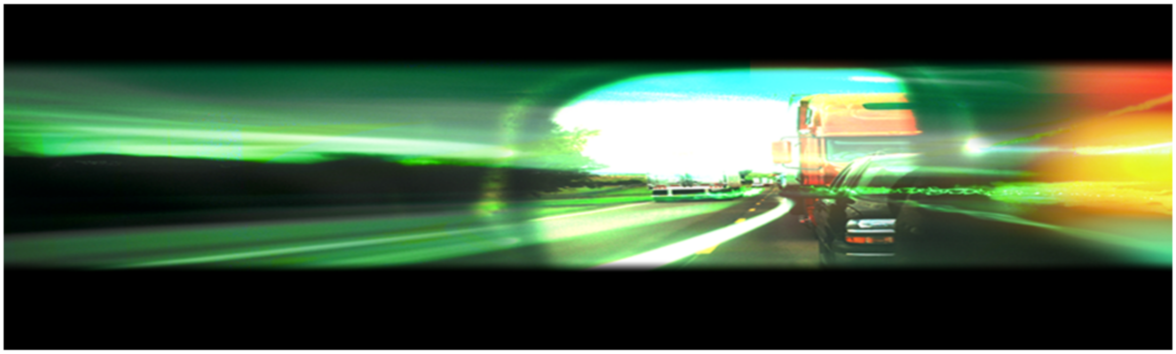


REAL-TIME COMMUNICATION ARCHITECTURE for CONNECTED-VEHICLE ECO-TRAFFIC SIGNAL SYSTEM APPLICATIONS

Final Report

Prepared for

US Department of Transportation
Research and Special Programs Administration

Axel Krings, Ahmed Serageldin,
Ahmed Abdel-Rahim, and Michael Dixon

February 2014

DISCLAIMER

The contents of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the information presented herein. This document is disseminated under the sponsorship of the Department of Transportation, University Transportation Centers Program, in the interest of information exchange. The U.S. Government assumes no liability for the contents or use thereof.

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.

4. Title and Subtitle Security and Survivability of Real-Time Communication Architecture for Connected-Vehicle Eco-Traffic Signal System Applications	5. Report Date February 2014
	6. Performing Organization Code KLK903
7. Author(s) Axel Krings, Ahmed Serageldin, Ahmed Abdel-Rahim, Michael Dixon	8. Performing Organization Report No. N14-12
9. Performing Organization Name and Address TranLIVE NIATT/University of Idaho 875 Perimeter Dr MS 0901 Moscow, ID 83844-0901	10. Work Unit No. (TRAIS)
	11. Contract or Grant No. DTRT12GUTC17
12. Sponsoring Agency Name and Address US Department of Transportation Research and Special Programs Administration 400 7th Street SW Washington, DC 20509-0001	13. Type of Report and Period Covered Final Report: January 1, 2012 to February 28, 2014
	14. Sponsoring Agency Code USDOT/RSPA/DIR-1

15. Supplementary Notes:

16. Abstract

Transportation Systems, and thus Intelligent Transportation Systems (ITS), are considered one of the most critical infrastructures. For wireless communication ITS use communication links based on Dedicated Short Range Communication (DSRC) in Wireless Access in Vehicular Environments (WAVE) systems. Due to the nature of wireless communication, the connected vehicle real-time communication and control infrastructure is exposed to the entire spectrum of threats to security and survivability from cyberspace all the way to direct physical manipulations. For the infrastructure to be trusted one has to consider external manipulations that could render DSRC safety applications useless. This research therefore investigates the impact of malicious act, in particular jamming, on the reliability and survivability of such applications.

17. Key Words Intelligent transportation systems, DSRC, safety critical applications, connected vehicles, WAVE,	18. Distribution Statement Unrestricted; Document is available to the public through the National Technical Information Service; Springfield, VT.

19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages 38	22. Price …

Acknowledgements

This work was sponsored by:

United States Department of Transportation,

University Transportation Centers Program

Table of Contents

List of Figures

List of Tables

Executive Summary

Vehicle-to-Vehicle Communications for Dedicated Short Range Communication (DSRC) Safety Applications is the dynamic wireless exchange of data between nearby vehicles that offers the opportunity for significant safety improvements. By exchanging vehicle-based data such as position, speed, and location, vehicle-to-vehicle (V2V) communications enables a vehicle to use safety applications, e.g., aiding in the assessment of threats and hazards with a 360 degree awareness of the position of other vehicles and the threat or hazard they present; calculate risk; issue driver advisories or warnings.

Although V2V communications uses diverse message types, the most important message for safety applications is the Basic Safety Message (BSM) as defined in the SAE J2735 Message Set Dictionary Standard. Due to the nature of wireless communication, however, BSMs used in V2V communication and control infrastructures are vulnerable to malicious acts ranging from cyber jamming to direct physical manipulation.

This report presents the findings from our investigation into the reliability of DSRC Safety Applications in the presence of malicious act. Several malicious scenarios were considered, including different jamming types, possibly in conjunction with humanly induced actions that cause hazards, e.g., the attacker causing a hazard while jamming a BSM to prevent communication between vehicles affected by the hazard.

Our research demonstrates how message dissimilarity and channel redundancy can be used to overcome the effects of malicious act. While the degree of redundancy is general, i.e., not fixed, specific redundancy levels are demonstrated and analyzed. The dual and triple-redundant schemes presented in this report enable channels with higher power ratings to communicate critical BSM safety application data with a higher-level of resilience to jamming attacks. Based on our research, we describe a new safety application communications architecture that does not deviate from and, therefore, can be efficiently incorporated into existing standards.

1 Problem Statement and Research Objectives

1.1 Problem

Intelligent Transportation Systems (ITS) are utilizing technology to increase traffic safety and environmental benefits. For example, according to the U.S. Department of Transportation (USDOT) ITS reduce traffic hazards, which cause about 43,000 deaths, 3 million injuries and consume over $230 billion dollars each year [1].

Dedicated Short Range Communication (DSRC) is the wireless communication protocol for safety applications in ITS using Vehicular ad hoc Networks (VANET). Due to the criticality of ITS, the reliability of its safety applications is of great concern. Much research has been dedicated to reliable message exchange in VANET, mainly focusing on the physical and Media Access Control (MAC) layers.

In contrast to investigating the low level approaches, the research presented here considers reliability from the safety application point of view when it is adversely affected by malicious act. Thus this research is shedding light on application layer reliability and survivability [2]. Specifically, the wireless communication shared medium can be targeted by intelligent adversaries to attack the applications, e.g., by using jamming to launch Wireless Denial of Service (WDoS) attacks. This could have great implications for a BSM, which is the most important message for safety applications as defined in the SAE J2735 Message Set Dictionary Standard.

Targeted jamming in conjunction with an instigated attack, e.g., by intentionally causing a hazard for vehicles while also launching a jamming attack, has the potential to cause accidents and fatalities. The demonstration of such scenarios by malicious parties has the potential to undermine public trust in the very technologies that are envisioned to increase safety in ITS.

A significant amount of research focused on the reliability of VANET, either focusing on applications with mechanisms using BSMs, or on applications that use new messages to increase the functionality of BSMs. However, there is a lack of research that considers safety applications relying on communication that will be affected by corruption or omission of the BSM.

1.2 Objectives

The objectives of this work are to increase reliability and survivability of DSRC Safety Applications, considering benign faults and malicious attacks. This is to be done without introducing mechanisms deviating for the existing standards. The main focus of the research is on the effects of malicious act. However, any mechanisms that increase the resilience against attacks will also benefit the reliability under normal operation.

2 Approach and Methodology

2.1 Background and Related Work

Many ITS projects have been introduced worldwide, especially in the USA, Europe and Japan. Initially all projects were concerned with communication and service models, e.g., adopting known communication solutions such as 2G and Wireless Local Area Networks (WLAN), which led to the development of many standards like IEEE 802.11p and the IEEE 1609 standards family. Later most projects in real-world vehicular environments were concerned with concepts and solutions optimized for interoperability between standards, performance of communications, and functionality of services [5]. This led to the adoption of 5.9 GHz Dedicated Short Range Communication (DSRC) over existing 900 MHz DSRC as it provides longer range and higher information capacity. To develop a national interoperable standard for 5.9 GHz DSRC, the Federal Highway Administration (FHWA) entered into cooperative agreement with the American Society for Testing and Materials (ASTM), leading to the publication of the ASTM E2213-03 standard [6] as approved standard for DSRC operations.

