behavior of HV and RV, and to measure the overall transmission range without the involvement of the jammer. The RV and HV were parked at the starting position, and then the RV increases its distance. The data rates tested were, 3 and 6 Mbps, transmitting on the safety channel (CH172), and the transmit power is set to 18 dBm

Table 4.2: First experiment commands

Data Rate	Vehicle Type	Command	Log file name
3 Mbps	HV	getwbsstxrxencdec -s 172 -t BSM -a 1 -o TXRX -X TXRXLOG -r 3.0 -j 18	HV-EX1-3-v1.pcap
	RV	getwbsstxrxencdec -s 172 -t BSM -a 1 -o TXRX -X TXRXLOG -r 3.0 -j 18	RV-EX1-3-v1.pcap
6 Mbps	HV	getwbsstxrxencdec -s 172 -t BSM -a 1 -o TXRX -X TXRXLOG -r 6.0 -j 18	HV-EX1-6-v1.pcap
	RV	getwbsstxrxencdec -s 172 -t BSM -a 1 -o TXRX -X TXRXLOG -r 6.0 -j 18	RV-EX1-6-v1.pcap

Table 4.3: Second experiment commands

Data Rate	Vehicle Type	Command	Log file name
3 Mbps	HV	getwbsstxrxencdec -s 172 -t BSM -a 1 -o TXRX -X TXRXLOG -r 3.0 -j 18	HV-EX2-3-v1.pcap
	RV	getwbsstxrxencdec -s 172 -t BSM -a 1 -o TXRX -X TXRXLOG -r 3.0 -j 18	RV-EX2-3-v1.pcap
	Jammer	Start_tx99 -f 5860 -m 1 -r 3000 -p 18 -c 0	
6 Mbps	HV	getwbsstxrxencdec -s 172 -t BSM -a 1 -o TXRX -X TXRXLOG -r 6.0 -j 18	RV-EX2-6-v1.pcap
	RV	getwbsstxrxencdec -s 172 -t BSM -a 1 -o TXRX -X TXRXLOG -r 6.0 -j 18	RV-EX2-6-v1.pcap
	Jammer	Start_tx99 -f 5860 -m 1 -r 3000 -p 18 -c 0	

as shown in table 4.2. The results of these experiments were depicted in Figures 4.3 and 4.4.

In the *second experiment* the jammer was involved, and its power was set to 18 dBm, and the purpose was to study the impact of the deceptive jammer on the communication between the HV and the RV. With both the HV and the RV are driving past the stationary jammer. We tested two different data rates, i.e., 3 and 6 Mbps as shown in table 4.3. In addition to different jamming rates, those are 3, 6 and 12 Mbps. The distance between the HV and the RV was average of 25 m, and the average speed of the vehicles is 15.6 m/s. The results of these experiments were depicted in Figures 4.5 and 4.6.

4.6 Conclusions

This chapter addressed jamming detection as a method to guide DSRC Safety Applications to a fail-safe mode. A new jamming-aware detection algorithm was introduced that uses two different types of metrics, i.e., distance between vehicles and

PDR. Furthermore, the algorithm uses predictions for distances and PDR when real information is not available due to jamming of the BSMs. The jamming model used was the deceptive jammer, and the impact of this jammer type on BSM reception was studied.

Field tests using vehicles equipped with Arada LocoMate OBUs revealed that disruption of BSMs by deceptive jammers was significant. However, different data rates of the deceptive jammer did not change the observed PDRs of vehicle communication. Furthermore, there were no significant differences of PDR between 3 and 6 Mbps data rates of the BSMs.

As jamming cannot be avoided, the jamming-aware algorithm used two metrics, each of which were observed and additionally predicted, to achieve detection of jamming. The field-test data demonstrated that the jamming-aware algorithm is capable of shifting DSRC Safety Applications to a fail-safe mode when jamming is detected.

4.7 ACKNOWLEDGEMENTS

We would like to thank Vinay Thadani and Nazeer Shaik from Arada Systems for their assistance and jammer programming. Furthermore we would like to thank Sanjeev Shrestha, Anirudh Bhandari, and Dan Pierce for their help conducting the field experiments.