Channel allocation and the power characteristics are important to the concept of redundant communication for safety applications. The DSRC WAVE system provides communication support to moving and stationary devices. In WAVE systems at least one of the engaged devices is associated with a vehicle, while the other may be any other WAVE device, e.g., another vehicle, roadside, or pedestrian. Thus it relates to Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Infrastructure-to-Vehicle (I2V) communications. WAVE systems support many types of stationary or mobile devices.

For stationary devices the WAVE standards define the Road Side Unit (RSU), which is permanently mounted. For mobile devices they define the On-Board Unit (OBU), which is mounted to a vehicle or any portable moving device [7]. The Federal Communication Commission (FCC) licensed 75 MHz of bandwidth at 5.9 GHz (5.850-5.925 GHz) to DSRC [1][6,7]. It should be noted that Japan allocated 80 MHz (5.770-5.850 GHz) and Europe 50 MHz (5.875-5.925 GHz) with recommendation to add 20 MHz (5.855-5.875).

There are seven 10 MHz channels from (5.855-5.925 GHz), consisting of one Control Channel (CCH), i.e., channel 178 (denoted by CH178), and six Service Channels (SCH) with even numbers, i.e., CH172, 174, 176, 180, 182, and 184. The remaining 5 MHz band (5.850-5.855 GHz) is reserved for future use. The first service channel, CH172, is a low power channel assigned to V2V communication, while the last channel, CH184, is a high power channel assigned to public safety applications, including road intersections [7]. Channels 174 and 176 can be combined to form CH175, and channels 180 and 182 could be combined to form CH181. Both channels, 175 and 181, are 20 MHz channels for higher data rate applications [1]. Table 1 and Table 2 show a summary of information related to channel allocation and power limits.

Table 1: DSRC Channel Allocations

<table>
<tr><td rowspan="2">Channel No</td><td rowspan="2">CH170</td><td rowspan="2">CH172</td><td>CH174</td><td>CH176</td><td rowspan="2">CH178</td><td>CH180</td><td>CH182</td><td rowspan="2">CH184</td></tr>
<tr><td colspan="2">CH175</td><td colspan="2">CH181</td></tr>
<tr><td>Channel Use</td><td>Reserved</td><td>SCH</td><td>SCH</td><td>SCH</td><td>CCH</td><td>SCH</td><td>SCH</td><td>SCH</td></tr>
<tr><td rowspan="2">Bitrate (Mbps)</td><td rowspan="2">na</td><td rowspan="2">3-27</td><td>3-27</td><td>3-27</td><td rowspan="2">3-27</td><td>3-27</td><td>3-27</td><td rowspan="2">3-27</td></tr>
<tr><td colspan="2">6-54</td><td colspan="2">6-54</td></tr>
<tr><td rowspan="2">Bandwidth (MHz)</td><td rowspan="2">5</td><td rowspan="2">10</td><td>10</td><td>10</td><td rowspan="2">10</td><td>10</td><td>10</td><td rowspan="2">10</td></tr>
<tr><td colspan="2">20</td><td colspan="2">20</td></tr>
<tr><td>Frequency Range (GHz)</td><td>5.850 – 5.855</td><td>5.855 – 5.865</td><td>5.865 – 5.875</td><td>5.875 – 5.885</td><td>5.885 – 5.895</td><td>5.895 – 5.905</td><td>5.905 – 5.915</td><td>5.915 – 5.925</td></tr>
</table>

Table 2: DSRC Channel Power Limits

Max allowable Effective Isotropic Radiated Power (EIRP) 44.8 dBm (30 W) EIRP = $P_t - L + G$							
CH	Public / Private	RSU			OBU		MIN GAIN dB$_i$
		Description	Antenna i/p power dB$_m$	EIRP dB$_m$	Antenna i/p power dB$_m$	EIRP dB$_m$	
CH 172	PUBLIC	Small and medium range operations	28.8	33	28.8	33	
	PRIVATE		28.8	33	28.8	33	
CH 174	PUBLIC		28.8	33	28.8	33	
	PRIVATE		28.8	33	28.8	33	
CH 175	PUBLIC		10	23	10	23	
	PRIVATE		10	23	10	23	
CH 176	PUBLIC		28.8	33	28.8	33	
	PRIVATE		28.8	33	28.8	33	
CH 178	PUBLIC		28.8	44.8	28.8	44.8	
	PRIVATE		28.8	33	28.8	33	
CH 180	PUBLIC	Small zone operations	10	23			6
	PRIVATE		10	23	20	23	6
CH 181	PUBLIC		10	23			6
	PRIVATE		10	23	20	23	6
CH 182	PUBLIC		10	23			6
	PRIVATE		10	23	20	23	6
CH 184	PUBLIC		28.8	40	28.8	40	
	PRIVATE		28.8	33	28.8	33	

Because the power levels associated with different channels play an important role in the assessment of survivability of our redundancy approach, the specific requirement in the standards need to be identified. The transmit power levels for public safety and private RSU and OBU operations in DSRC channels were introduced in the ASTM E2213-03 standard [6]. It should be noted that the maximum allowable Effective Isotropic Radiated Power (EIRP) in accordance with FCC regulations is 44.8 dBm (30 Watt) for government, while the maximum allowable EIRP is 33 dBm (2 Watt) for nongovernment [12].

Since we are only interested in the reliability of V2V safety applications, we will only present the maximum allowable power for public safety OBU operations and some RSU operations. Public Safety OBU operations in Channels CH172, CH174, and CH176 shall not exceed 28.8 dBm antenna input power and 33 dBm EIRP. Public Safety OBU operations in CH175 shall not exceed 10 dBm antenna input power and 23 dBm EIRP. Public Safety OBU operations in CH178 shall not exceed 28.8 dBm antenna input power and 44.8 dBm EIRP. Public Safety RSU and OBU operations in CH184 shall not exceed 28.8 dBm antenna input power and 40 dBm EIRP.

The DSRC Channels CH180, CH181 and CH182 are used to implement small zone operations. Public Safety and Private RSU installation in these channels shall not exceed 10 dBm antenna input power and 23 dBm EIRP. OBU operations in CH180, CH181 and CH182 shall not exceed 20 dBm antenna input power and 23 dBm EIRP. RSUs and OBUs shall transmit only the power needed to communicate over the distance required by the application being supported. Also it should be noted that, according to the ASTM E2213-03 standard [6], the receiver minimum input level sensitivity will be less than or equal to -85 dBm for 3 Mbit/s data rate, which is the lowest data rate for DSRC applications, and the sensitivity value varies according to the data rate used. The Packet Error Rate shall be less than 10% at a Physical Layer Service Data Unit length of 1000 bytes for rate-dependent input levels. Figure 1 shows a summary of information related to channels.

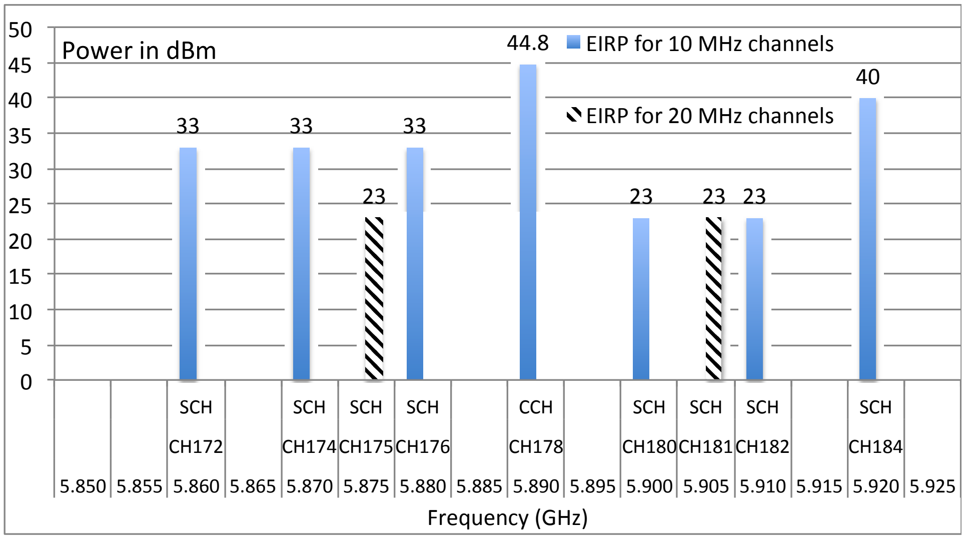


Figure 1: DSRC channel allocation and power limits.