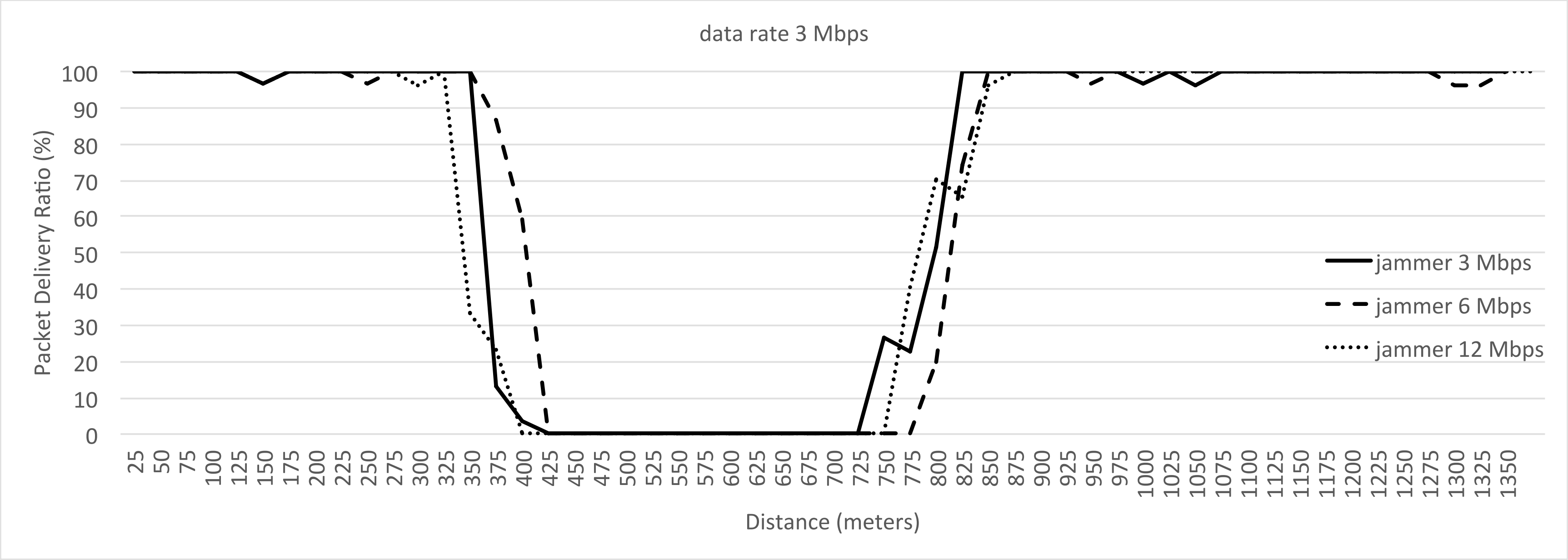

Figure 4.5: PDR at 3 Mbps with deceptive jamming

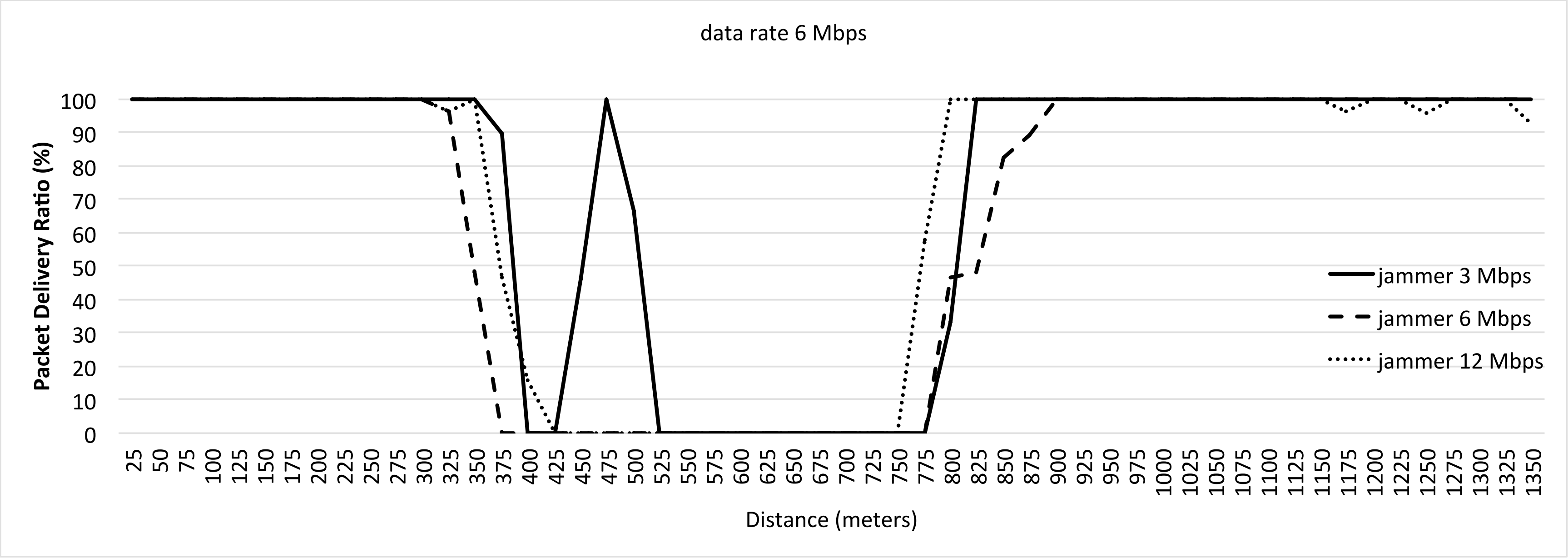

Figure 4.6: PDR at 6 Mbps with deceptive jamming

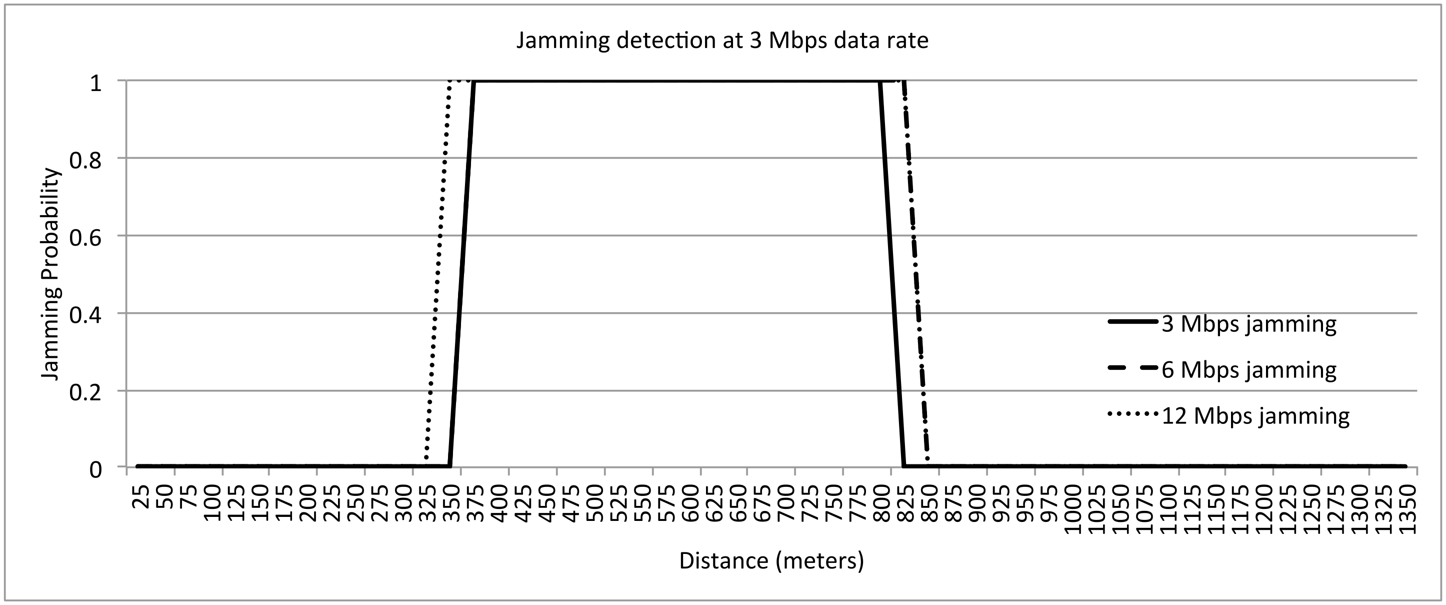

Figure 4.7: Evaluation of jamming-aware algorithm for 3 Mbps data rate

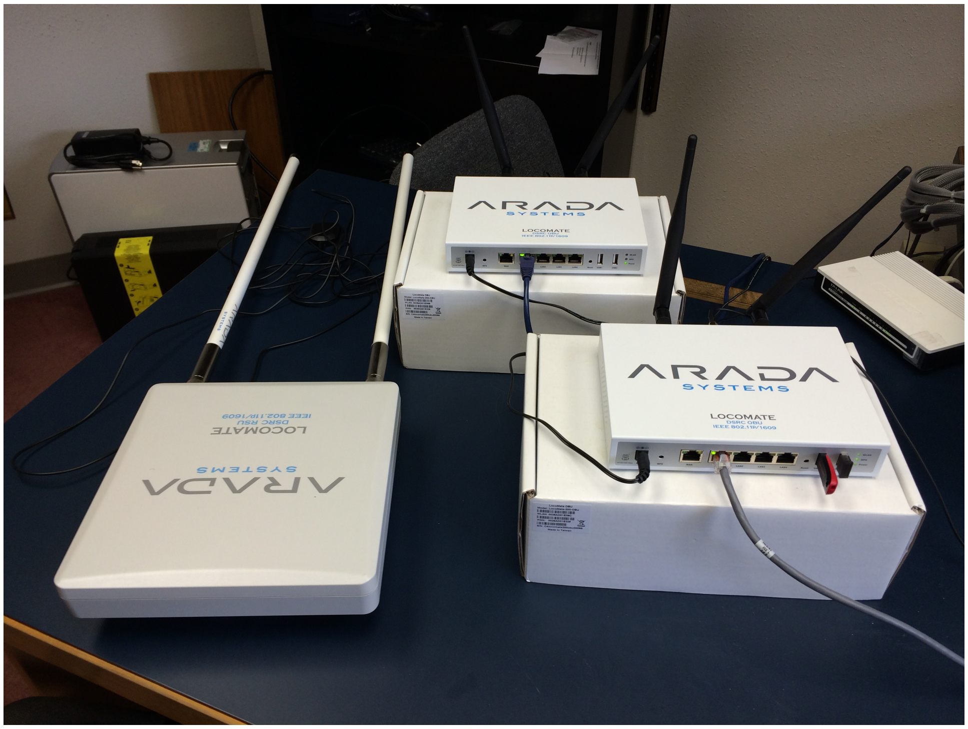

Figure 4.8: LocoMate OBUs

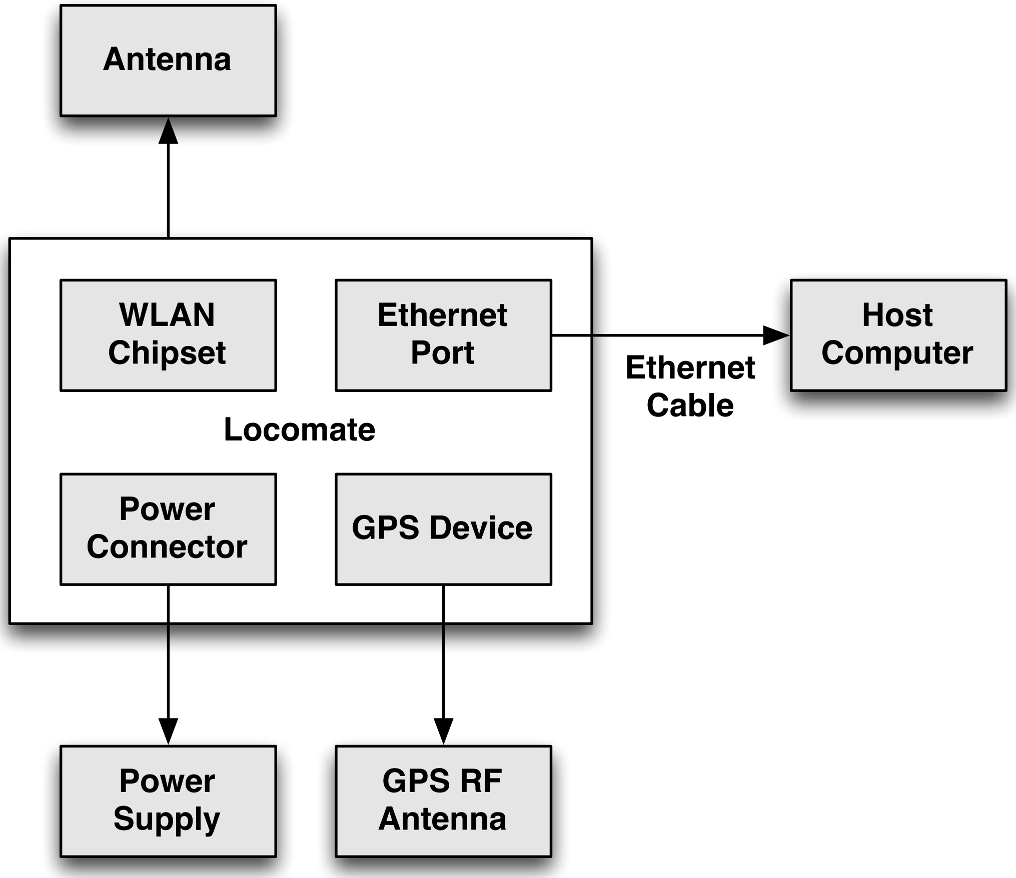

Figure 4.9: LocoMate connections

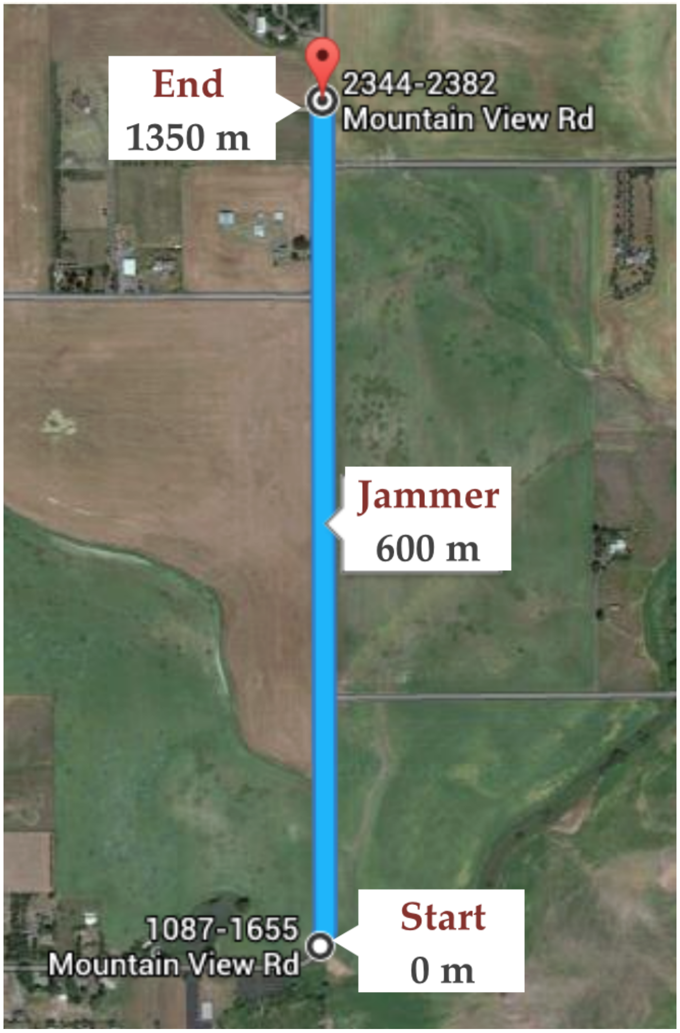

FIGURE 4.10: Testing area

CHAPTER 5
A Recovery Strategy for DSRC Safety Applications Subjected to Jamming Attacks

In this chapter we investigate the impact of message rates, power levels and data rates on reliability and channel efficiency. Specifically, we demonstrate the impact of increased safety message rates on channel performance. Jamming detection is used to transition DSRC Safety Applications to stricter modes of operation, i.e., fail-safe mode, and a recovery algorithm is introduced to aid in transitioning the Safety Applications back to an operational mode faster, thereby reducing the impact of jamming. The recovery algorithm that will be presented in this chapter dynamically adjust message rates, power levels and data rates only in situations where communication anomalies, such as jamming, are detected. Mathematical analysis and data collected during field tests, show that the recovery strategy helps Safety Applications to transition from fail-safe mode to operational mode earlier.

5.1 RELATED WORK

To overcome the impact of jamming, an approach of message and channel redundancy has been demonstrated in [64, 65] for the case of constant, random and intelligent jamming. This approach implies using alternative messages, namely the À la Carte (ACM) and Probe Vehicle Data (PVD) to deliver safety related data using redundant channels. These messages were defined in SAE J2735 [40] and they facilitate BSM functional redundancy, i.e., communicating the BSM-relevant data on any service channel. In addition, these messages can be used along with the BSMs in a dual and triple redundancy scheme. The redundant channels were carefully selected to ensure wide separation in the frequency spectrum.

While this approach showed to be effective, using redundancy imposes extra overhead/usage of the dedicated limited bandwidth, which is intended to be used by multiple DSRC applications. Furthermore, the research in [64, 65] did not not deal with challenges such as MAC layer efficiency, channel congestion and fail-safe operation of the Safety Applications.

5.2 RELIABILITY AND REDUNDANCY

Recall that each OBU broadcasts a BSM every 100 ms on the safety channel (CH172), leading to a rate of 10 BSM/s [40] and [52]. Now we extend the concept of redundancy by increasing this message rate and investigate its impact on Safety Application reliability as well as overhead. Let us consider the forward collision warning application in Figure 2.4a), where the RV brakes hard, e.g., to avoid an obstacle. Braking hard will result in a brake system status alert indicated in the RV's BSM. From the HV point of view this means that at least one BSM containing this status needs to be received to alert the driver early enough to account for reaction time. Thus the Safety Application reliability is the probability of the HV receiving at least one BSM message before it is too late to react, i.e., at time t_{react}.

In line with the standard definition of reliability, i.e., $R(t)$ is the probability that the system is working to specifications during the entire time interval $[0, t]$ [76], we can define our application reliability $R(t)_{app}$ as the probability of receiving at least one BSM message before t_{react}. If we denote the i^{th} BSM by BSM$_i$ then at least one of the BSM$_i$, $i = 1, ..., x$, needs to be received, where BSM$_x$ is the last BSM before t_{react}. Thus the application fails only if no BSM message is received before t_{react}. The unreliability $Q(t)_{app} = 1 - R(t)_{app}$, i.e., the probability that no BSM$_i$, $i = 1, .., x$, was received can now be expressed as

$$Q(t)_{app} = \prod_{i=1}^{x} Q_i(t_i) \tag{5.1}$$

where Q_i is the probability that BSM$_i$ was not received at t_i. It should be noted that $Q_i(t_i)$ is the packet error probability of BSM$_i$. If N redundant channels are used, then $Q_N(t)_{app} = \prod_{j=1}^{N} Q_{c_j}(t)$, where $Q_{c_j}(t) = \prod_{i=1}^{x} Q_i(t_i)$ represents the unreliability for each channel, as computed by Equation 5.1 for one channel. These methods for calculating Safety Application unreliability and channel redundancy have been introduced in [63].

Raising the BSM rate has the potential to increase the reliability of the system, but that depends on the jamming scenario shown in Figure 5.1. The figure shows the intensity of jamming indicated by the color depth. The left region triggers jamming detection, which can be used to force the Safety Application into a fail-safe mode. The right region is unaffected by jamming. The region in the middle is however of interest as increasing the BSM rate will be shown to alleviate modest jamming. This does not only apply to the safety channel (CH172), but can be extended to different channels, e.g., CH178 using ACM in a dual redundant approach, or by including CH184 using PVD to derive a triple redundant scheme.

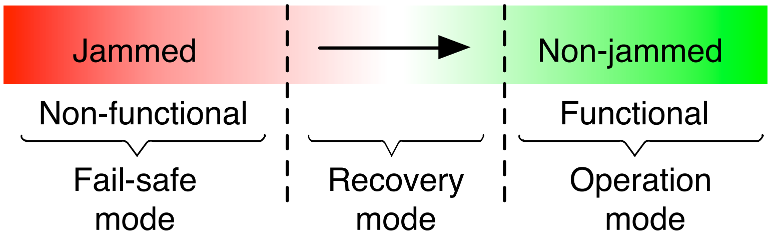

Figure 5.1: Jamming impact regions

Increasing message rates and using redundant channels both increase Safety Application reliability, as the number of terms in the product of Equation 5.1 increases, thus reducing application unreliability $Q(t)$. However designing Safety Applications to operate in either of the aforementioned strategies is an aggressive approach, as it drastically decreases channel efficiency, specifically, the number of messages grow with the BSM rate from each vehicle. But redundancy is only needed to overcome a transient or abnormal situation. So, a more reasonable approach is to use redundancy only when an abnormal situation is detected.

5.3 Impact of different BSM rates

The increased number of BSMs due to higher BSM rates is an extra burden on the MAC layer and has the potential to decrease the PDR due to collisions.

Several factors play vital roles in determining the upper bound of BSM rates, i.e., the number of vehicles in the neighborhood, the data rate, and the message size. To get a feeling for this upper bound, Figure 5.2 shows the maximum available BSM rates for different data rates and two sample BSM sizes, 300 and 180 Bytes, using a PHY Preamble = 32μs, DIFS = $64\mu s$, PLCP header = $8\mu s$. For example, at a data rate of 6Mbps and 300 Bytes message size, Transmission Delay = $\frac{Message\ Size}{Data\ Rate} = \frac{8\times 300}{6000000} = 400\mu s$, and now by adding all delays $32\mu s + 64\mu s + 8\mu s + 400\mu s$, this sums up to a total delay of $504\mu s$ per message. As BSM data rates higher than 6Mbps have been shown to be too unreliable in the presence of jamming, the data rates that should be used by DSRC Safety Applications are 3Mbps and 6Mbps [65]. For a 6Mbps data rate, the maximum number of messages the media can handle is 1984 BSM/s for 300 Bytes message size. This can be calculated considering the Maximum Throughput = $\frac{Message\ Size}{Total\ Delay} = \frac{2400 bits}{504\mu s} = 4,761,904\ bits/sec$. Thus, when sending a BSM of size 300 Bytes (2400 bits), the total messages that can be handled by the media is = $\frac{maximum\ throughput}{packetsize} = 1984\ BSM/s$. Likewise, at 6 Mbps and for a message size of 180 Byes, the maximum number of messages the media can handle is 2906 BSM/s. Based on these numbers and the fact that each vehicle sends 10 BSM per second, one can get an upper bound on the number of vehicles that theoretically can be handled by the media. However, these numbers do not consider potential collisions, as they would occur when large numbers of vehicles send BSMs.

The maximum number of messages for different data rates shown in Figure 5.2 was calculated without any consideration for collisions. But in order to have a more reliastic view of the impact of redundant BSMs on the medium, one must consider the impact of transmission collisions. Collisions occur when two or more vehicles attempt to send a message in the same transmission channel at the same time. Consequently, these collisions result in corrupted packets, consume the bandwidth, and degrade the PDR especially when the number of vehicles increase.

Recall that VANET uses the DCF and CSAM/CA of the IEEE 802.11, as previously mentioned in Subsection 2.1.2. The ways in which these collisions happen can be either direct, or as a result of a hidden terminal. In *direct collision*, the sender and receiver are within the transmission range of each other, however, they simul-

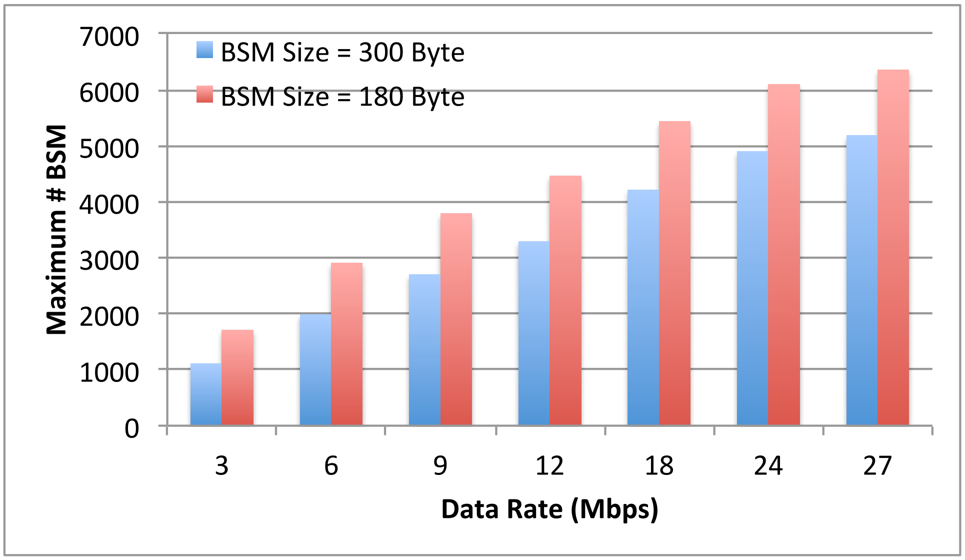

FIGURE 5.2: Upper bound on BSM rates for different data rates

taneously send at the same time due to similar back-off times. On the other hand, *hidden terminal* refers to the situation when three (or more) nodes are positioned in a way, where the outer nodes are not within the transmission range of each other, but within the range of the middle node. This situation will lead to more collisions, since the outer nodes cannot sense the presence of each other, leading to simultaneous communicating with the middle node.

To avoid these collisions, several mechanisms have been implemented in wired and wireless networks, of those are physical carrier sensing and virtual sensing [72]. *Physical carrier sensing* indicates that the sender will physically monitor the medium and if the medium is busy, the sender will defer transmission. Only after the medium is sensed idle, the sender can transmit the data frame after a random back-off time. This is to avoid direct collisions with other nodes who are also competing the for the medium.

Whereas *virtual sensing* set a Network Access Vector (NAV), which is a counter for the duration required for a packet to be transmitted. The NAV is set based on the Request-to-Send and Clear-to-Send (RTS/CTS) frames [43]. Which implies that before a source attempts to transmit a packet, it sends an RTS and wait for a corresponding CTS reply from the destination. Hidden nodes, that happen to be outside the source range, will still be able to hear the CTS reply and set their

NAV accordingly. during the NAV duration, the nodes will not attempt to send, thus reducing the collisions for the hidden terminal situations. However, for Safety Applications in VANETs, virtual sensing is not suitable, since the BSMs are being broadcast to high speed vehicles with a required minimum delay. Thus, the hidden terminal situation has potentially more grave impact on Safety Applications in VANETs.

We study the impact of transmission collisions on PDR with respect to vehicle density, using the MAC layer model presented in [78]. The model specifically measures the performance of the IEEE 802.11p MAC protocol, for both hidden and direct collision cases.

Let N_{tr} denote the average number of vehicles in the transmission range,

$$N_{tr} = 1 + 2\beta R \tag{5.2}$$

where β is the vehicle density in [vehicles/km] and R is the transmission range.

The the queue utilization ρ can be expressed as,

$$\rho = \lambda E\left[S\right] \tag{5.3}$$

where λ is the packet generation rate [packets/sec] and $E[S]$ is the average service time.