Testing communications related to vehicles was spearheaded by the VSC-A team [4]. It is a collaborative effort in the area of WAVE safety applications initiated in December 2006 by USDOT and the Vehicle Safety Communications 2 Consortium (VSC 2 Consortium), consisting of several vehicle manufactures (Ford, Mercedes-Benz, Toyota, Honda and General motors). The VSC-A project final report was distributed by the USDOT National Highway Traffic Safety Administration (NHTSA), which provides information and results of testing V2V communication using DSRC at 5.9 GHz to improve the system and enable new communications-base safety applications. One of the most important goals in the VSC-A project was to develop and test a BSM for V2V communication that can be used by safety applications to communicate in all directions of the host vehicle. It also proves the limitations of traditional safety systems such as radar.

There has been significant focus on the reliability of VANET. Research either focused on 1) applications with mechanisms utilizing the BSM, or 2) applications that use new messages to increase the functionality of a BSM.

As an example of the first kind, redundancy was utilized in [8], where a non-interactive voting algorithm performed by the vehicle was introduced to detect malicious behavior. The algorithm depends on BSM broadcasts from other vehicles' reaction to an event to infer on the truth in that event. A different redundancy approach was taken in [9], where a data-centric misbehavior detection scheme is introduced. It is not based on voting, but on observation of the movement of vehicles in response to their reaction to the event, such as a crash. However, both previous approaches will be affected by corruption or omission of the BSM they depend on.

As an example of the second kind, a collaborative protocol introducing a new message was used in [10] to deal with communication interruptions by moving obstacles as an effort to forward BSMs. Such a scenario can occur if a large vehicle blocks line-of-sight between two communicating vehicles. The blocking vehicle is made part of the message-forwarding scheme. In [11] a new message was introduced to disseminate data to other vehicles more efficiently. This message is involved in a grouping scheme based on roads. Communication between vehicles involves selected relay nodes with best line-of-sight within each group.

2.2 Wave Standards

Since the focus of this research is the investigation of survivability mechanisms based solely on existing standards it is necessary to present their relevant details. Many standards have been developed to support the 5.9 GHz DSRC short to medium range communication for ITS applications. Several ITS standards that support the WAVE architecture's different layers have already been published. Their most important aspects related to this research are discussed below and illustrated in Figure 2.

2.2.1 ASTM E2213-03 Standard

The ASTM E2213-03 standard [6] describes the specification of the Medium Access Control (MAC) Layer and Physical (PHY) Layer using the DSRC services to be used in wireless communications. It is used in high-speed vehicle environments up to 200 Km/h and over short distances up to 1000 meters with very low latency and is based on the IEEE 802.11 and IEEE802.11a in the 5.9 GHz band. The standard supports a special implementation for the physical layer as introduced by IEEE 802.11a, and it uses the MAC layer of IEEE 802.11. The changes to the physical layer of IEEE 802.11a is that the Orthogonal Frequency Division Multiplexing (OFDM) will provide DSRC with data payload communication capabilities of 3,4,5,6,9,12,18,24 and 27 Mbit/s, and in channel combinations it will be able to support 6,9,12,18,24,36,48 and 54 Mbit/s. Based on the ASTM E2213-03 standard, the IEEE 802.11 working group developed the IEEE 802.11p [12,13], which is an amendment to include the specifications discussed by ASTM E2213-03 standard to support WAVE systems.

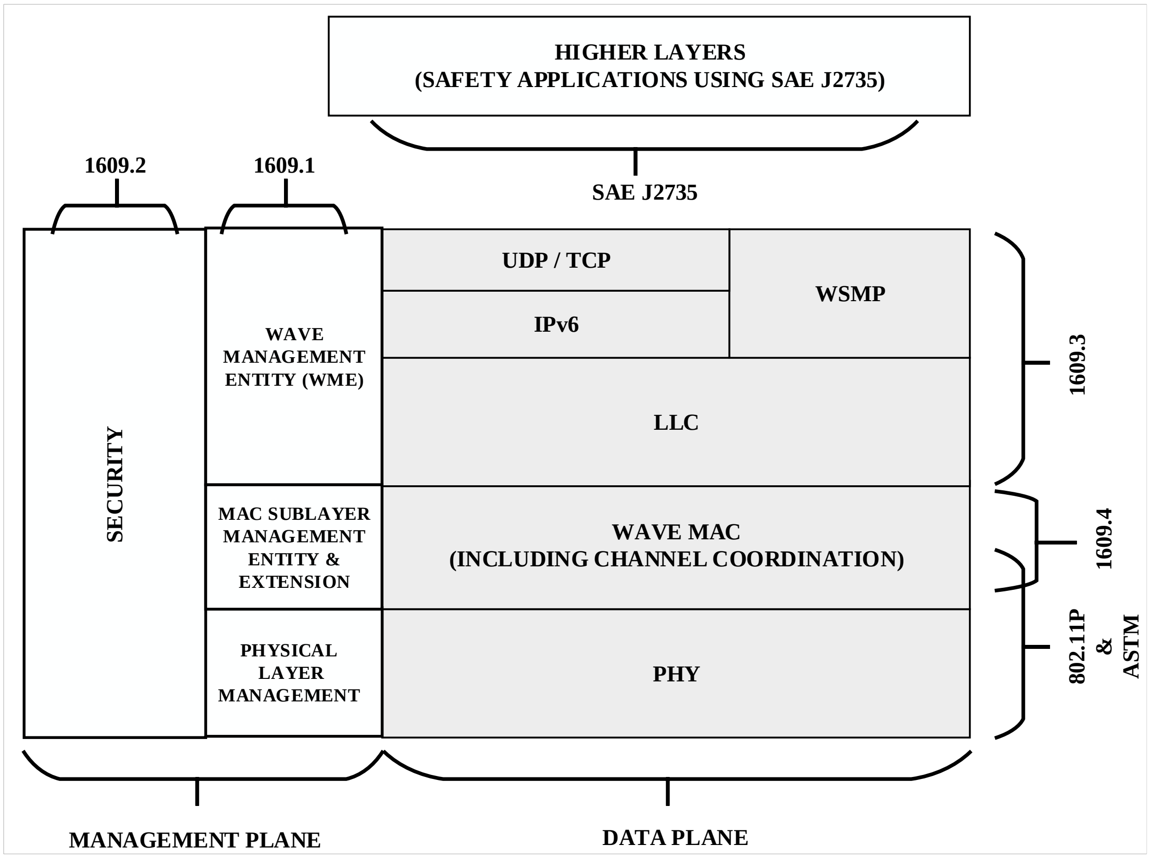

HIGHER LAYERS
(SAFETY APPLICATIONS USING SAE J2735)
SAE J2735
1609.2
1609.1
SECURITY
WAVE MANAGEMENT ENTITY (WME)
MAC SUBLAYER MANAGEMENT ENTITY & EXTENSION
PHYSICAL LAYER MANAGEMENT
UDP / TCP
IPv6
WSMP
LLC
WAVE MAC
(INCLUDING CHANNEL COORDINATION)
PHY
1609.3
1609.4
802.11P & ASTM
MANAGEMENT PLANE
DATA PLANE

Figure 2: DSRC protocol architecture related to WAVE standards.

2.2.2 IEEE 1609 Standard Family

For the upper layers, the IEEE 1609 Work Group published a list of standards for wireless communications in vehicular environments.

The IEEE 1609.0 Standard

IEEE 1609.0 [7] is a draft guide for WAVE, which describes the DSRC/WAVE architecture for the devices in a mobile vehicular environment, and it provides an overview of the system, its components, and operations. Also it is considered a guide to other 1609 standards. IEEE 1609.0 defines the WAVE Service Advertisement (WSA) in which the application provider advertises a service to WAVE devices. The WSA has all the required information like service channel, priority, or repetition rate. When a WAVE device receives this advertisement, it will check whether the advertised application is of interest.

The IEEE 1609.2 Standard

IEEE 1609.2 [1] focuses on WAVE security services for applications and management messages. Due to the critical nature of safety application using WAVE devices and the wireless nature of communication, this standard addresses the need for privacy of application user data. The standard introduces new customized security mechanisms, rather than using the existing Internet security mechanisms. While the existing Internet standards are designed for flexibility and extensibility, we need the new mechanisms to optimize bandwidth and real-time low latency processing. Broadcast applications, which do not use encryption, should not include any personal identifying information, e.g., license plate numbers. Non-broadcast applications however encrypt messages to protect privacy. The standard suggests that there must be a method, which permits all the devices and applications in WAVE to be known and trusted by the Certificate Authority (CA), and all certificates must be only used by authorized entities. All applications must be granted authorization before using the safety channel.