Now let τ be the probability that a vehicle transmit in a random slot considering that it has a packet in the queue,

$$\tau = \frac{1}{\overline{W} + 1} \tag{5.4}$$

where $\overline{W}$ is the average number of back-off slots.

The probability of direct collision P_{dc} is calculated as follows,

$$P_{dc} = \left(1 - (1-\rho)\left(1 - P_b\right)(1-\rho\tau)^{N_{tr}-1}\right) \tag{5.5}$$

Note that P_b represents the probability that a channel is sensed busy when a new packet arrive,

$$P_{dc} = (N_{tr} - 1)\,\lambda T \left(\frac{1 - P_{dc}}{2}\right) \tag{5.6}$$

where T is the complete transmission time of a packet including DIFS period.

Finally, the PDR_{dc} for direct collision case is,

$$PDR = 1 - P_{dc} \tag{5.7}$$

As for the hidden terminal case, let P_{hc} represents the probability of a hidden terminal collision,

$$P_{hc} = 1 - (1 - P_{dc})\,P(S_1)\,P(S_2) \tag{5.8}$$

where, S_1 denotes the event where non of the hidden terminals transmit, considering the number of hidden terminals is N_{ph} this probability can be expressed as,

$$P(S_1) = 1 - N_{ph}\lambda T \left(1 - \frac{P_{dc}}{2}\right) \tag{5.9}$$

and S_2 denotes the case where a vehicle start its transmission,

$$P(S_2) = e^{-\lambda N_{ph}(t_{data} - t_{DIFS})} \tag{5.10}$$

where, t_{data} is the transmission time for a packet, and t_{DIFS} is the duration of DIFS period.

Finally, the PDR_{hc} for hidden terminal case is expressed as,

$$PDR = 1 - P_{hc} \tag{5.11}$$

For calculating the PDR for the direct collision, and hidden terminal cases, we use Equations 5.7 and 5.11 respectivly. The parameters used to model the collisions are listed in Table 5.1. The model described in [78], which is the basis for this analysis, considers Safety Applications for vehicles in a multi-lane highway. However, the distances between lanes are insignificant compared to the length of the network.

Table 5.1: MAC model parameters

Average number of back-off slots, W	16
Transmission range, R	600 m
DIFS time	64 micro s
Data rate	6 Mbps
BSM rates	10, 20 and 30 BSM/s
BSM size	180 Bytes
Vehicle density	2-200 vehicles/km

Note that, in the analysis we use a transmission range of 600 meters, as it was observed during field tests described previously in Section 4.4.

Figure 5.3 shows the impact of direct collisions on the PDR with respect to various vehicles densities. As the vehicle density increases, i.e., from 2 to 200 vehicles/km, the PDR shows degradation for all the three tested BSM rates. However, for the 10 BSM/s message rate, the impact of direct collisions on PDR is minimal. Even at vehicle density of 200 vehicle/km, the PDR remains reasonable at 92%. When increasing the BSM rate to 20 BSM/s, the PDR drops to %72. Further increase in rate to 30 BSM/s, yields PDR of only 4%, which will render the Safety Application useless at high vehicle densities. One could only use such high BSM rates at lower vehicles densities, e.g., sending 20 BSM/s at vehicles densities below 115 vehicles/km, or 30 BSM/s for 78 vehicles/km.

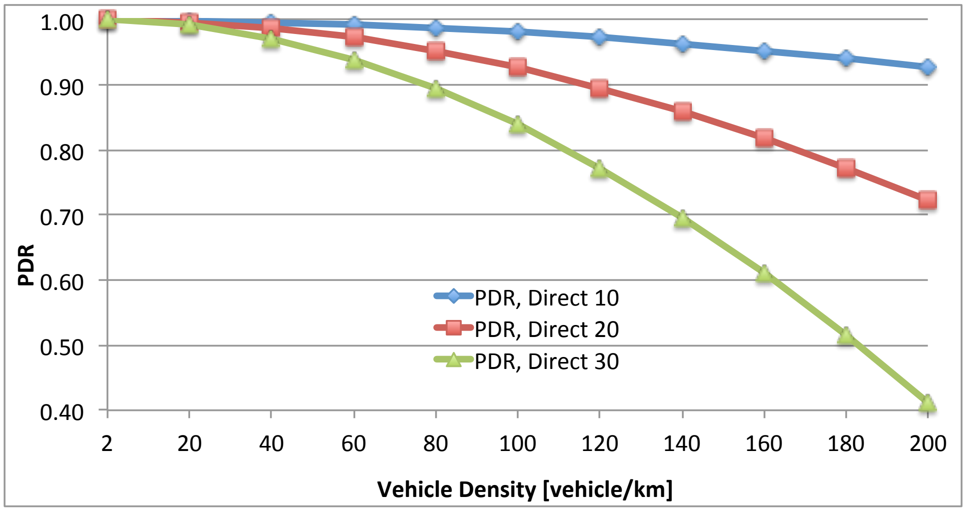

Figure 5.3: Impact of direct collisions on PDR (BSM size=180 Byte, data rate=6Mbps, BSM rate=10,20,30 BSM/s)

Next, we investigate the impact of hidden terminal collisions on the PDR with respect to various vehicles densities as shown in Figure 5.4. Here, a PDR above 90% is only achievable at a density of 20 vehicles/km when sending at a rate of 10 BSM/s, and higher BSM rates result in a significant problem, questioning the suitability of the 802.11p MAC layer in relatively dense neighborhoods [78].

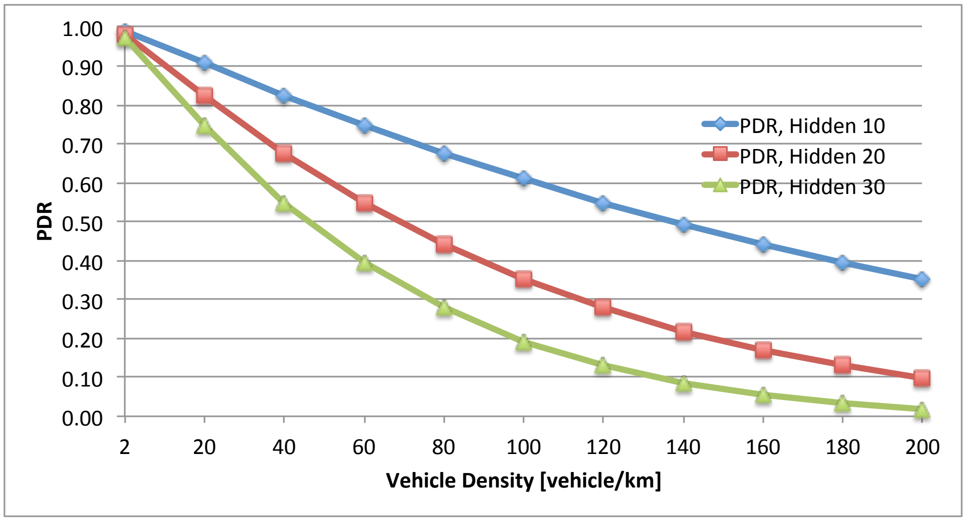

Figure 5.4: Impact of collisions resulting from hidden terminals (BSM size=180 Byte, data rate=6Mbps, BSM rate=10,20,30 BSM/s)

In summary, higher BSM rates are beneficial to reliability, however, it will decrease channel efficiency. This tradeoff will be addressed in the next section.

5.4 Jamming Detection, Fail-Safe Mode, and Recovery

A jamming mitigation strategy for DSRC Safety Applications will be presented next. It uses jamming detection as a mechanism to transition the applications to fail-safe mode, and a recovery algorithm to transition back to a functional mode.

5.4.1 *Detection Algorithm*

Jamming detection is based on the new jamming-aware algorithm, that has been introduced in Chapter 4. The jamming aware-algorithm detects jamming based on estimations of vehicle location and PDR.

Upon detection, the Safety Application is assumed to be no longer dependable and transitions to a fail-safe mode, in which case the driver is notified that the Safety Application is no longer available. Two different types of metrics were used by the algorithm, i.e., distance between vehicles and PDR. It uses predictions and consistency checks for distances and PDR when real information is not available due to jamming of the BSMs. The jamming-aware algorithm has already been presented with greater details, for that matter we refer the reader to .

Recall the algorithm in Figure 4.2, which transitions to fail-safe mode in two situations, i.e., when jamming is detected and when GPS information is contradictory. The latter case is outside the scope of this research. Hence, we did not include it in our experiments, and it can be considered in future work.

5.4.2 *Recovery Mode*

The recovery algorithm shown in Figure 5.5 is invoked once jamming is detected and the Safety Application transitions to fail-safe mode. Once jamming is detected the application will go to a fail-safe mode, and a $Confidence.Level$ parameter is set to 0. This low confidence level indicates that the application is not trusted due to jamming, and thus no safety alert messages will be issued to the driver. The recovery algorithm will proceed by calculating $Max.Rate$, which is the maximum possible number of BSMs a vehicle is allowed to send. The $Max.Rate$ can be determined based on the last observed number of vehicles before entering the jammed area. The algorithm then compares the current BSM rate, i.e., $BSM.Rate$ against $Max.Rate$. If $BSM.Rate$ is less than $Max.Rate$, the algorithm will increase the current BSM rate. This check will ensure that the upper bound of a channel capacity is not be exceeded. After increasing $BSM.Rate$, the algorithm will wait for receiving BSMs for a duration of Δt. If no BSMs are received during Δt, the algorithm further increases the $BSM.Rate$, if possible. In case a BSM is received during Δt, the content of the message is examined to see if it is a high priority BSM, i.e., one that indicates a hazard. For high priority BSMs, e.g., relating a forward collision warning due to hard braking event, a warning will be passed to the driver from within the recovery mode. On the other hand, if the content of the received messaged does not relate to a potential hazard, no warning will be passed. For each successful BSM reception the level of confidence is increased. Once a *Threshold* of confidence is reached, the *BSM.Rate* is reset and the algorithm issues a mode switch from fail-safe to normal operational mode. However, if the threshold is not met, the recovery mode will wait for another Δt to receive more messages at the same increased rate, and the process will be repeated again.

We emphasize that the increase in BSM rates only occurs during execution of the recovery algorithm. This means that the standard 10 BSM/s rate is used otherwise.

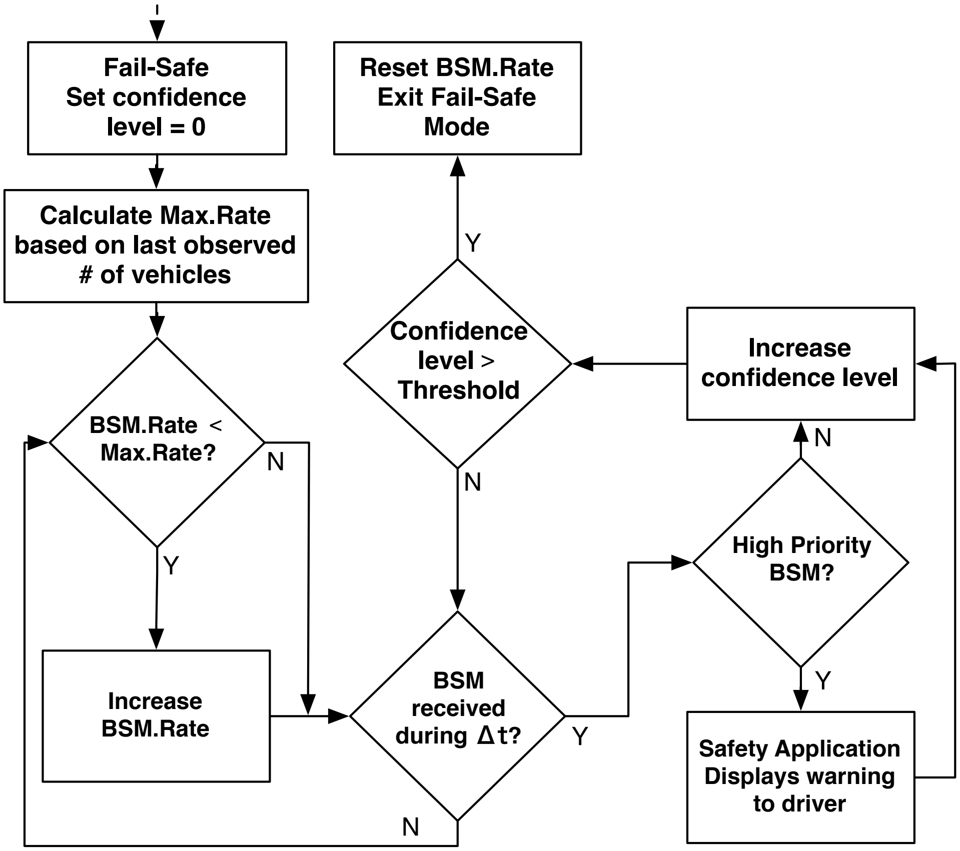
Fail-Safe
Set confidence level = 0
Reset BSM.Rate
Exit Fail-Safe Mode
Calculate Max.Rate based on last observed # of vehicles
Y
Confidence level > Threshold
Increase confidence level
BSM.Rate < Max.Rate?
N
N
N
High Priority BSM?
Y
Increase BSM.Rate
BSM received during Δt?
Y
Y
Safety Application Displays warning to driver
N

Figure 5.5: Recovery algorithm

5.5 Performance evaluation

The usefulness of the concepts behind the recovery algorithm will be studied next using two types of jammers, the constant jammer, and the deceptive jammer. For the constant jammer we have estimated the impact using analytical models, as for the deceptive jammer we have used field experiments and actual DSRC equipment.

5.5.1 *Constant Jammer*

Assume the scenario depicted in Figure 5.6, in which an RV is followed by an HV, going on a single-lane road. Suppose that the RV encounters a hazard and starts to brake. This action will result in the dissemination of BSMs that carry braking information from the RV to surrounding vehicles. Assume the speed of the two vehicles is set to 35 mph (15.6 m/s) and the space between them, i.e., the safety distance, is equivalent to $3s$. The reaction time t_{react} is the time required by the driver from recognizing an alert to the application of the brakes. Typical reaction times are within $0.9s$ [77]. For simplicity we assume $t_{react} = 1s$. Therefor, for the assumed inter-vehicle spacing of $3s$, this will leave only $2s$ for the HV to receive BSMs regarding this event before it is too late to react. Let the source of a malicious attack in this scenario be a constant jammer. We assume the jammer is positioned behind the HV, and the impact of jamming is determined using the equations in Subsection 3.5.1. Thus, we define the unreliability $Q(t)$ of the Safety Application by the inability of the HV to successfully receive at least one BSM before t_{react}, as previously indicated in Section 5.2. The inability of the HV to receive BSMs from the RV is directly related to the jammer's signals overpowering the legitimate communication signals.

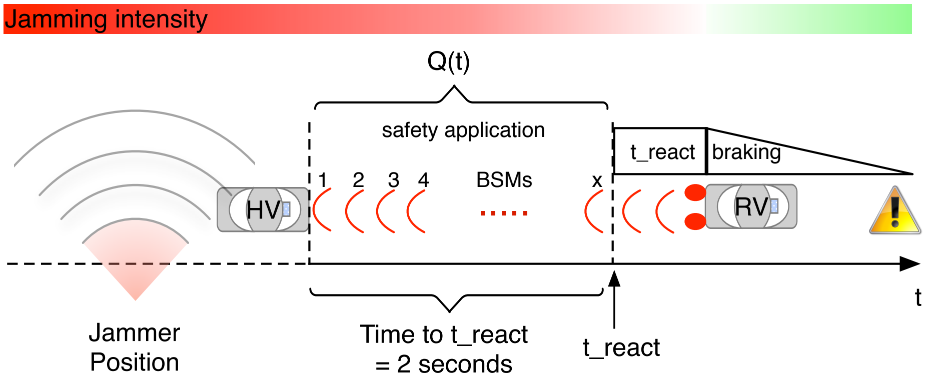

FIGURE 5.6: Constant jammer scenario

Next we study the impact of BSM rates, power levels and data rates on the unreliability $Q(t)$ of the Safety Application. As we always assume that the communication for BSMs occurs in the safety channel (CH172).