Basic Safety Messages are secured using digital signatures. The standard states that to minimize overhead on a congested channel, the BSM uses implicit certificates with fast verification based on Elliptic Curve Digital Signature Algorithm (ECDSA)-256. Also it is stated that on receiving a BSM, the data validity period is 5 seconds. Due to the short validity time the VSC-A team suggested using a 224-bit key over the 256-bit key, which requires 50 percent less processing. The VSC-A team argued that a 224-bit key is enough to prevent forgery by attackers not having valid certificates [4].

The IEEE 1609.3 Standard

IEEE 1609.3 [14] for WAVE networking services is concerned with connectivity between vehicles to vehicles, vehicles to roadside or between any WAVE devices. The standard focuses on 1) network and transport layer protocols and 2) services supporting multi-channel connectivity between WAVE devices, providing addressing and data delivery services within a WAVE system. It defines service requests from higher-level layers that are accepted by the WAVE Management Entity (WME), which provides access to SCHs causing the transceiver device to be tuned to a specific channel during channel intervals. The service can be requested from a provider, user, CCH Service, management services, or timing advertisement service.

The standard defines two roles for the devices involved. The first is a provider, which advertises its services by transmitting WSA. The second is a user who is interested in the WSA, thus accepting the application messages on the specified SCHs. The standard classifies the types of devices using the allocated WAVE channels to 1) single-physical layer device (not capable of simultaneous operation on multiple radio channels), 2) multi-physical devices (capable of simultaneous operation on multiple radio channels), and 3) switching devices, which have one single-physical layer device capable of switching between channels. IEEE 1609.3 defines two protocol stacks that will be used in the WAVE system. The first is the WAVE Short Message Protocol (WSMP), designed for optimized operations. The second is the Internet Protocol Version 6 (IPv6), which supports transport protocols such as User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). The WAVE Short Messages (WSM) can be used on any channel, while the IP traffic is only used on the service channels.

The IEEE 1609.4 Standard

IEEE 1609.4 [15] for WAVE multi-channel operations is concerned with the specification of multi-channel wireless connectivity supported by the MAC sublayer between WAVE devices. It also describes multi-channel operation channel routing and switching for different scenarios. The standard defines channel coordination where switching devices are concurrently alternating access on the CCH and SCH intervals for data exchange. The channel access includes many options such as 1) continuous access, which requires no coordination because it allows continuous access to one channel, 2) alternating access between SCH and CCH, which requires coordination, 3) immediate SCH access, which allows access to SCH without waiting for the next SCH interval, and 4) extended SCH access, which allows access to SCH without pauses for CCH access. The standard specifies synchronization (for the above access options) based on common time references to perform channel coordination. Devices without local time sources can acquire timing information from other WAVE devices.

2.2.3 The SAE J2735 DSRC Message Set Dictionary Standard

SAE J2735 [16] was introduced for message exchange in ITS applications. This standard specifies the message set, its frames, and data elements for use by applications in 5.9 GHz DSRC to support interoperability between WAVE devices. It uses a dense encoding of messages and the general design goal is to maximize the support for short broadcast style messages. In this paper we will only define five (of a total of fifteen) messages, which will be used in our proposed solutions. The five messages used are listed below and will be defined in detail in Section 4:

- Message (MSG_A_la_Carte)
- Message (MSG_BasicSafetyMessage)
- Message (MSG_ProbeDataManagement)
- Message (MSG_ProbeVehicleData)
- Message (MSG_RoadSideAlert)

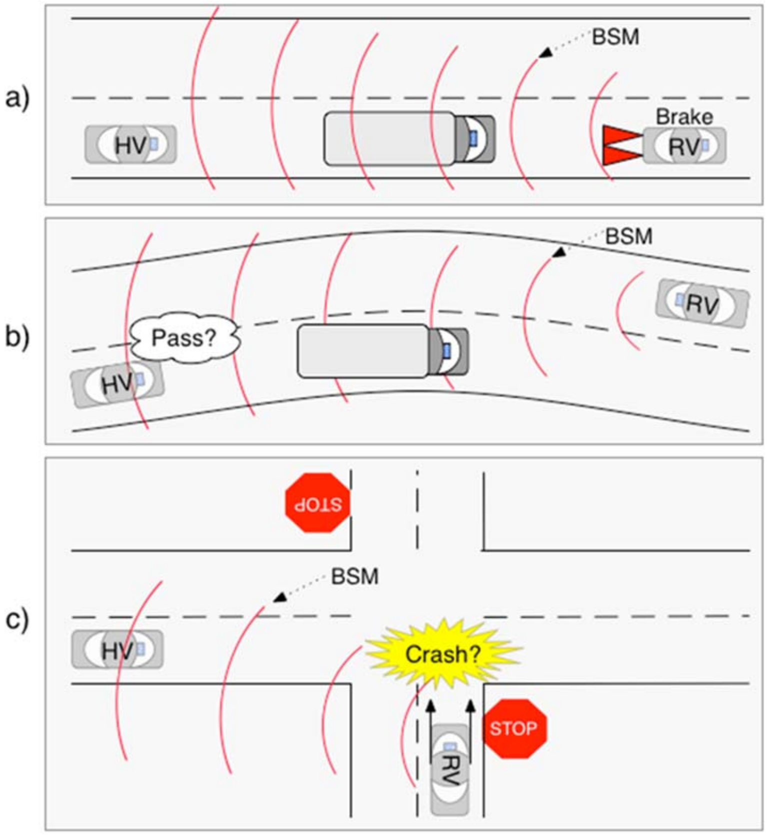
3 Safety Application Scenarios

In order to discuss how one can increase survivability (in Section 6), we selected several scenarios. The scenarios involve a Host Vehicle (HV) and one or more Remote Vehicles (RV). Our interest is the status of the host vehicle as it is affected by the status of the remote vehicles. For this purpose we selected the scenarios from real-world applications, i.e., real-word scenarios listed by the VSC-A project. These scenarios have been tested by the VSC-A project and include the vehicle manufacturers, have been analyzed, and have led to the development of the safety applications [4]. The applications and associated crash scenarios are illustrated in Table 3, based on [4] the safety applications shown in the table rows are: Emergency Electronic Brake Lights (EEBL), Forward Collision Warning (FCW), Blind Spot Warning + Lane Change Warning (BSW+LCW), Do Not Pass Warning (DNPW), Intersection Movement Assist (IMA), and Control Loss Warning (CLW). Three of the scenarios have been selected as examples to illustrate the proposed redundant solutions are depicted in Figure 3.

Table 3: Safety Applications Related to Crash Scenarios

No	Safety Applications \ Crash Scenarios	EEBL	FCW	BSW	LCW	DNPW	IMA	CLW
1	Lead Vehicle Stopped	na	x	na	na	na	na	na
2	Control Loss Without Prior Vehicle Action	na	na	na	na	na	na	x
3	Vehicle(s) Turning at Non-Signalized Junctions	na	na	na	na	na	x	na
4	Straight Crossing Paths at Non-Signalized Junctions	na	na	na	na	na	x	na
5	Lead Vehicle Decelerating	x	x	na	na	na	na	na
6	Vehicle(s) Changing Lanes – Same Direction	na	na	x	x	na	na	na
7	Vehicle(s) Making a Maneuver – Opposite Direction	na	na	na	na	x	na	na

Note: “na” = not applicable



.

Figure 3: Selected crash scenarios.

3.1 Scenario 1: Lead Vehicle Stopped

This scenario, shown in Figure 3a above, uses the Forward Collision Warning (FCW) application, which alerts the driver of the host vehicle of an impending rear-end collision with a remote vehicle traveling ahead in the same direction and on the same lane. For example, when a remote vehicle brakes hard, in the figure this is the first vehicle labeled RV, it broadcasts this event via a BSM to the surrounding vehicles. The vehicles following the remote vehicle will use this information to alert the driver about a possible collision. This may be very useful in situations with low visibility, e.g., heavy fog or vision obstruction by large vehicles. The algorithm in the remote vehicle may transmit this event before the next scheduled transmission time with higher priority than routine BSM broadcasts.

3.2 Scenario 2: Vehicle(s) Making a Maneuver -- Opposite Direction

Here the Do Not Pass Warning (DNPW) Application is used. It alerts a host vehicle attempting a passing maneuver that is not safe. In Figure 3b, the RV traveling in the opposite direction occupies the passing zone of HV.