The Impact of BSM Rates — To look at the impact of BSM rates on safety application unreliability $Q(t)$ three different BSM rates have been studied, i.e., 10, 20 and 40 BSM/s, as shown in Figure 5.7. For this experiment, the transmission power was set to $P_t = 21\ dBm$, the jammer power was set to $P_j = 15\ dBm$, and the data rate was set to $R = 6\ Mbps$. The figure shows how $Q(t)$ is affected by jamming for different BSM rates. As can be seen $Q(t)$ is almost 1, indicating total failure, for the entire range up to $0.4s$ prior to t_{react}. High BSM rates show improvement, however the unreliability only decreases when there is almost no time left to react. BSM rates of 10 and 20 BSM/s resulted in unacceptable unreliabilities of more than 0.2 and 0.45 respectively. At time t_{react} (0 in the figure), only the message rate of 40 BSM/s satisfied the safety application's unreliability requirements with $Q(t_{react}) = 0.04$, implying a safety application reliability of 0.96. However, in general, this is too close to the cutoff allowing to react. On the other hand, in context of saving lives using Safety Applications, this still may be helpful. The above discussion only considers BSM rates and does not consider the impact of other adjustments, such as transmission power and data rates, as will be shown next.

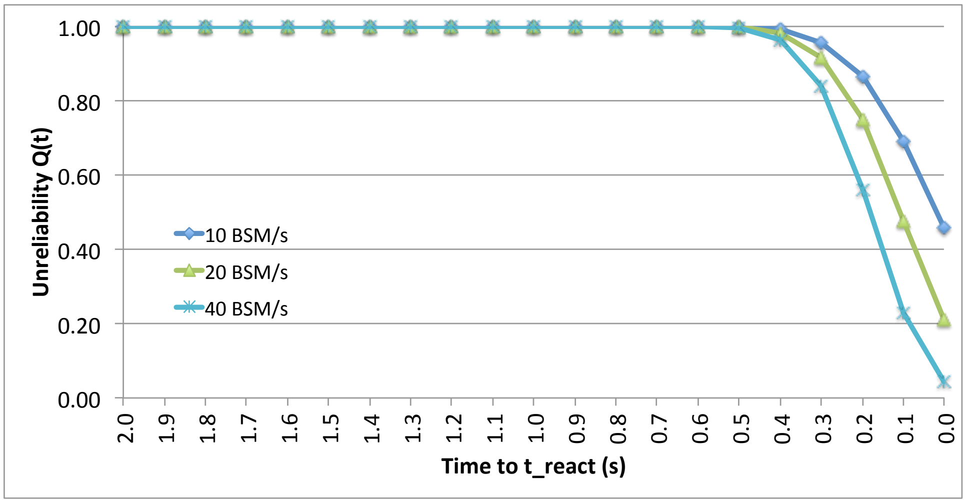

Figure 5.7: The impact of BSM rates on $Q(t)$

The Impact of Transmission Power — To investigate the impact of transmission power levels on $Q(t)$ three power levels have been examined, i.e., 21 dBm, 23 dBm and 25 dBm. In this experiment the BSM rate was fixed at a standard 10 BSM/s, the power of the jammer P_j was set to 15 dBm and the data rate was set to $R = 6\ Mbps$.

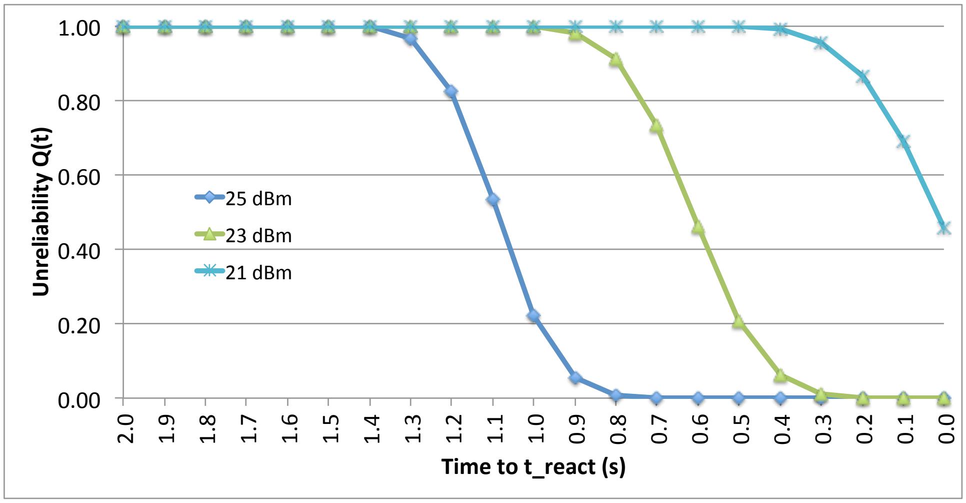

Figure 5.8: The impact of transmission power on $Q(t)$

Figure 5.8 shows how jamming affects $Q(t)$ for different transmission power levels. For a transmission power of 21 dBm, the unreliability remains at almost 1 most of the time, and $Q(t)$ starts to decrease only around $0.4s$ from t_{react}. However, for this power level $Q(t)$, was insufficient. Further increase in the transmission power to 23 dBm shows an earlier decline in $Q(t)$, which now starts to drop prior to $0.9s$ from t_{react} and reaches an acceptable unreliability around 0.4s before t_{react}. Finally, when the transmission power is set to 25 dBm, $Q(t)$ starts dropping around $1.4s$, reaching acceptable $Q(t)$ about $0.9s$ prior to t_{react}. The improvements in reliability is due to the increase of the SJR as the transmission signals get stronger. This is indeed favorable, since it contributes to allowing the Safety Application to receive at least 1 BSM before t_{react}. From a driver's point of view, higher transmission powers result in more time to react.

Note that the transmission power levels selected here are within the levels specified in the FCC amendment [48]. The amendment indicates that for public safety operations in CH172 the power levels shall not exceed 33 dBm EIRP, as was mentioned in Subsection 2.1.1.

The Impact of Data Rate — To look at the impact of data rates on $Q(t)$, two data rates have been investigated, i.e., 3 and 6 Mbps. In this experiment the power of the jammer P_j was set to 15 dBm, the transmission power to $P_t = 21$ dBm and the BSM rate was fixed at the standard 10 BSM/s. Higher data rates were not considered as they found to be unreliable in the case of constant jamming [64].

Figure 5.9 shows how jamming impacts the safety application unreliability for the two data rates. For 6 Mbps $Q(t)$ starts to decline only 0.4s before t_{react}, but never reaches acceptable unreliability. However, when the lower data rate of 3 Mbps was used, $Q(t)$ starts to decline before 1.1s and satisfies the application unreliability before 0.6s from t_{react}, thus giving the driver this additional time to react.

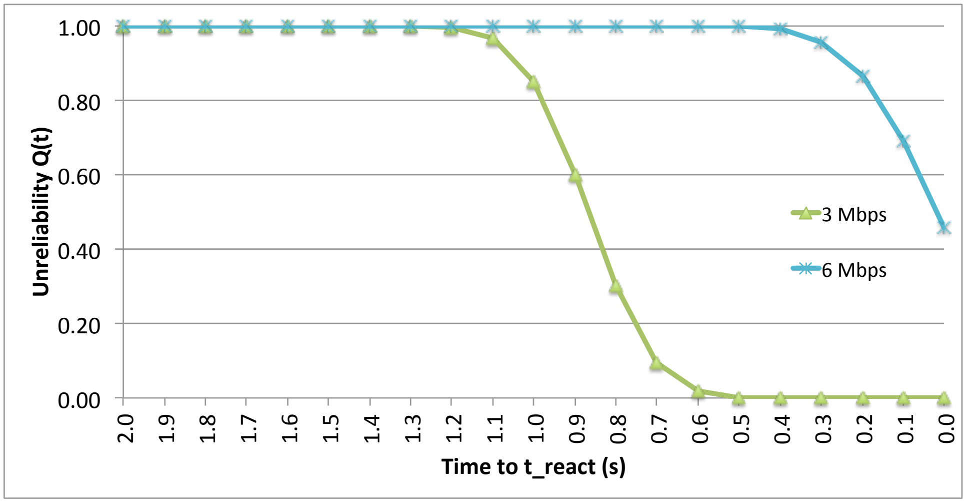

Figure 5.9: The impact of data rate on $Q(t)$

The advantage of using the lower data rates is due to the fact that the 3 Mbps data rate uses Binary Phase Shift Keying (BPSK) with coding rate of 1/2, whereas 6 Mbps uses Quadrature Phase Shift Keying (QPSK) with coding rate 1/2 as per the ASTM E2213 standard [39]. Higher modulation modes tends to be more prone to transmission errors, which causes increased BER [79].

5.5.2 *Deceptive Jammer*

The recovery concepts presented in Subsection 5.4.2 are now studied for the case of a deceptive jammer. Specifically, we focus on the impact of BSM rates, transmission power levels and data rates on the recovery time. Recall that in the case of a constant jammer, the unreliability $Q(t)$ was used to measure of the impact of each one of these parameter on the Safety Application. However, in the case of the deceptive jammer, the results were acquired by actual field experiments. Therefor, we can no longer obtain the individual Q_i, i.e., the probability that BSM_i was not received at t_i. Thus, to measure the impact of the BSM rates, the transmission power and the data rates, we use the *recovery time*, which we define as, the time required for the HV to resume steady reception after passing the jammer. Note that after the HV passes the jammer, intermittent reception of BSMs could take place, however, we assume that the communication is totally recovered only when a steady reception is resumed. The field experiments were conducted with an RV followed by an HV driving on a straight 2-lane road with an average speed of 35 mph (15.6 m/s), passing a stationary deceptive jammer on the roadside. The vehicles traverse in such moderate speed to allow better understanding of the impact of the tested parameters in the presence of the jammer, in addition, not over exceed the speed limit of the test road. The HV was followed by a third vehicle, which was included for the purpose of collecting additional data for future use, in addition to investigating its impact on the two communicating vehicles when leaving the jammed zone. The reception during these field experiments was studied from the HV point of view, as our concern is the vehicle receiving the alert messages.

The position of the test vehicles is shown in Figure 5.10. The RV is followed by the HV, which in turn is followed by a third vehicle. In Figure 5.10 a) the RV is the first vehicle exposed to the impact of deceptive jamming. This impact of the jammer is different when the vehicles have passed. This is depicted in Figure 5.10 b), where one would expect the last two vehicles to have a shielding effect on the RV. The impact of the jammer on the RV in the two scenarios, i.e., moving towards or leaving from the jammer position, is visible in the figures presenting the results of the field test below.

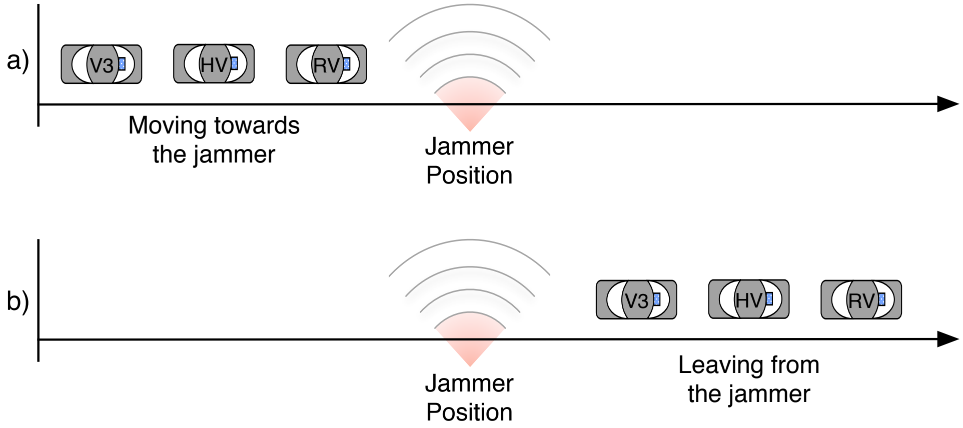

FIGURE 5.10: The position of the test vehicles before and after passing the jammer

TABLE 5.2: Field test parameters

OBU Model	Arada Systems LocoMate Classic
Vehicle speed	15.6 *m/s*
Test range	straight 2-lane road
Test range length	1000 m
Jammer position	500 m from starting point
BSM generation	10, 20, and 40 BSM/s
Channel	Safety Channel 172
Effective bandwidth	8.3 MHz
Transmitter power	21, 23 and 25 dBm
Transmitter data rate	3 and 6 Mbps
Jammer power and data rate	18 dBm and 6 Mbps

The exact parameters used for these field tests are shown in Table 5.2. For a more detailed information regarding the equipment and testing area we refer the reader to Section 4.5. However, some light will be shed on the challenges for conducting these field experiments next.

FIELD EXPERIMENT CHALLENGES — In this section we will discuss the challenges we encountered during the field experiments, their impact, and how we addressed them. The choice of ideal test conditions was important to ensure that the observed changes are due to the tested parameter, and not due to other external factors. To avoid and to eliminate these external factors, the field experiments were repeated several times. In our discussion, these conditions can be categorized into those related to the test road geometry, those related to the environment, and those related to the physical attributes of the OBUs and the test vehicles.

Road geometry: varying levels of elevation, or increased curvatures may impact the transmission between two test vehicles. These variations in the geometry of the test road can result in areas of missed communication or weakened reception of BSMs. This effect was experienced during earlier test trials, e.g., by experiencing loss of line of sight, which prompted us to experiment with different locations. The final choice for a test range was the straight two-lane road segment shown in Figure 5.11.

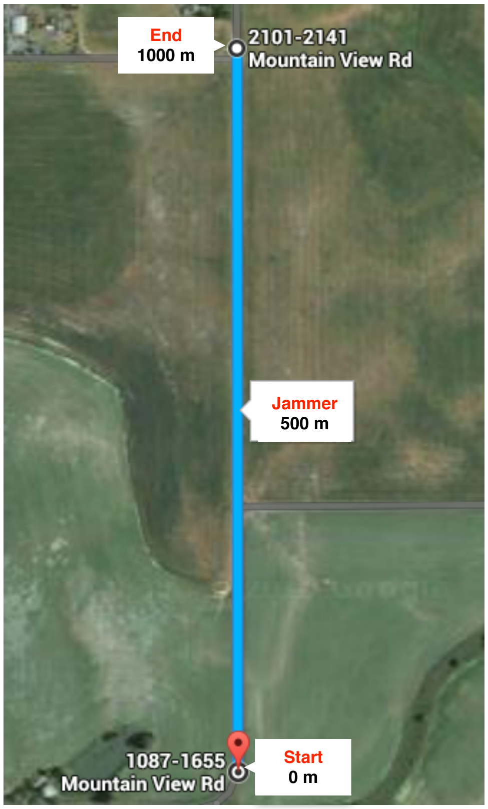

FIGURE 5.11: Testing range for the deceptive jammer

Environmental conditions: dense roads or heavily populated areas have the potential to increase the transmission impairments. In fact, any reflecting surfaces, such as buildings along roadsides or passing vehicles can cause attenuation due to losses and scattering, which degrade the signal strength and quality. To avoid these impairments, for the test road we picked a rural area with minimum traffic density and no buildings. However, we could not control traffic flow and thus occasional vehicles, as this was a public road. Furthermore, weather conditions impact the quality of the signals, such as increased heat or rain. Although several trials were performed in rainy conditions, we selected the results from the experiments conducted on clear days.

Physical aspects: the orientation of the antennas is crucial; OBUs use omni directional antennas [52], which radiate signals uniformly in all directions. Thus, changes in the antenna direction cause different areas of coverage. This, in fact, also affected our experiments and called for additional repetitions due to misplaced antenna direction. In order to avoid the impact of the vehicles themselves, such as metal parts, the antennas were placed on top of the test vehicles.