3.3 Scenario 3: Straight Crossing Paths or Turning at Non-Signalized Junctions

Crossing or turning at non-signalized junctions uses the Intersection Movement Assist (IMA) application, which alerts the host vehicle that it is not safe to proceed due to high collision probability with a remote vehicle in the intersection. The host vehicle communicates with all nearby remote vehicles and receives their broadcasted BSM. After that the in-vehicle unit analyzes all data received from other vehicles and predicts their future paths. If the analysis detects the probability of a collision, a warning is issued to the host vehicle's driver. In Figure 3c such warning is issued if the data in the BSM of the RV suggests to the HV that the RV is not stopping.

4 Redundancy-Based Survivability Architecture

The discussion above has the common thread that the BSM is the main mechanism used by all safety applications. The BSM is the main mechanism to communicate critical data used by all safety applications. This message is limited to one specific channel and thus represents a single point of failure. There are many ways this channel can be affected and possible faults may originate from simple obstacles, jamming, or the channel congestion phenomenon following a channel switch [14,15], to name a few.

To increase the message exchange reliability in the ITS safety applications, we propose an alternative, redundant approach. Specifically, first we propose message dissimilarity using other messages from the SAE J2735 standard [16] capable of providing the application with all required data as a BSM. Second we propose channel redundancy by transmitting the proposed messages on different channels, i.e., other than the BSM's safety channel. The alternate channels used for redundancy have higher power ratings than the safety channel. The use of redundant channels results in large reliability gains for safety applications in the presence of jamming.

4.1 BSM and Message Dissimilarity

BSM is defined in SAE J2735 [19] and is a V2V message. This message is used by a variety of applications in an exchange of safety data regarding the vehicle state. The message is broadcasted by each vehicle to other surrounding vehicles at a rate of 10 times per second, or other rates depending on the application. The broadcast range of a BSM is about 300 meters, which depends on the transmitting power on the used channel.

A BSM consists of two parts. Part I is mandatory and contains the most required fields for safety applications, including position (latitude, longitude, elevation and accuracy), motion (speed, heading, angle and acceleration), brake system status and vehicle size. Part II of the message is optional and is used when required by the application.

As defined by [16] BSMs are transmitted on a pre-agreed channel, i.e., CH172, using the WSM protocol. It is not required for senders to advertise for this service, and also not required from the receiver to confirm or take any action to join this service. To facilitate BSM functional redundancy, we need to identify messages that have the same structure and information to support safety applications. We identified two different suitable messages, i.e., À la Carte Message (ACM) and Probe Vehicle Data (PVD) message, from the fifteen total messages defined in SAE J2735.

4.1.1 Redundancy Using ACM

The first message is the À la Carte Message, which is a V2V message. As its name suggests, it can include any data frames, data elements, or any external content defined in the standard in a field called (ALLInclusive). All message fields can be added as required. For example, we can add the content of the BSM, i.e., (BSMblob) [16], to get an ACM containing equivalent information. The message has all the flexibility of the BSM and can even support more data than BSMs if desired by an application.

4.1.2 Redundancy Using PVD

The second message is Probe Vehicle Data. It is a V2I message, a unicast from the OBUs to an RSU using the WSM protocol on a service channel determined by the RSU. All PVD messages are authenticated and no acknowledgment from the RSU is required. A PVD message contains information about the full position vector, vehicle type, and most importantly, it has a vector of snapshots, which define the vehicle's traveling behavior.

Each snapshot contains

1. a full report of the vehicle position (longitude, latitude, elevation and accuracy),
2. the time in milliseconds,
3. its motion (speed, heading and transmission state),
4. the confidence information about time, position and speed,
5. the VehicleStatus field, which contains all the vehicle's sensor reading including the brake status, and
6. the VehicleSafetyExtension field, which includes path history, events, timing and path prediction. In short, the PVD message contains a superset of the information found in the BSM and is thus suitable for providing BSM data redundancy.

What specific information is to be included in the PVD message and which vehicle's message is relevant is controlled by a message named Probe Data Management Message (PDM)? The PDM can add more privilege to the use of PVD by controlling data collected from the vehicles as follows. PDM is an I2V message broadcast from the RSU to OBUs. The PDM can 1) control the time/distance OBUs join the RSU and begin to send data using the SnapshotTime and SnapshotDistance fields, 2) control the coverage pattern using the direction HeadingSlice field, 3) instruct specific classes of OBUs to collect data using the Sample field, and 4) indicate the frequency OBUs will send data using the TxInterval field.

4.2 Safety Channel and Channel Redundancy

As shown in the previous subsection, in terms of information content the ACM and PVD messages contain all the required fields to support the functionality of a BSM in a safety application. However, to eliminate the aforementioned single point of failure (BSM is limited to CH172) they should be on different channels. In [1] it was stated, "both public safety and non-public safety users should be eligible for licensing on all channels, subject to priority for safety/public safety." This is confirmed also in [7], i.e., any of the control or service channels could be configured for use as a safety channel.

Given the flexibility of channel assignments mentioned above we suggest that the redundant channels should be far away in the frequency spectrum from the BSM safety channel to increase resilience against natural and malicious external interference such as shadowing or jamming. This separation assumption is proven by the VSC-A project. In validation of the DSRC PHY protocol with regards to cross-channel interference (CCI) the VSC-A project exposed in a field test that the interference in a band adjacent to the target band causes more performance degradation than similar interference in a band further from the target band. The VSC-A team concluded that no change is needed in PHY protocol, and that CCI concerns should be addressed in higher layers [4]. This is in agreement with our approach, which resolves this redundancy issue in the application layer.

In order to use different channels in the redundancy scheme it is important to elaborate on the WAVE radio switching device to understand the details of channel accesses by WAVE devices, in order to make intelligent decisions about channel spacing and redundancy. According to [7,15] in-channel switching based on time division multiplexing a single WAVE device is required to exchange information on a SCH while participating on the CCH. Access to channels is based on 100 ms periods, for CCH and SCH intervals. It is divided into 50 ms for each interval. This however imposes significant capacity constraints on V2V safety communication, because the safety channel will be available less than half the time for safety messages. One of the goals of the VSC-A research was to avoid the capacity constraint by defining one dedicated channel for safety messages, i.e., an always-on safety channel, which according to [1] is CH172. Having a full-time access safety channel removes the need for channel switching and doubles the channel access time. However, the implementation of this concept requires that each OBU be equipped with two radios [4].

Therefore we assume using at least two WAVE radio devices per OBU for best performance. Dissimilar redundancy can be achieved by using the first device dedicated to CH172, the always-on safety channel, for exchanging BSMs with full performance. The second device will be a switching radio device that exchanges information on other SCH while participating on CCH.

4.2.1 Dual Redundant Channel Selection

There are two important factors that affect our selection to redundant channel, 1) the channel distance in the frequency spectrum, and 2) the maximum allowed channel transmitting power, shown in Figure 1. As stated in [15] any device listens to control channel, CH178, by default. Furthermore, CH178 is optimally spaced from CH172 in terms of interference isolation. In addition the EIRP of CH178 is higher than that of CH172, i.e., 44.8 dBm and 33 dBm respectively. Therefore CH178 lends itself as an optimal candidate for the redundant channel as any other choice of channels would require additional switches of devices to monitor that channel. One way to manage access of CH178 for redundant messages in this scheme is to use the Wave Short Message Protocol Safety Supplement (WSMP-S) [15]. The WSMP-S header can be used to arbitrate the control channel for safety messages. In our case these are the redundant counterparts to the BSM, which should take precedence over lower priority messages sent over the control channel. For reasons described above, one candidate for a redundant analog to the BSM is the ACM, which is to be sent on the CCH with higher priority to take precedence over other messages. This implements a system with dual redundancy utilizing dissimilarity, i.e., two different messages on two different channels, to increase survivability of safety applications. Should there be a need to increase redundancy levels beyond two, e.g., as the result of conflicting values due to benign or malicious reasons, or out of concern that both mechanisms fail, a third redundancy level is required.

4.2.2 Triple Redundancy Involving the ITS Infrastructure

As shown in Figure 1, the most applicable choice for the third redundant channel is using CH184. The advantages of using CH184 are twofold. First it maximizes the spectrum separation to the other channels used in the redundancy scheme, which provides higher resilience to interference. Second, the EIRP of CH184 is higher than that of CH172, i.e., 40 dBm and 33 dBm respectively.

In the last subsection we introduced dual redundancy using ACM, which is a V2V message redundant to a BSM on a different channel. Both messages used in dual redundancy are V2V involving message exchange between 2 vehicles. To make the system more resilient, diversity will be introduced as a third approach to involve the infrastructure. Involving the ITS infrastructure is not a new concept. For example, the RSU as an active actor has been recommended in the CICAS-V project [17] for signalized intersections in which the RSU alerts approaching vehicles of possible collisions.