Physical aspects that relates to the vehicle's attributes, i.e., the inter-vehicle distance and the speed, are also important. Varying inter-vehicle distances could lead to fluctuation in the received signals. As the distance between the two vehicles changes, the level of signal strength and the overall SNR is affected. For that reason, efforts have been made to pace the two vehicles together, and maintain their inter-vehicle distance. However, closer analysis afterwards revealed variations in distance for different trials. Avoiding the effect of these variations in each experiment proved difficult, yet, conducting large numbers of trials was impractical due to the amount of effort associated with filed tests in terms of vehicle times and personnel involved. Extended longterm testing is beyond the scope of this dissertation. Thus, the results introduced next are typical scenarios from the field experiments, and are intended to show the potential of the recovery concepts in the presence of the deceptive jammer.

The Impact of BSM Rates — To study the impact of the BSM rates on the recovery time, three different BSM rates were tested, i.e., 10, 20 and 40 BSM/s. The results for each of these rates are shown in Figures 5.12, 5.13 and 5.14 respectively. In each case, the number of received BSMs by the HV is measured over the whole period of time; from the starting point to the end of the test area of Figure 5.11. The time in which the HV passes the jammer is marked with a dashed line. It can be observed that the passing time slightly differs in each figure, this is due to the small variations of the vehicle's speed during the different field trials.

Figure 5.12 shows the results of a typical experiment using the standard 10 BSM/s rate on the recovery time. When the HV passed the jammer at $t = 31s$ no BSMs were received. This is because at this point the impact of jamming is at its peak, and the HV is almost parallel to the jammer. Only after $12s$ from passing the jammer, a steady reception of BSMs was resumed, and the HV was again able to receive BSMs from the RV with only intermittent reception occurred prior that time.

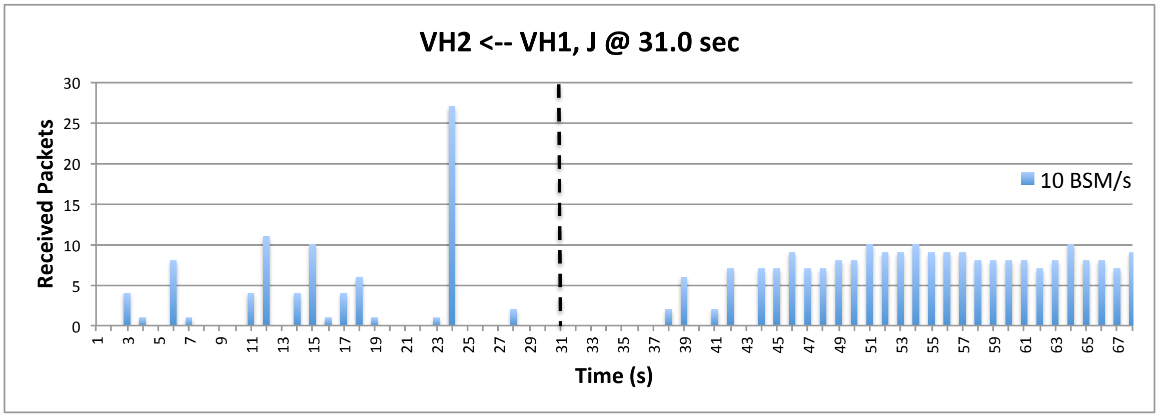

Figure 5.12: Reception using 10 BSM/s

The observed impact of sending at 20 BSM/s on the recovery time is shown in Figure 5.13. Now the RV has increased its sending rate to 20 BSM/s, and the HV passed the jammer at point $t = 31s$. As can be seen in the figure, the HV has regained steady reception at $t = 41s$ and thus, the observed recovery time for this trial was $9s$.

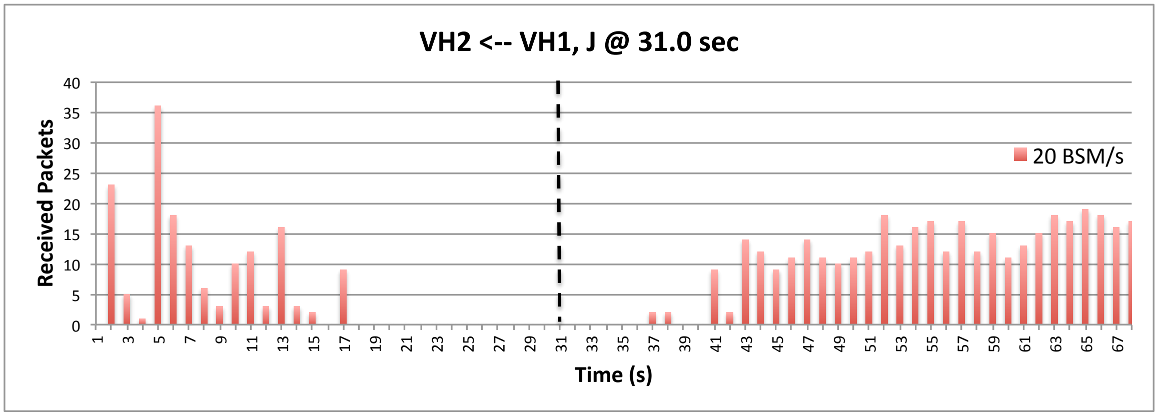

Figure 5.13: Reception using 20 BSM/s

Finally, Figure 5.14 shows the results of an experiment using 40 BSM/s, where the HV passed the jammer at $t = 29s$. In this scenario, the HV resumed receiving BSMs constantly from the RV at $t = 39s$, which accounts for a recovery time of $9s$.

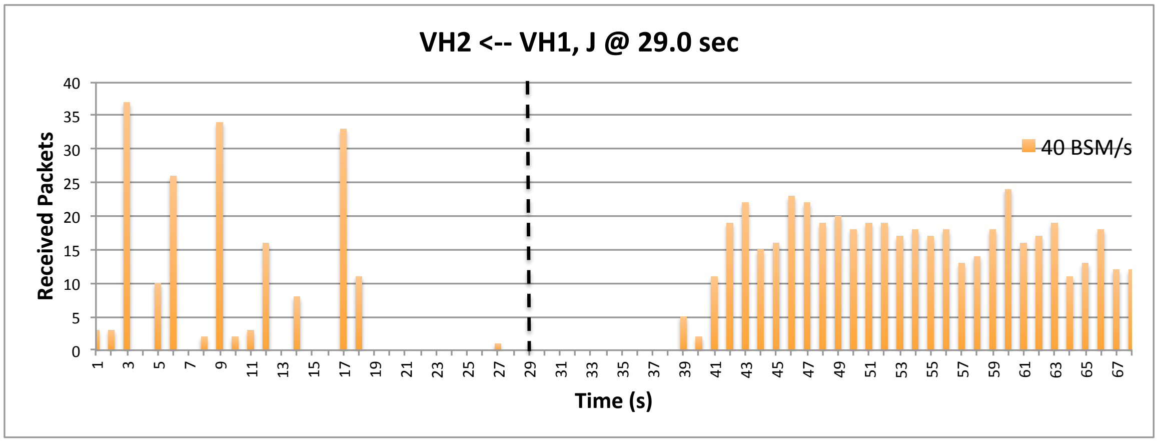

Figure 5.14: Reception using 40 BSM/s

The Impact of Transmission Power — To investigate the impact of transmission power on the recovery time in the presence of a deceptive jammer, three different power levels have been investigated, i.e., 21, 23 and 25 dBm. The impact of these different power levels on the recovery time for typical test runs is shown in Figures 5.15, 5.16 and 5.17 respectively.

A scenario which considers transmitting with power level of 21 dBm and the corresponding recovery time is shown in Figure 5.15 . Here, the HV passed the jammer at point $t = 31s$, and at this point the communication was dropped completely due the impact of the deceptive jammer. However, at point $t = 41s$ a steady reception of BSMs observed, which means the recovery time in this case was $9s$.

The case of transmission power level of 23 dBm and the resulting recovery time is shown in Figure 5.16. In this case, the HV passed the jammer at point $t = 28s$, and a steady reception was only resumed after $7s$ from the point where the HV passed the jammer.

A scenario that considers a transmission power level of 25 dBm is studied in Figure 5.17. In this figure, the HV passed the jammer at $t = 28s$, and regained

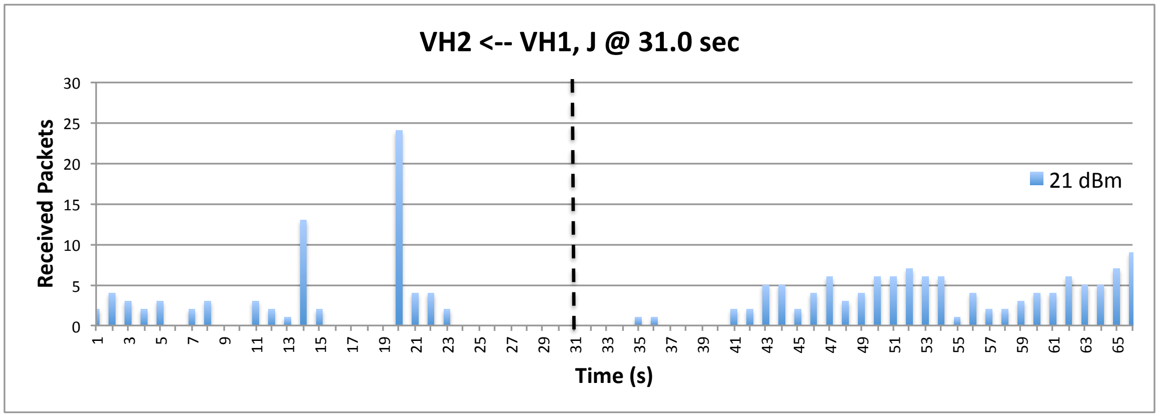

Figure 5.15: Reception using 21 dBm transmission power

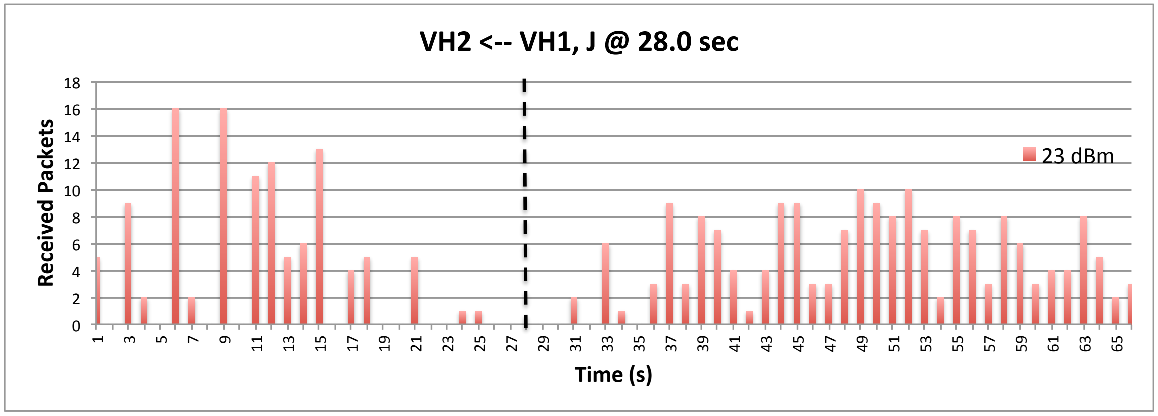

Figure 5.16: Reception using 23 dBm transmission power

steady reception by $t = 39s$. Thus, the observed recovery time when using this power level was $10s$.

The Impact of Data Rate — To look the impact of data rates on the recovery time, we have experimented with two different data rates, i.e., 3 and 6 Mbps. The results are depicted in Figures 5.18 and 5.19 respectively.

An example of using a data rate of 3 Mbps is shown in Figure 5.18. During this scenario, the HV passed the deceptive jammer at $t = 30s$, and resumed the reception of BSMs from the RV at $42s$. Thus the smaller data rate of 3 Mbps, has resulted in a recovery time of $11s$.

A scenario using 6 Mbps data rate is shown in Figure 5.19. In this trial, the HV passed the jammer at point $t = 31s$ and a constant reception of BSMs was regained at $t = 44s$, accounting for a recovery time of $12s$.

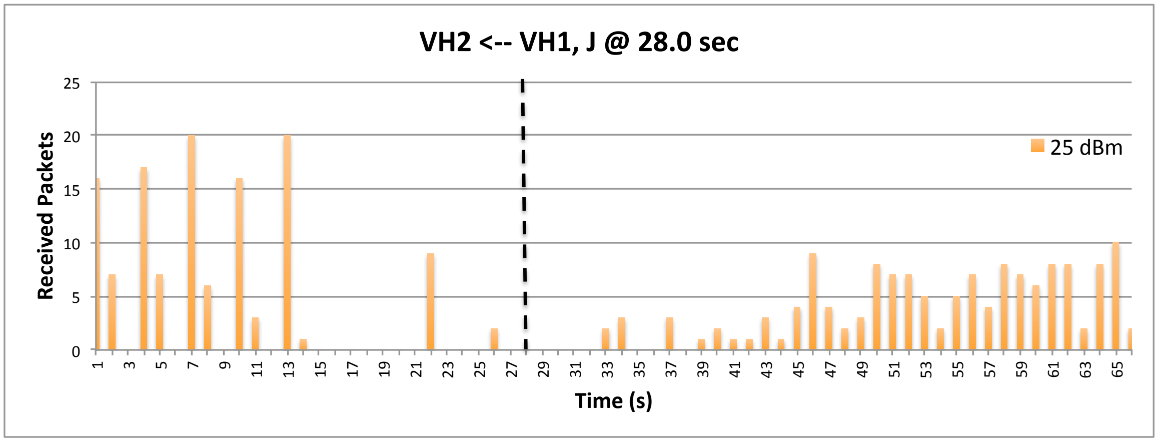

Figure 5.17: Reception using 25 dBm transmission power

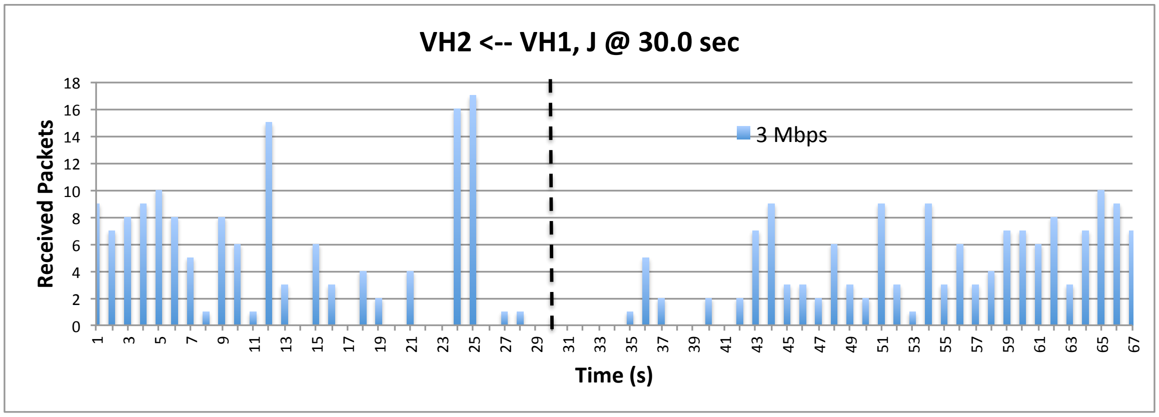

Figure 5.18: Reception using 3 Mbps data rate

After analyzing the data collected form the field experiments, abnormal spikes were observed. This behavior indicate that the number of received BSMs exceeds that of the transmitted ones. For instance, in Figure 5.12 at $t = 24s$ the number of received BSMs was more than 25, while the number of sent ones was 10. This abnormal behavior is due to fact that the deceptive jammer is preventing the OBU from accessing the media, during which time, the OBU queues the packets generated by the application layer for deferred sending. However, since jamming is taking place, packets were not sent in time, and accumulated over a period of time. This is mostly apparent in the beginning of the test period as the communication was partially affected by the jammer. Once the OBU gets momentarily access to the media, all queued packets were pushed at once, and thus, resulting in the spikes

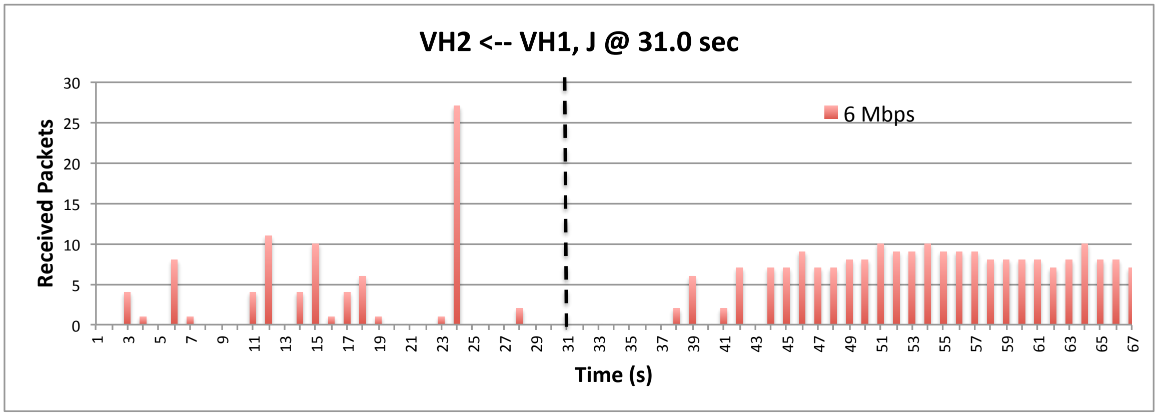

Figure 5.19: Reception using 6 Mbps data rate

observed. The queue, however, has a certain capacity, which prevents the buffering of all packets during such cases of prolonged inaccessibility to the media.