The RSU can serve as a third mechanism in the redundancy scheme to communicate safety information. Specifically, the RSU can use the collected PVD messages and respond to the OBU in case of a detected hazard. In reference to the SAE J2735 there will be local systems that can be authorized to collect data directly from the RSU [16]. We recommend this system be used for collision detection, which triggers a Road Side Alert (RSA) message to be broadcasted.

The RSA is an I2V message sent from the RSU to OBUs to alert travelers about nearby hazards. For urgent and critical messages the RSA is sent as periodic broadcasts using the WSM protocol on a high power channel, either CCH or SCH. In case of lower urgency the IP protocol can be used to send this message as a periodic broadcast over a service channel. This message can be embedded and used as a building block for any other DSRC message, e.g., it is used for Emergency Vehicle Alert messages. The RSA has a FullPositionVector field, which describes the location of the hazard and whether it is fixed or moving. The message also contains the heading and priority. We can use the ITIS.ITIScodes fields to send alerts to vehicles if the infrastructure detects a hazard. For the implementation we suggest the use of the high power channel, CH184, as discussed in the beginning of the subsection.

4.3 Implications of Triple Redundancy

To demonstrate this redundancy scheme a triple redundant application of the scenario in Figure 3c, i.e., the Straight Crossing Paths or Turning at Non-signalized Junctions, will be used. The motivation to use this scenario and not FCW is that now the RSU is involved, which is more likely situated in intersections. Consider the Intersection Movement Assist application used in the host vehicle and the scenario shown in Figure 4a.

In the traditional scenario, which only uses BSMs, the host vehicle would receive a BSM from a remote vehicle crossing in its path. If an obstacle blocks the BSM or the channel is jammed by an attacker, the host vehicle will not be aware of a possible impending collision. Using the redundant scheme, the hazards condition will only occur if the BSM and all redundant message mechanisms fail or are compromised. In Figure 4a, the redundant schemes are provided using the ACM and the PVD involving the RSU.

The communication associated with FCW in Figure 3a is depicted in Figure 4b. Assume that CH172 is the target of a jamming attack. This will prevent the host vehicle from receiving a BSM indicating that the remote vehicle is braking hard. Without redundancy HV cannot alert the driver. ACM is utilizing a different channel, i.e., CH178, and assuming that jamming does not reach the frequency spectrum of this channel the safety application will succeed.

The same arguments can be applied to another scenario, in which vehicle(s) make passing maneuvers. The redundancy of the previous case applies and if an RSU is present triple redundancy can be used.

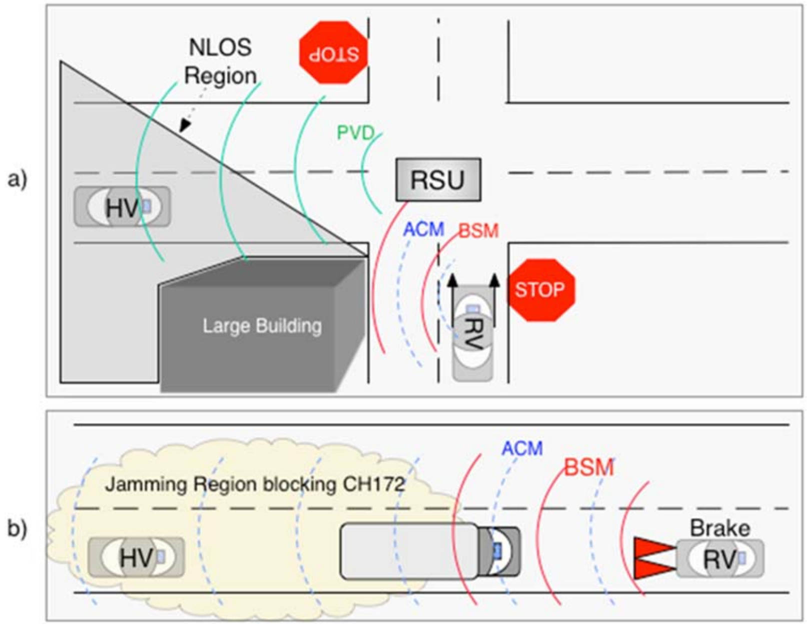


Figure 4: Demonstration of triple redundancy mechanism.

To determine the effectiveness of the redundant schemes one can lean on reliability analysis. If one describes the redundant system as a parallel system, which is defined to fail only if all redundant components fail, then the unreliability of the combined system is the product of the unreliabilites of the individual components [18]. Whereas this product rule only applies when using the assumptions of failures of electronic components, and not for non-exponential failure behavior, it still provides some intuition. A more precise model would need to consider more complicated hazard functions, as described in [19], which however exceed the scope of this paper.

5 Wireless Communication and Jamming

Since DSRC is a wireless protocol, it inherits all problems from the shared wireless media, including malicious act such as Wireless Denial of Service (WDoS). A common attack in wireless communication is jamming, which can be launched, using off-the-shelf equipment, to interfere or block legitimate transmission by emitting radio signals that do not obey the standardized MAC protocol.

A jammer is defined by [20] to be “an entity who is purposefully trying to interfere with the physical transmission and reception of wireless communications.” Jamming cannot be avoided by regular security mechanisms such as authentication, digital certificates, or encryption, because the jammer is often disregarding higher layers, focusing on disrupting the physical communication at the lower layers. Several jamming types have been identified in [20, 21]. Our considerations focus on the following three types:

Constant Jammer: This type of jammer emits a constant radio signal interfering with legitimate communication, violating the underlying MAC protocol. This is considered the worst case of jammer by many researchers as it indiscriminately affects the signal of ongoing communication. However, it is the least energy efficient and is relatively easy to detect and locate.
Random Jammer: Here the attacker jams for t_j and sleeps for t_s seconds. The jam and sleep periods may be unpredictable, e.g., t_j and t_s can be samples of two random variables T_j and T_s, respectively, following different distributions [21]. Random jammers consume less energy than constant jammers, but can be harder to detect.

Intelligent Jammer: This type of jammer is sometimes called a “Protocol Aware Jammer.” It is capable of interpreting and analyzing ongoing transmissions and can thus target specific message types or selected messages. As a result it can be used in sophisticated attack scenarios. It is extremely difficult to detect and very energy efficient.

In this research, we investigate the safety application reliability as constant, random and intelligent jammers affect it. We picked the constant jamming because it can create wide blind spots and induce immense performance degradation [22]. Random jamming was picked, as its impact on reliability is limited, depending on sleeping period. Intelligent jamming was selected because it is highly sophisticated.

6 Quantitative Analysis of Impact of Redundancy

Application reliability is highly dependent on the message exchanges and requirements of the specific application considered. For our research we selected the FCW application, as it is the highest ranked safety application based on crash frequency, cost and functional years lost according to the VSC-A project [4]. The timing issues related to the FCW application host and remote vehicles of Figure 3a are shown in Figure 5.

The position of the jammer in this scenario is assumed to be right next to the RV. A hypothetical situation would be an adversary with a jammer causing the event that leads to braking, e.g., by launching an obstacle into the moving traffic. Starting with the moment of hard braking at time t_{brake} the RV emits a BSM every 100ms. The HV needs to be alerted of the potential collision with the RV early enough to react. The reaction time is the time from the driver receiving an alert to his/her reaction, i.e., the time from t_{react} to t_{brake}. Reaction is only possible if the HV receives at least one BSM from the RV, which is the minimum the application requires detecting the event, before t_{react}. Specifically, as demonstrated using Figure 5, the HV must receive at least one of the first x BSM, i.e., BSM_1 , ..., BSM_X , before it is too late to react at time t_{react}. Thus t_{react} is the deadline for the FCW application to warn the driver of a possible collision, leaving enough reaction time to brake. Any BSM received after that will arrive too late for the driver to react. Typical reaction times are within 0.9s [23].

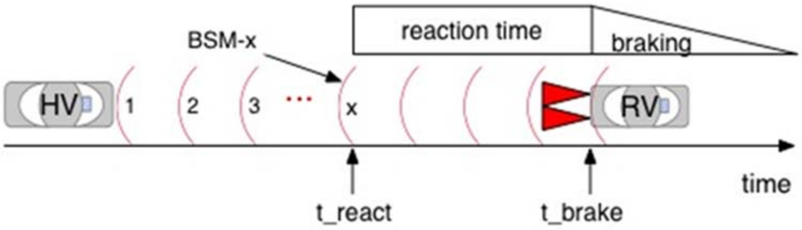


Figure 5: BSM propagation during FCW.

Figure 6 shows FCW scenarios, where the host vehicle's reception of the BSM is affected by jamming, i.e., the jamming signal degrades the signal to noise ratio at the receiver of HV. This degradation however is related to the length of two distance vectors, i.e., the HV-to-jammer distance and the HV-to-RV distance. These distances change as the vehicles are moving and the jammer is by our assumption stationary. A hypothetical situation would be an adversary with a jammer causing the event that leads to braking, e.g., by launching an obstacle into the moving traffic. We assume the distance between the HV and RV is constant, even during braking. This is over-conservative, but it accounts for special cases where brakes could be applied aggressively in conjunction with the gas pedal during brief periods.

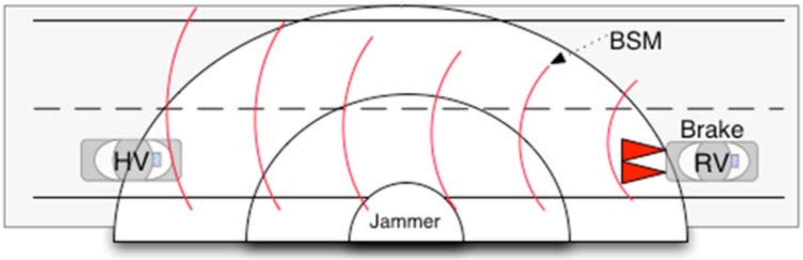


Figure 6: FCW under jamming.

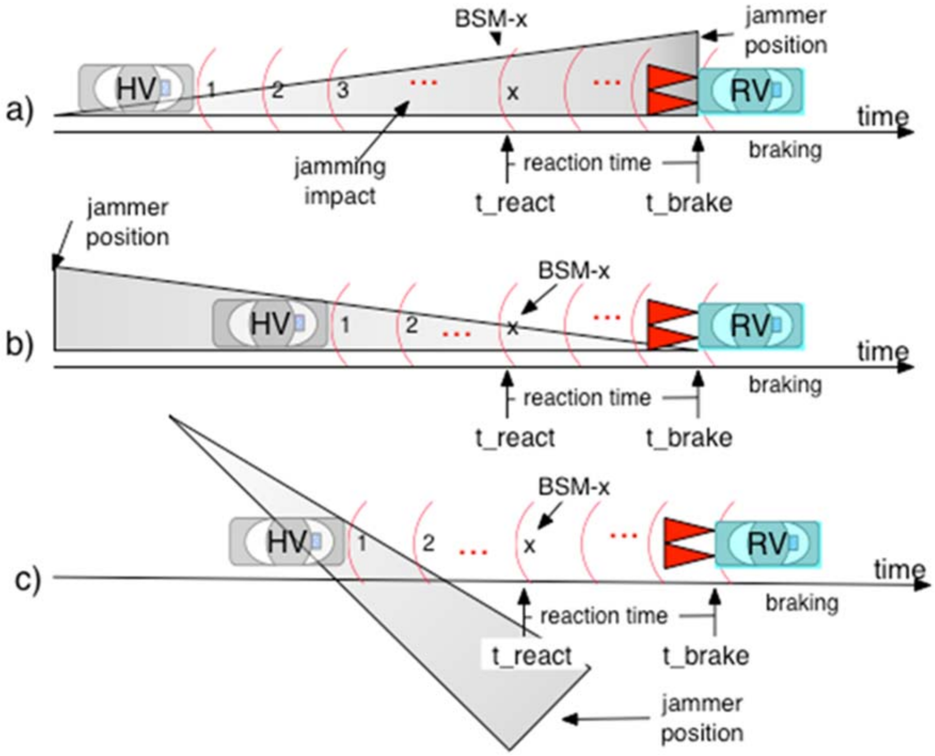


Figure 7: Jammer positions.

Three interesting jamming scenarios are shown in Figure 7. Whereas the figure shows the timeline, it should be clear that these times relate to distances. In Figure 7a the jammer is positioned right next to the RV as it brakes. As the HV approaches the jammer, the jamming effect on the reception increases. In Figure 7b the jammer is positioned behind the HV, and thus as the HV drives, the distance from the jammer gets larger. A larger distance between the HV and the jammer can also be the result of the jammer retreating further away from the road, as seen in Figure 7c. The distances between the HV and RV and where and how far from the HV the jammer is positioned has great impact on the application reliability.

The FCW application reliability is directly linked to the probability of the HV receiving a BSM before it is too late to react. Thus the application reliability depends on the packet error ratio (PER), or packet error probability and their impact on message exchanges. 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], [24], we can define the FCW application reliability as the probability of receiving at least one BSM before t_{react}, i.e., one of BSM_i, for i = 1, .., x. Since the application fails only if no BSM is received before t_{react}, and since the reliability of one BSM is independent of that of another BSM, we use the unreliability Q(t) = 1−R(t), i.e., the probability of all x messages being lost, which is:

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

where Q_i is the probability that BSM i was not received, i.e., the PER of BSM_i, and t_i is the time BSM_i should be received. Note that this time is linearly related to the distance between HV and the jammer when BSM_i should be received.

In order to obtain the application unreliability indicated in Equation 1, we need the values of Q_i. Packet error probabilities are derived from the Signal-to-Jamming Ratio (SJR), which depend on signal powers and distances, as it applies for each BSM_i. We assume that jamming noise dominates any other noise. The SJR is given in [21] by

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

Also we can use the Jamming-to-receiver Signal Ratio (JSR), which is the inverse of SJR

$$JSR = \frac{P_j G_{jr} G_{rj} R^2{}_{tr} L_r B_r}{P_t G_{tr} G_{rt} R^2{}_{jr} L_j B_j} = \frac{P_j G_{jr} R^2{}_{tr} L_r}{P_t G_{tr} R^2{}_{jr} L_j}$$

where subscript j refers to the jammer, r to the receiver and t to the transmitter. The transmission power of node y is denoted by P_y, the antenna gain from node y to z by G_{yz}, the distance between nodes y and z by R_{yz}, the communication link's signal loss by L_r, the jamming signal loss by L_j, and the nodes y bandwidth by B_y. After cancellation of terms that are equal, due to the assumption that the jammer and OBU have equal capabilities, the SJR to the right of the equation remains.

We assume that distance between the HV and RV is constant, even during braking. This is over-conservative, but it accounts for special cases where brakes could be applied aggressively in conjunction with the gas pedal during brief periods. Using the standard definition of EIRP we get

$$SJR_{dB} \;=\; EIRP(t)_{dB} - EIRP(j)_{dB} + 20logR_{jr} - 20logR_{tr} \qquad (3)$$

the impact of the SJR is now used to calculate the PER, or packet error probability. However, we need to consider modulation for different bit rates. As stated in ASTM E2213-03 standard [6], DSRC uses Orthogonal Frequency Division Multiplexing (OFDM) and uses Binary Phase Shift Keying (BPSK) or Quadrature Phase Shift Keying (QPSK) and 16-Quadrature Amplitude Modulation (16-QAM), which support the mandated data rates of 3Mbps, 6Mbps and 12Mbps. These rates will be subject of our investigations, i.e., for 3Mbps using BPSK with coding rate 1/2, for 6Mbps using QPSK with coding rate 1/2, and for 12Mbps 16-QAM with coding rate 1/2, as defined in [6] and shown in Table 5. Assuming Additive white Gaussian noise (AWGN) channel model, the bit error probability P_b(PSK) for BPSK and QPSK can be expressed using the complementary error function *erfc*() as

$$P_b(PSK) = \frac{1}{2} erfc\left(\sqrt{\frac{E_b}{N}}\right) \qquad (4)$$

where E_b / N is the ratio of average energy per bit to noise power spectral density. For 16-QAM we have the following bit error rate with k = $\log_2$ 16 = 4

$$P_b(QAM) = \frac{3}{2k} erfc\left(\sqrt{\frac{kE_b}{10N}}\right) \qquad (5)$$

this is related to the SJR by

$$\frac{E_b}{N} = SJR\frac{B}{R} \qquad (6)$$

where *R* is the channel information data rate and *B* is the channel occupied bandwidth, as shown in Table 4.

The packet error probability P_p is now approximated by

$$P_p = 1 - \; (1 - \; P_b)^N \qquad (7)$$

where *N* is the number of bits of the BSM. Whereas this equation assumes independence of faults. It can still serve as an approximation, since jamming is considered constant over the jamming time and is reflected in the Bit Error Rate (BER). For details about the impact of bit-to-bit dependence on packet error rate the reader is referred to the literature, e.g., [25].