Table 5.3: Recovery times for deceptive jammer of the trials presented

Deceptive Jammer (Field Experiment)	**BSM/s**			**Power (dBm)**			**Data Rate (Mbps)**	
	10	20	40	21	23	25	3	6
Recovery Time (Seconds)	12.0	9.0	9.0	9.0	7.0	10.0	11.0	12.0
Distance (meters)	145	115	125	106	68.5	120	125	150

Table 5.3 shows the observed recovery times and distances between HV and RV for the representative cases presented. Given the aforementioned variability of results due to unavoidable differences in distances and environmental conditions, the observed results by themselves are inconclusive for generalization. However, the represented scenarios confirm what the mathematical models and intuition suggest. What appeared irregular behavior at first site, e.g., the increasing recovery time when the power level was increased from 23 dBm to 25 dBm, was the result of actual distances observed in the post analysis of the data. Thus, the reader should consider the column "Distance" when looking at the recovery times. Despite our best attempts to keep distances between different trials constant and consistent, this proved to be hard to achieve, e.g., without a towrope between vehicles. However, a facility to conduct such test was not available for the test range length required.

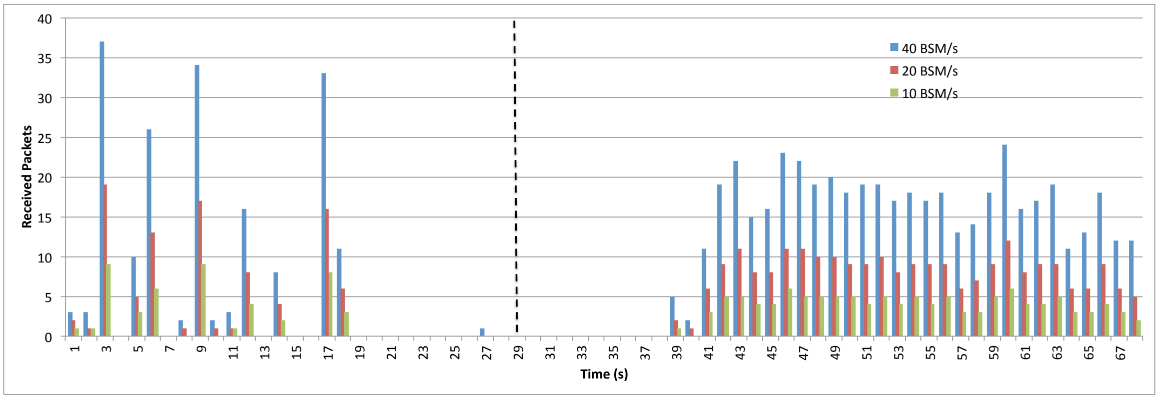

Figure 5.20: Comparing the impact of BSM rates

That said, in order to facilitate fair comparison with similar test conditions, one could mimic different BSM rates in a post analysis based on a single field trial. In Figure 5.20 we compare different BSM rates, i.e., 10, 20 and 40 BSM/s, based on the data of field test with 40 BSM/s. This allows us to understand the impact of different BSM rates while maintaining almost the exact same test conditions, i.e., environmental and physical, such as distances, antenna positions and speed. In the figure, the original data of 40 BSM/s was used to generate the case for 20 BSM/s by taking every second BSM. Likewise, the case of 10 BSM/s was generated by taking every fourth BSM. However, the aforementioned conditions using this approach are not exactly identical. The reason for this is that the transmitter queue behavior for 40 BSM/s is unlikely to be exactly the same for rates of 10 and 20 BSM/s. Now, sending at rate 10 BSM/s resulted in $11s$ recovery time, while sending at higher rates of 20 and 40 BSM/s resulted in less recovery time of $9s$. These results are in line with our previous observations during the field experiments, which were summarized in Table 5.3.

The real impact of transmission power levels for the deceptive jammer could not be directly observed, due to the variation in inter-vehicles distances during the field experiment. The variations in distances led to varying levels of SNR, which in turn impacted the reception of BSMs. Hence, the change in recovery times we observed during the field test was also affected by the distance between the test vehicles, i.e., a bigger distance resulted in longer recovery time.

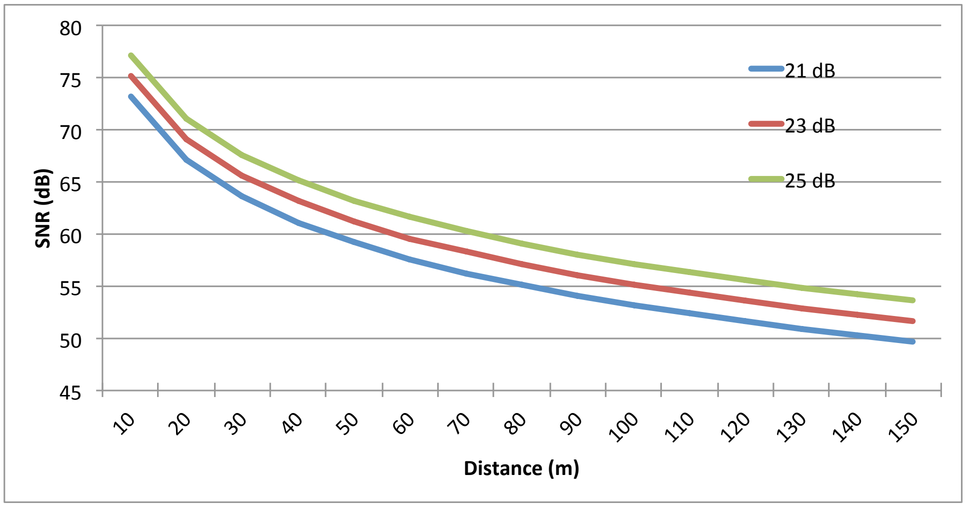

Figure 5.21: The impact of relative distance between vehicles on SNR

To understand the real impact of higher powers from a theoretical point of view, the relation between SNR levels and inter-vehicle distances are shown in Figure 5.21. For instance, if we assume a fixed distance of 100 m between the vehicles, we can observe the real impact of using higher transmission power. Now comparing for 23 dBm and 25 dBm at 100 m shows improvement in SNR levels. Higher SNR levels mean lower BER and overall higher chances of receiving messages [80].

Unlike the case of deceptive jammer where variation in physical conditions was hard to maintain, for the case of the constant jammer presented in Subsection 5.5.1, similar test conditions was achievable, since a mathematical model was used.

5.6 Conclusions

In this chapter we have proposed a new recovery strategy based on adjusting the communication parameters, i.e., BSM rates, transmission power levels and data rates only when jamming is detected. This has shown to help increase the reliability of the Safety Applications, by transitioning them from the jammed to the non jammed state faster. We have also studied the tradeoff between channel efficiency and reliability by investigating the impact of increased number BSMs in the safety channel. The maximum possible number of BSMs obtained for both cases, direct and indirect collisions. Direct collisions result from what is known as the hidden terminal situation. It was shown that for the case of hidden terminal case, the safety channel will struggle supporting high number of vehicles when sending at rates higher than 10 BSM/s.

We furthermore studied the concepts behind the recovery algorithm, by considering the impact of BSM rates, transmission power and data rates on the reliability of the Safety Applications, for both constant and deceptive jammers. For the constant jammer, increasing the BSM rates slightly improved the reliability of the Safety Application. However, only the message rate of 40 BSM/s could satisfy the unreliability requirement of the Safety Application, with $Q(t_{react}) = 0.04$. Increasing the transmission power, on the other hand, has improved the reliability of the Safety Application and has reduced the unreliability $Q(t)$. Finally, using the lower data rate of 3 Mbps improved the reliability of the Safety Application, and thus, allowing more time for the driver to react.

For the deceptive jammer, our field tests with commercial DSRC equipped vehicles, show that adjusting these parameters affected recovery times. In the experiments conducted we could observe a general trend of decreased recovery times as the BSM rate was increased. That trend was also confirmed by replicating different BSM rates using a single field test, in order to minimize unavoidable variations in field parameters. It also indicated that higher BSM rates result in less recovery time. The same was observed for decreased data rates or increased transmission power of the OBUs. However, as explained before, the variability of distances in the field tests had impact on the results, therefore making it impractical to compare different trial runs for each data point.

In summary, a novel recovery strategy was presented, that uses the concept of adjusting the rate of sending safety messages, transmission powers and data rates only when jamming is detected. The results, based on mathematical analysis and data collected during field tests, show that this recovery strategy can help the Safety Applications to transition from fail-safe mode to operational mode earlier. In the context of safety critical applications, this has the potential to reduce accidents and save lives.

CHAPTER 6

Conclusions and Future Work

The focus of this research was Safety Application reliability in VANETs. Several methods were suggested for improving the reliability of Safety Applications. In particular, we proposed three approaches to be incorporated into the application layer and Safety Application design, namely an adaptive threshold-based agreement algorithm, a jamming-aware Safety Application for detecting jamming attacks, and recovery using multiple parameter adjustments. These approaches were tested through simulations, analytical models, and field experiments, and the results show their effectiveness.

The critical nature of Safety Applications calls for higher reliability against potential failures, whether benign or malicious. It is paramount that Safety Applications reliably perform their basic functions even under hostile conditions, because their failures could have severe consequences, including injury and death.

Throughout this dissertation, we have considered wireless jamming as a source of malicious activity. The current standards have incorporated security mechanisms such as digital signatures, authentication, and encryption. However, these are not sufficient in the face of jamming attacks. Jamming is relatively easy to implement but has a high potential for destructiveness and can render Safety Applications useless. More aggressive attacks can be carried out through coordination between the jammer and other entities to cause havoc. Our algorithms operate within the limits of current standards, and may be useful for Safety Application developers or standards organizations.

In our first contribution, we proposed a novel threshold-based agreement algorithm. It is possible for an OBU to be misled into formulating faulty packets and having them digitally signed. Thus, techniques like content awareness and agreement are useful. The algorithm calculates the decision threshold from a number of vehicles in the proximity that actually witness an event. The results show improvement over the previous methods discussed in the literature.

As a second contribution, we have proposed a new algorithm for detecting the presence of jamming attacks and switching the Safety Application into a fail-safe mode. The algorithm is based on a multiple-metric approach and uses two metrics, i.e., the distance and the PDR. The field test results show that the new algorithm is capable of detecting the presence of a deceptive jammer and capable of switching the Safety Application to a fail-safe mode.

Finally, we introduced novel recovery strategies for improving Safety Application reliability. These strategies operate within the maximum limits identified in the standards for data rates and transmission power levels. The BSM transmission rates however, which go beyond what safety standards suggest, apply only during observed jamming. The idea of "shifting gears" was employed in this design. In our case, it means that three different communication parameters are dynamically adjusted when jamming is detected. It is the adjustments of the BSM rate, the transmission power level, and the data rate to the observed jamming that constitutes the "shifting." The results were twofold. First, for a constant jammer, the mathematical model showed improvement in the reliability of the Safety Application when higher BSM rates, higher power, and lower data rates were used. Second, for a deceptive jammer, the same was observed in most cases, but because of unavoidable variations in test conditions, such as inter-vehicle distances and speed, the results were not conclusive enough for generalized quantification. However, the variations of test conditions could be eliminated for the case of adjustments of the BSM rates, which followed the general trend observed.

Several avenues could be explored in future work. The algorithms presented here could be studied in combination with other kinds of malicious activities and faults, such as Sybil attacks and other induced value faults. In addition, stress tests and measurements of resource utilization for V2V communication equipment are necessary for determining the impact of these solutions in environments with high traffic density.

Whereas we have studied the impact of single parameters, i.e., BSM rates, power levels, and data rates, on the unreliability of Safety Applications in the case of constant jammers, we did not explicitly test the effect of coupling two or more parameters. However, it seems reasonable to expect that, by combining multiple parameters, the combined impact could lead to further improvements in reliability. The impact of such hybrid approach should be investigated further.

A multi-modal technique that combines DSRC with other available technologies such as radar, lidar and computer vision, could be studied to further improve the reliability of the Safety Applications in the presence of jamming. In addition, testing the algorithms to measure their performance in different settings, such as higher vehicle speeds or higher traffic density could be considered.

In this work we have tested the design concepts and algorithms with actual OBUs and laboratory settings and field experiments. However, it is imperative to combine and integrate the contributions in actual Safety Applications and evaluate their combined effectiveness.

Lastly, because field tests are very time- and resource-intensive, test procedures should be developed that result in less variability of key parameters, such vehicle speed and inter-vehicle distance.

During our research, we observed several important recurring motivational patterns:

1. Security mechanisms like digital signatures, authentication, and encryption are useful, but are insufficient in cases of deliberate denial-of-service and jamming attacks.

2. The detection of malicious activities is paramount and should be part of any design of Safety Applications rather than an add-on feature.

3. The incorporation of security measures into Safety Applications should conform to existing standardization efforts, as such solutions have higher chances of being adopted.

4. There is no substitute for practical field tests, and a long-term strategy for testing solutions is inevitable.

5. Safety Application reliability cannot be valued high enough. Any demonstrated maliciously induced failure could undermine public trust in the applications and their underlying technologies.

Bibliography

[1] *Traffic Safety Facts: Crash Stats*, U.S. Department of Transportation, National Highway Traffic Safety Administration, DOT HS 812 219, Nov 2015.

[2] M. H. Azadmanesh and R. M. Kieckhafer, *Exploiting Omissive Faults in Synchronous Approximate Agreement,* in IEEE Transactions on Computers, vol. 49, no. 10, pp. 1031-1042, Oct 2000.

[3] L. Lamport, R. Shostak and M. Pease, *The Byzantine Generals Problem,* in ACM Transactions on Programming Languages and Systems (TOPLAS), 1;4(3):382-401, Jul 1982.

[4] M. Pease, R. Shostak and L. Lamport, *Reaching Agreement in the Presence of Faults,* in Journal of the ACM (JACM), 1;27(2):228-34, Apr 1980.

[5] F. J. Meyer and D. K. Pradhan, *Consensus with Dual Failure Modes,* in IEEE Transactions on Parallel and Distributed Systems, vol. 2, no. 2, pp. 214-222, Apr 1991.

[6] P. Thambidurai and Y.K. Park, *Interactive consistency with multiple failure modes,* in Proceedings of the Seventh Symposium on Reliable Distributed Systems, Columbus, OH, pp. 93-100, 1988.

[7] W. B. Johnson, *Design and Analysis of Fault-Tolerant Digital Systems,* Addison-Wesley Publishing Company, New York, 1989.

[8] A. Avizienis, J. C. Laprie, B. Randell and C. Landwehr, *Basic concepts and taxonomy of dependable and secure computing,* in IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, pp. 11-33, Jan.-March 2004.

[9] M. Raya, and J. Hubaux, *The Security of Vehicular Ad Hoc Networks,* in Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks. ACM, 2005.

[10] M. Raya, P. Papadimitratos and J. p. Hubaux, *Securing Vehicular Communications,* in IEEE Wireless Communications, vol. 13, no. 5, pp. 8-15, October 2006.

[11] B. Parno and A. Perrig, *Challenges in Securing Vehicular Networks,* in Workshop on hot topics in networks (HotNets-IV), 2005.

[12] P. Golle, D. Greene and J. Staddon, *Detecting and Correcting Malicious Data in VANETs,* in Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks. ACM, 2004.

[13] S. Zeadally, R. Hunt, Y.S. Chen, A. Irwin and A. Hassan, *Vehicular Ad Hoc Networks (VANETS): Status, Results, and Challenges,* in Telecommunication Systems 50.4: 217-241, 2012.

[14] A. Studer, F. Bai, B. Bellur and A. Perrig, *Flexible, Extensible, and Efficient VANET Authentication,* in Communications and Networks, Journal of 11.6: 574-588, 2009.

[15] A. Studer, E. Shi, F. Bai and A. Perrig, *TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs,* in Sensor, Mesh and Ad Hoc Communications and Networks, pp. 1-9, 2009.

[16] Y. Hao, Y. Cheng, C. Zhou and W. Song, *A Distributed Key Management Framework with Cooperative Message Authentication in VANETs,* in IEEE Journal on Selected Areas in Communications, vol. 29, no. 3, pp. 616-629, March 2011.

[17] Jie Li, Huang Lu and M. Guizani, *ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs,* in IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 4, pp. 938-948, April 2015.

[18] J. Petit and Z. Mammeri, *Authentication and Consensus Overhead in Vehicular Ad Hoc Networks,* in Telecommunication systems 52.4: 2699-2712, 2013.

[19] Z. Cao, J. Kong, U. Lee, M. Gerla and Z. Chen, *Proof-of-relevance: Filtering False Data via Authentic Consensus in Vehicle Ad-hoc Networks,* in IEEE INFOCOM Workshops, pp. 1-6, 2008.

[20] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura and K. Sezaki, *CARAVAN: Providing Location Privacy for VANET,* in Washington University Seattle, Department of Electrical Engineering, 2005.

[21] K. Sampigethaya, M. Li, L. Huang and R. Poovendran, *AMOEBA: Robust Location Privacy Scheme for VANET,* in IEEE Journal on Selected Areas in Communications, vol. 25, no. 8, pp. 1569-1589, Oct. 2007.

[22] C.D. Jung, C. Sur, Y. Park and K.H. Rhee, *A Robust Conditional Privacy-Preserving Authentication Protocol in VANET,* in Security and Privacy in Mobile Information and Communication Systems. Springer Berlin Heidelberg, 35-45, 2009.

[23] X. Lin, X. Sun, P. H. Ho and X. Shen, *GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications,* in IEEE Transactions on Vehicular Technology, vol. 56, no. 6, pp. 3442-3456, Nov. 2007.

[24] C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin and N. Triandopoulos, *Anonysense: Privacy-Aware People-Centric Sensing,* in Proceedings of the 6th international conference on Mobile systems, applications, and services. ACM, 2008.

[25] J. Freudiger, M. Raya, M. Félegyházi and P. Papadimitratos, *Mix-Zones for Location Privacy in Vehicular Networks,* 2007.

[26] J. Shi, R. Zhang, Y. Liu and Y. Zhang, *PriSense: Privacy-Preserving Data Aggregation in People-Centric Urban Sensing Systems,* in IEEE INFOCOM, 2010 Proceedings, pp. 1-9, 2010.

[27] B. Awerbuch, A. Richa, and C. Scheideler, *A Jamming-Resistant MAC Protocol for Single-Hop Wireless Networks,* in Proceedings of the twenty-seventh ACM symposium on Principles of distributed computing. ACM, 2008.

[28] W. Xu, W. Trappe, and Y. Zhang, *Anti-Jamming Timing Channels for Wireless Networks,* in Proceedings of the first ACM conference on Wireless network security. ACM, 2008.

[29] G. Alnifie, and R. Simon, *A Multi-Channel Defense Against Jamming Attacks in Wireless Sensor Networks,* in Proceedings of the 3rd ACM workshop on QoS and security for wireless and mobile networks. ACM, 2007.

[30] A. Hamieh and J. Ben-Othman, *Detection of Jamming Attacks in Wireless Ad Hoc Networks Using Error Distribution,* in IEEE International Conference on Communications, Dresden, pp. 1-6, 2009.

[31] B. Wang, Y. Wu, K. J. R. Liu and T. C. Clancy, *An Anti-Jamming Stochastic Game for Cognitive Radio Networks,* in IEEE Journal on Selected Areas in Communications, vol. 29, no. 4, pp. 877-889, April 2011.

[32] R. Zhang, Y. Zhang and X. Huang, *JR-SND: Jamming-Resilient Secure Neighbor Discovery in Mobile Ad Hoc Networks,* in IEEE 31st International Conference on Distributed Computing Systems (ICDCS), Minneapolis, pp. 529-538, 2011.

[33] B. Xiao, B. Yu, and C. Gao. *Detection and Localization of Sybil Nodes in VANETs,* Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks. ACM, 2006.

[34] G. Guette and B. Ducourthial, *On the Sybil Attack Detection in VANET,* in IEEE International Conference on Mobile Adhoc and Sensor Systems, Pisa, pp. 1-6, 2007.

[35] M.S. Bouassida, G. Guette, M. Shawky and B. Ducourthial, *Sybil Nodes Detection Based on Received Signal Strength Variations within VANET,* in IJ Network Security 9.1: 22-33, 2009.

[36] J. Grover, M.S.Gaur, and V. Laxmi, *A Novel Defense Mechanism Against Sybil Attacks in VANET,* in Proceedings of the 3rd international conference on Security of information and networks. ACM, 2010.

[37] S. Ruj, M. A. Cavenaghi, Z. Huang, A. Nayak and I. Stojmenovic, *On Data-Centric Misbehavior Detection in VANETs,* in IEEE Vehicular Technology Conference (VTC Fall), San Francisco, CA, 2011, pp. 1-5, 2011.

[38] J. B. Kenney, *Dedicated Short-Range Communications (DSRC) Standards in the United States*, Proceedings of the IEEE, vol. 99, no. 7, pp. 1162-1182, 2011.

[39] *Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems - 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, ASTM E2213-03, 2010.

[40] *Dedicated Short Range Communications (DSRC) Message Set Dictionary. Society of Automotive Engineers*, SAE J2735, November 2009.

[41] *Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application*, Report DOT HS 812 014, August 2014.

[42] *IEEE Standard for Information technology–Telecommunications and information exchange between systems–Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments*, IEEE Std 802.11p, 2010.

[43] *IEEE 802.11, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Std., June 2007.

[44] *IEEE Draft Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture*, IEEE P1609.0â/D5, September 2012.

[45] *IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages*, IEEE Std 1609.2TM, 2013.

[46] *IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services*, IEEE Std 1609.3TM, 2010.

[47] *IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operation*, IEEE Std 1609.4TM, 2010.

[48] *Amendment of the Commission's Rules Regarding Dedicated Short-Range Communication Services in the 5.850-5.925 GHz Band (5.9 GHz Band)*, Federal Communications Commission FCC 03-324, 2004.

[49] B. Ostermaier, F. Dotzer and M. Strassberger, *Enhancing the Security of Local DangerWarnings in VANETs - A Simulative Analysis of Voting Schemes,* in The Second International Conference on Availability, Reliability and Security, pp. 422-431, Vienna, 2007.

[50] J. Petit and Z. Mammeri, *Dynamic Consensus for Secured Vehicular Ad Hoc Networks,* in IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 1-8, Wuhan, 2011.

[51] K. Pelechrinis, M. Iliofotou and S. V. Krishnamurthy, *Denial of Service Attacks in Wireless Networks: The Case of Jammers*, in IEEE Communications Surveys & Tutorials,, vol.13, no.2, pp.245,257, 2^{nd} Quarter 2011.

[52] Vehical Safety Communications-Applications (VSC-A) Final Report. DOT HS 811 492 A. U.S. Department of Transportation, NHTSA. September 2011.

[53] G. Di Crescenzo, Y. Ling, S. Pietrowicz and T. Zhang, *Non-interactive Malicious Behavior Detection in Vehicular Networks,* in IEEE Vehicular Networking Conference (VNC), Jersey City, NJ, pp. 278-285, 2010.

[54] M. Raya, A. Aziz, and J.P. Hubaux, *Efficient Secure Aggregation in VANETs,* in Proceedings of the 3rd international workshop on Vehicular ad hoc networks. ACM, pp. 67-75, 2006.

[55] A. D. May, *Traffic Flow Fundamentals*, Englewood Cliffs, NJ: Prentice-Hall, 1990.

[56] W. Xu, K. Ma, W. Trappe and Y. Zhang, *Jamming Sensor Networks: Attack and Defense Strategies,* in IEEE Network, vol. 20, no. 3, pp. 41-47, May-June 2006.

[57] W. Xu, T. Wood, W. Trappe, and Y. Zhang, *Channel Surfing and Spatial Retreats: Defenses Against Wireless Denial of Service,* In Proceedings of the 3rd ACM workshop on Wireless security (WiSe '04), New York, NY, USA, p80-89, 2004.

[58] *Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems - 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, ASTM E2213-03, 2010.

[59] G. Noubir, *On Connectivity in Ad Hoc Networks Under Jamming using Directional Antennas and Mobility,* In Wired/Wireless Internet Communications, pp. 186-200, Springer Berlin Heidelberg, Feb. 2004.

[60] G. Noubir and G. Lin, *Low-Power DoS Attacks in Data Wireless LANs and Countermeasures,* in SIGMOBILE Mobile Computing and Communications Review, p29-30, July 2003.

[61] A. D. Wood, J. A. Stankovic and G. Zhou, *DEEJAM: Defeating Energy-Efficient Jamming in IEEE 802.15.4-based Wireless Networks,* in 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, SECON '07, San Diego, CA, pp. 60-69, 2007.

[62] M. D. Aime, G. Calandriello and A. Lioy, *A Wireless Distributed Intrusion Detection System and a New Attack Model,* in 11th IEEE Symposium on Computers and Communications, ISCC '06. Proceedings, pp. 35-40, 2006.

[63] A. Serageldin, H. Alturkostani and A. Krings, *On the Reliability of DSRC Safety Applications: A Case of Jamming,* in IEEE International Conference on Connected Vehicles and Expo (ICCVE), Las Vegas, NV, pp. 501-506, 2013.

[64] A. Serageldin and A. Krings, *The Impact of Redundancy on DSRC Safety Application Reliability under Different Data Rates,* in 6th International Conference on New Technologies, Mobility and Security (NTMS), Dubai, pp. 1-5, 2014

[65] A. Serageldin and A. Krings, *The Impact of Dissimilarity and Redundancy on the Reliability of DSRC Safety Applications,* in 28th International Conference on Advanced Information Networking and Applications Workshops (WAINA), Victoria, BC, pp. 417-424, 2014.

[66] O. Puñal, A. Aguiar, and J. Gross, *In VANETs we Trust?: Characterizing RF Jamming in Vehicular Networks,* In Proceedings of the ninth ACM international workshop on Vehicular inter-networking, systems, and applications (VANET '12). ACM, New York, NY, p83-92, 2012.

[67] A. Hamieh, J. Ben-Othman and L. Mokdad, *Detection of Radio Interference Attacks in VANET,* in IEEE Global Telecommunications Conference, GLOBECOM 2009, Honolulu, HI, pp. 1-5 2009.

[68] N. Lyamin, A. Vinel, M. Jonsson and J. Loo, *Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks,* in IEEE Communications Letters, vol. 18, no. 1, pp. 110-113, January 2014.

[69] A.T. Nguyen, L. Mokdad, and J. Ben-Othman, *Solution of Detecting Jamming Attacks in Vehicle Ad Hoc Networks,* In Proceedings of the 16th ACM international conference on Modeling, analysis & simulation of wireless and mobile systems (MSWiM '13). ACM, New York, NY, USA, p405-410, 2013.

[70] Ó. Puñal, C. Pereira, A. Aguiar and J. Gross, *Experimental Characterization and Modeling of RF Jamming Attacks on VANETs,* in IEEE Transactions on Vehicular Technology, vol. 64, no. 2, pp. 524-540, Feb. 2015.

[71] Sklar, B. *Digital Communications: Fundamentals and Applications*, 2nd Edition, Prentice Hall PTR, 2001.

[72] J. Peng, L. Cheng and B. Sikdar, *A Wireless MAC Protocol with Collision Detection,* in IEEE Transactions on Mobile Computing, vol. 6, no. 12, pp. 1357-1369, Dec. 2007.

[73] Arada Systems, www.aradasystems.com

[74] W. Xu, W. Trappe, Y. Zhang, and T. Wood, *The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks,* In Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing (MobiHoc '05). ACM, New York, NY, USA, p46-57, 2005.

[75] H. Alturkostani, A. Chitrakar, R. Rinker, and A. Krings, *On the Design of Jamming-Aware Safety Applications in VANETs,* in Cyber and Information Security Research Conference (CISR 2015), Oak Ridge National Laboratory, Tennessee, USA, April 2015.

[76] W. B. Johnson, *Design and Analysis of Fault-Tolerant Digital Systems*, Addison-Wesley Publishing Company, New York, 1989.

[77] G. Johansson and K. Rumar, *Drivers? Brake Reaction Times,* in HumanFactors The Journal of the Human Factors and Ergonomics Society 13, no.1, pp.23-27, 1971.

[78] M.I. Hassan, H.L.Vu, T. Sakurai, *Performance Analysis of the IEEE 802.11 MAC Protocol for DSRC Safety Applications,* in IEEE Transactions on Vehicular Technology, vol.60, no.8, p.3882-3896, Oct. 2011.

[79] L. Hanzo, M. Munster, B. Choi and T. Keller, *OFDM and MC-CDMA for Broadband Multi User Communications, WLANs and Broadcasting,* John Wiley & Sons, Jan 28, 2005.

[80] R. A. Shafik, M. S. Rahman and A. R. Islam, *On the Extended Relationships Among EVM, BER and SNR as Performance Metrics,* in the International Conference on Electrical and Computer Engineering, ICECE '06., Dhaka, pp. 408-411, 2006.

APPENDIX A
MatLab Functions

The following are the MatLab functions that have been used in Chapter 3. The code has been divided into several functions, in order to generate mobility, simulate transmission and jamming and to calculate agreement.

A.1 MOBILITY GENERATION FUNCTION

```
function [Dist, movement] = mobility(T,max_time,acceleration,
    deceleration,max_speed,Tbrake_start,Tbrake_end,N)

%calculate the speed and distance for a lead vehicle according
     to car
%following model in one lane highway. All inputs are metric.
%N is the number of following vehicles in one lane

%%
% Lead vehicle in one lane

%initiate timer up to max_time seconds with T step
time=0:T:max_time;
time=time';
a=length(time);

%convert acceleration and deceleration from m/s^2 to ft/s^2
acceleration=acceleration/0.3048;
deceleration=deceleration/0.3048;

%convert max_speed from m/s to Mph
```

```
max_speed=max_speed*2.23694;

%initiate acceleration matrix
acc = ones (1,a);
acc = acc.*acceleration;
acc = acc';

%initiate speed matrix
speed = zeros (1,a);
speed_Mph = zeros (1,a);
speed_mps = zeros (1,a);
speed_Mph=speed_Mph';
speed = speed';
speed_mps = speed_mps';

%calculate acceleration/deceleration matrix according to
   braking times
for j=2:a
    speed (j) = speed (j-1) + ((acc(j-1)+acc(j))/2)*T;
    speed_Mph (j) = (speed (j)*60*60)/5280;

    if time(j) < Tbrake_start && speed_Mph(j)<max_speed;
        acc(j)= accelration;

    elseif time(j) > Tbrake_end && speed_Mph(j)<max_speed;
        acc(j)= 0.0;

    elseif time(j)>= Tbrake_start && time(j)<= Tbrake_end
        acc(j)=decleration;

    else
```

```
        acc(j)=0.0;
    end

end

%calculate speed and convert from feet/s to mile/h
for j=2:a
    speed (j) = speed (j-1) + ((acc(j-1)+acc(j))/2)*T;
    if speed (j) < 0
        speed (j) = 0;
    end
    speed_Mph (j) = (speed (j)*60*60)/5280;
    speed_mps (j) = ((speed_Mph (j) *1.60934*1000)/3600);

end

%calculate distance from starting point

distance = zeros (1,a);
distance_m = zeros (1,a);
distance = distance';
distance_m = distance_m';

for j=2:a
    distance (j) = distance (j-1) + (speed (j-1) * T) + (((acc
        (j-1) + acc (j))/2))*((T^2)/2);
    distance_m (j) = distance (j-1) ./ 3.2808;
end

%%
% Following vehicles
% initiate acc, speed and dist
T_react=1; %reaction time (seconds)
%N=30; %number of vehicles
D_headway=-131; %distance headway (spacing between vehicles) (ft)
Sensitivity=0.5; %sensitivity parameter (sec^-1)

v{1}(2,:)=speed; %assigning initial lead vehicle speed

for i=1:N
   v{i}(1,:)=[time];
   v{i}(3,:)=zeros(1,a); %acc (ft/s^2)
   v{i}(4,:)=zeros(1,a); %speed (ft/s)
   v{i}(5,:)=zeros(1,a); %dist (ft)
   v{i}(6,:)=zeros(1,a); %speed (m/s)
   v{i}(7,:)=zeros(1,a); %distance (m)
   v{i}=v{i}';

    for j=2:a
    %calculate acceleration (ft/s^2)
    v{i}(j,3)=(Sensitivity*(v{i}(j-1,2)-v{i}(j-1,4)))*(T_react/T);

    %calculate speed (ft/s)
    v{i}(j,4) = v{i}(j-1,4) + ((v{i}(j-1,3)+v{i}(j,3))/2)*T;
        if v{i}(j,4) < 0
             v{i}(j,4) = 0;
        end

    %convert speed from ft/s to m/s
    v{i}(j,6) = (v{i}(j,4)*60*60)/5280;
```

```
        v{i}(j,6) = (( v{i}(j,6) *1.60934*1000)/3600);

        %replace the speed value of the leading vehicle
        v{i+1}(2,j)=v{i}(j,4);

        %calculate the distance (ft)
        v{i}(1,5) = D_headway *(i); %spacing between vehicles
        v{i}(j,5) = v{i}(j-1,5) + (v{i}(j-1,4) * T) + (((v{i}(j-1,3) + v{i}(j,3))/2))*((T^2)/2);

        %convert distance from ft to m
        v{i}(1,7) = v{i}(2,5) ./ 3.2808;
        v{i}(j,7) = v{i}(j,5) ./ 3.2808;
        end

end

% %return movement matrix for the lead vehicle and following vehicles

movement= cell(1,N);
for i=1:N
    movement{i}= [v{i}(:,3) v{i}(:,6) v{i}(:,7)];
    %movement{i}= dataset({movement{i} ['Acc_' num2str(i)] ,['Speed_' num2str(i)],['Distance_' num2str(i)]});
end

%uncomment following two lines for exporting to MS Excel
%movement = cell2mat(movement);
%movement = [time acc speed_mps distance_m movement]
```

```
%%
%calculate relative distance
Dist= cell(1,N);

for i=1:N
    for j=1:N
        Dist{j,i} = movement{i}(:,3)-movement{j}(:,3);
    end
end
```

A.2 TRANSMISSION FUNCTION

```
function [BSM, total_received]=transmission

%This function calculate basic safety message reception for
    each vehicle
% The output is as follows , v{to ,from}
%―――――――――――――――――――――――――――――――――――――――――
% Time | Distance | BER | BSM | Brake |
%―――――――――――――――――――――――――――――――――――――――――
%
% Time: Time Stamp of received Message
% From: Specify the sender vehicle
% Distance: Relative distance between sender and receiver
% BER: Bit Error Rate for physical layer
% BSM: 1= successfully received , 0= Not received

%
% The mobility function will be used as mobility model for
    physical movement
% of vehicles , values can be used , such as relative distance ,
    speed ,
% deceleration , etc .
%
% Transmission distance will be set to 300m
%
% PDR, Throughput for specific vehicles or group of vehicles
    can be
% obtained

%The following are suppose to be the same for all lanes:
```

```
%T: step time (seconds)
%max_time: overall travel time for all vehicles (seconds)
T=0.1;
max_time=120;
N=30; %number of vehicles

%initiate timer up to max_time seconds with T step
time=0:T:max_time;
time=time';
a=length(time);

%initiate Bit Error Rate
BER= ones(a,1);
BER= BER.*10e-6;



%initiate reception
received= zeros (a,1);
brake=zeros (a,1);



%calculate mobility
[distance, movement]=mobility(T,max_time,1.1,-1.4,15,50,70,N);

BSM = cell(N,N);

for i=1:N
    for j=1:N
        for m=1:a
            if abs(distance{i,j}(m)) < 300 && abs(distance{i,j
                }(m))>0
                received (m,1)=1;
            elseif abs(distance{i,j}(m)) == 0
                received (m,1)=0;
            else
                received (m,1)=0;
            end

            if movement{1,j}(m) < 0
                brake(m,1)=1;
            else
                brake(m,1)=0;
            end
        BSM{i,j}=[time, abs(distance{i,j}), BER, received,
           brake];
        end
    end
end

for i=1:N
    for j=1:N
        total_received(i,j)= sum(BSM{i,j}(:,4));
    end
end
```

A.3 JAMMING FUNCTION

```
function [BER]=jamming(Pt,Pj,R,B,L)

%Pt: Power of transmitter (dBm)
%Pj: Power of jammer (dBm)
%R: Data Rate (bits/sec)
%B: Bandwidth (Hz)
%L: Packet length (bits)

% Pt=20;
% Pj=15;
% R=6e6;
% B=8.3e6;
% L=2400;

%This function calculate (SJR) Signal to Jamming Ratio and Bit
    Error Rate (BER)
%for each receiving vehicle under the effect of jamming.

%The function uses the relative distances between the two
   vehicles which
%has been calculated in the mobility function.

%The following are suppose to be the same for all lanes:
%T: step time (seconds)
%max_time: overall travel time for all vehicles (seconds)
T=0.1;
max_time=120;
N=30; %number of vehicles
```

```
%initiate timer up to max_time seconds with T step
time=0:T:max_time;
time=time';
a=length(time);



%calculate mobility
[distance, movement]=mobility(T,max_time,1.1,-1.4,15,50,70,N);

%Jammer Position (meters)
Rj=560;

%convert powers from (dBm) to (watts)
Pt=10^(Pt/10)/1000;
Pj=10^(Pj/10)/1000;

BER = cell(N,N);
SJR= zeros (a,1);
SJRdBm = zeros (a,1);
EbNo= zeros (a,1);
Pb= zeros (a,1);
Pp= zeros (a,1);

for i=1:N
    for j=1:N
        for m=1:a
            if i~=j
                SJR(m,1)=(Pt*((Rj-movement{1,j}(m,3))^2))/((
                    Pj*((distance{i,j}(m))^2)));
                SJRdBm(m,1)=log(SJR(m,1))*10;
                EbNo(m,1)=(SJR(m,1)*B)/R;
                Pb(m,1)=0.5*(erfc(sqrt(EbNo(m,1))));
                Pp(m,1)=(1-((1-Pb(m,1))^L));

            else
                SJR(m,1)=0;
                SJRdBm(m,1)=0;
                EbNo(m,1)=0;
                Pb(m,1)=0;
                Pp(m,1)=0;
            end
            BER{i,j}=[time, SJR, SJRdBm, EbNo,Pb, Pp];
        end
    end
end
```

A.4 TRANSMISSION WITH JAMMING FUNCTION

```
function [BSM, total_received]=transmission_jamming

%This function calculate basic safety message reception for
    each vehicle
% The output is as follows, v{to,from}
%------------------------------------------------------------------
% Time | Distance | BER | BSM | Brake|
%------------------------------------------------------------------
%
% Distance: Relative distance between sender and receiver
% BER: Bit Error Rate for physical layer
% BSM: 1= successfully received , 0= Not received

%
% The mobility function will be used as mobility model for
    physical movement
% of vehicles, values can be used, such as relative distance,
    speed,
% deceleration, etc.
%
% Transmission distance will be set to 300m
%
% PDR, Throughput for specific vehicles or group of vehicles
    can be
% obtained

%The following are suppose to be the same for all lanes:
%T: step time (seconds)
%max_time: overall travel time for all vehicles (seconds)
```

```
T=0.1;
max_time=120;
N=30; %number of vehicles

%initiate timer up to max_time seconds with T step
time=0:T:max_time;
time=time';
a=length(time);

%initiate Bit Error Rate
% BER= ones(a,1);
% BER= BER.*10e-6;

[BER]=jamming(20,10,6e6,8.3e6,2400);



%initiate reception
received= zeros (a,1);
brake=zeros (a,1);
%calculate MAC
% needs to have MAC model here

%calculate mobility
[distance, movement]=mobility(T,max_time,1.1,-1.4,15,50,70,N);

BSM = cell(N,N);

for i=1:N
    for j=1:N
        for m=1:a
```

```
            if abs(distance{i,j}(m)) < 300 && abs(distance{i,j}(m))>0 && BER{i,j}(m,5)<0.00125
                received (m,1)=1;
            elseif abs(distance{i,j}(m)) == 0
                received (m,1)=0;
            else
                received (m,1)=0;
            end

            if movement{1,j}(m) < 0
                brake(m,1)=1;
            else
                brake(m,1)=0;
            end
        BSM{i,j}=[time, abs(distance{i,j}),BER{i,j}(:,5),
           received, brake];
        end
    end
end

for i=1:N
    for j=1:N
        total_received(i,j)= sum(BSM{i,j}(:,4));
    end
end
```

A.5 AGREEMENT FUNCTION

```
%The following are suppose to be the same for all lanes:
%T: step time (seconds)
%max_time: overall travel time for all vehicles (seconds)
T=0.1;
max_time=120;
N=30; %number of vehicles

%initiate timer up to max_time seconds with T step
time=0:T:max_time;
time=time';
a=length(time);

%calculate mobility
[distance, movement]=mobility(T,max_time,1.1,-1.4,15,50,70,N);

Nr=0; %total number of vehicles in decision area for event (i
    )
Ns=0; %total number of vehicles in detection area for event (
    i)

transmission_range=300;
detection_area=100;

event_loc_start=movement{1,1}(501,3);
event_loc_end=movement{1,1}(612,3);

braking_distance=event_loc_end-event_loc_start;
reaction_distance=1*15;
```

```
diss_area_start=event_loc_start-transmission_range;
diss_area_end=event_loc_end-detection_area-braking_distance-
   reaction_distance;

detect_area_start=event_loc_end-detection_area;
detect_area_end=event_loc_end;

for i=1:N
        for m=1:a
            if m>501 && m<612 && movement{1,i}(m,3) >
               diss_area_start && movement{1,i}(m,3)<
               diss_area_end
                Nr=Nr+1;
                break
            elseif m>501 && m<612 && movement{1,i}(m,3) >
               detect_area_start && movement{1,i}(m,3)<
               detect_area_end
                Ns=Ns+1;
                break
            end
        end
end


%calculate overall transmission
[BSM,total]=transmission_jamming;

%BSM reception during event (i)
for i=1:N
    for j=1:N
        BSM_event{i,j}=BSM{i,j}(501:612,:);
    end
end



%initiate timer for event (i)
time_event=50:T:61;
time_event=time_event';
b=length(time_event);

%build agreement table
agreement = cell (1,Nr);

for i=Ns+1:Ns+Nr
    for j=1:Ns
        for m=1:a
            if BSM{i,j}(m,4)==1 && BSM{i,j}(m,5)==1
                agreement{1,i}(m,j)=1 %BSM and alert received
            elseif BSM{i,j}(m,4)==1 && BSM{i,j}(m,5)==0
                agreement{1,i}(m,j)=2 %BSM received and no
                   alert received
            elseif BSM{i,j}(m,4)==0
                agreement{1,i}(m,j)=0 %No BSM received
            end

        end
    end
    agreement{1,i}=[time, agreement{1,i}];
end

%build decision table
sum_no_alert=zeros(a,1);
```

```
sum_count=zeros(a,1);
sum_alert=zeros(a,1);

positive_decision=zeros(a,1);
%negative_decision=zeros(a,1);

%lower_threshold=10;
%upper_threshold=20;     %static

decision= cell(1,Nr);

for i=Ns+1:Ns+Nr
    total_alert= zeros(a,1);
    total_no_alert= zeros(a,1);
    total_count=zeros(a,1);
    for j=2:Ns+1
        for m=1:a
            if agreement{1,i}(m,j)==1
                total_alert(m)=total_alert(m)+1;
            elseif agreement{1,i}(m,j)==2
                total_no_alert(m)=total_no_alert(m)+1;
            end
            total_count(m)=total_alert(m)+total_no_alert(m);
        end
    end
    decision{1,i}=[time, total_alert, total_no_alert,
       total_count, sum_alert, sum_no_alert, sum_count,
       positive_decision];
end
s=1;
```

```
for i=Ns+1:Ns+Nr
    for m=1:a
        upper_threshold=(decision{1,i}(m,4)*(0.3*10));
        decision{1,i}(m,5)=sum(decision{1,i}(s:m,2)); %
           sum_alerts
        decision{1,i}(m,6)=sum(decision{1,i}(s:m,3)); %
           sum_no_alerts
        decision{1,i}(m,7)=sum(decision{1,i}(s:m,4)); %
           sum_count
            if decision{1,i}(m,7)>upper_threshold && decision
               {1,i}(m,5)>decision{1,i}(m,6)
            decision{1,i}(m,8)=1;    %alert
            s=m+1;
            elseif decision{1,i}(m,7)>upper_threshold &&
               decision{1,i}(m,5)<decision{1,i}(m,6)
            decision{1,i}(m,8)=2;    %no alert
            s=m+1;
            else
            decision{1,i}(m,8)=0; %delayed
            end
           %s=1;
    end
    s=1;
end

%calculate total decisions in decision area
correct=0;
incorrect=0;
total_decisions=0;

for i=Ns+1:Ns+Nr;
```

```
    for m=501:611
        if decision{1,i}(m,8)==1;
            correct=correct+1;
        elseif decision{1,i}(m,8)==2
            incorrect=incorrect+1;
        end
        total_decisions=correct+incorrect;    %dynamic/Adaptive
    end
end
        %total_decisions=(floor(b/(upper_threshold/Ns)))*(Nr);
              %static
        precentage_correct=correct/total_decisions
        %precentage_incorrect=incorrect/total_decisions
        precentage_incorrect=1-precentage_correct

%calculate Packet Delivery Ratio in Dissemination Area
sent=Ns*b*Nr; %total packets sent
received=0;
for i=Ns+1:Ns+Nr
    received= received+sum(decision{1,i}(501:611,4));
end
PDR=received/sent
```