7 Results

7.1 Impact of Jamming without Putting Channel Power Limit in Consideration

The JSR for two constant jammers is plotted in Figure 8, for the scenario of Figure 7a. The assumptions for the graph are as follows: P_t was set to 20dBm, P_j to 10dBm and 15dBm, R_{tr} is set to the safety distance between vehicles of 3s, or 45.9m, corresponding to a vehicle speed of 35mph, with an assumed reaction time of 1s. R_{jr} is the varying distance from the jammer as the HV moves. All other parameters, *G*, *L* and *B*, are assumed equal for both, thus canceling each other out. The impact of thermal noise compared to the large jamming power is assumed negligible. If we assume a total safety distance of 3s and subtract 1s of reaction time, this only leaves the first 2 seconds to receive a BSM before it is too late to react. Since the interval between two BSMs is 0.1s, a maximum of 20 BSMs could possibly be received, and thus the last message that may be received in Figure 7a is BSM$_{20}$.

As can be seen in the graph, the impact of the jammer increases with the message index, with BSM$_1$ least affected by jamming.

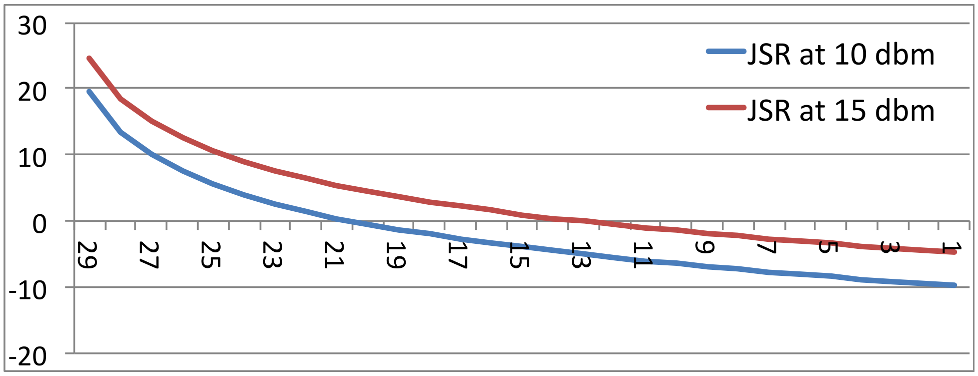


Figure 8: Jamming-to-signal ratio in dB related to messages BSMi.

7.1.1 Impact of Constant Jammer on Q(t)

The impact of the JSR is now used to calculate the PER. The BSMs are sent on the 6Mbps CH172 using QPSK 1/2 encoding [6,7]. The bit error probability P_b for QPSK can be expressed using Equation 4. We assume a BSM length of 300 Bytes, giving $N = 2400$ bits. The packet error rate P_p is the unreliability Q_i used in Equation 1. Its impact on the FCW application's unreliability $Q(t)$ in the case of a constant jammer is shown in Figure 9. The x-axis label i indicates the total number of BSMs that were sent by t_i and may be received before t_{react}, whereas the y-axis is the corresponding unreliability $Q(t) = \prod_{i=1}^{x} Q_i(t_i)$ for $x = i$.

For the 15dBm jammer the application unreliability is close to 1 (total failure) during most of the plot. However, in the 10dBm case the unreliability decreases drastically. The final unreliabilities, with 20 BSMs sent, for the 15dBm jammer scenario was 0.993, which is unacceptable. For the 10dBm jammer case however the jammer has insignificant impact, i.e., the probability of missing all 20 BSMs due to jamming was 10^{-18}.

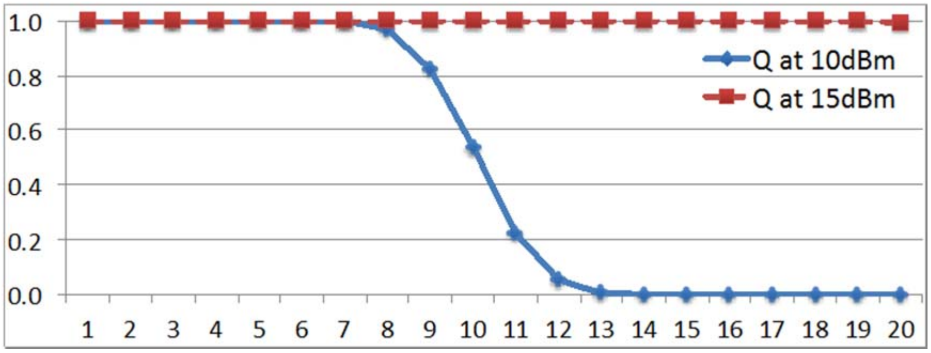


Figure 9: *Q*(*t*) under constant jamming over number of BSMs sent.

7.1.2 Impact of Random Jammer on Q(t)

Figure 9 was for the worst case-jamming scenario, i.e., a constant jammer. The reliability in the presence of a random jammer is highly affected by the probability that a BSM is sent during a sleep period. To simplify matters, let P_s be the probability that an entire BSM falls into a sleeping period.

If a BSM is sent during any sleep time before the reaction time t_{react}, the application reliability is at least as high as the probability of receiving that unjammed BSM. Thus, the application unreliability as it is affected by random jamming is

$$Q_{rand}(t) = \prod_{i=1}^{x} (1 - P_s) Q_i(t_i) \tag{8}$$

where $Q_i(t_i)$ is the unreliability of a BSM reception at t_i during jamming. Equation 8 shows that the unreliability is dominated by the probability that at least one BSM falls in the sleeping period. The impact of sleeping probability P_s on unreliability is shown in Figure 10. For the 15dBm jamming scenario the unreliability, which was unacceptable in Figure 9, falls off very fast with increasing sleeping probability P_s. In fact, increasing jamming power has little impact on the graph, i.e., it is P_s that impacts $Q(t)$. It is obvious that $Q(t)$ in the 10dBm case is already insignificantly small, even with $P_s = 0$. This special case of random jamming, i.e., where sleeping probability is zero, is equivalent to constant jamming. Recall that the unreliability for constant jamming in Figure 9 was 10^{-18} for the 20 messages.

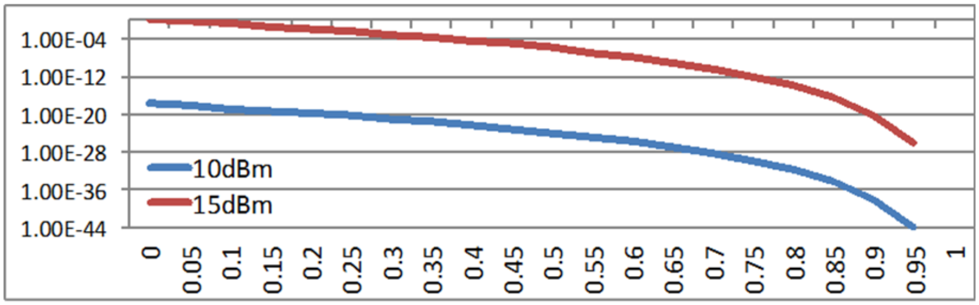


Figure 10: Impact of sleeping probability (x-axis) on *Q*(*t*) (y-axis).

7.1.3 Impact of Redundancy on *Q*(*t*)

Considering only benign faults, a system consisting of N redundant subsystems Cj , j = 1,..,*N* , fails only if all *N* subsystems fail, i.e., it functions as long as at least one subsystem functions up to specifications [24]. The unreliability of such system is therefore the product of the unreliabilities of the subsystems. In our case the application unreliability Q_{Cj} of each channel $C_j(t)$ is defined by Equation 1 and thus

$$Q_N(t) = \prod_{j=1}^{N} Q_{C_j}(t) = \prod_{j=1}^{N} \prod_{i=1}^{x} Q_i(t_i) \tag{9}$$

this equation assumes independence of faults. However, its usage is argued as a good approximation due to the fact that jamming of different channels is assumed to be by different radios and the transmission of dissimilar messages is not time-synchronized, e.g., they are not coordinated to overlap.

A dual-redundant system can be defined by adding redundancy using ACM, as described before. The redundant channels are CH172 and CH178 with individual unreliabilities denoted by $Q_{172}(t)$ and $Q_{178}(t)$ respectively. This leads to an application unreliability $Q_{dual}(t) = Q_{172}(t)Q_{178}(t)$, which can be simplified in this section without considering different channel power limits to $Q_{dual}(t) = Q(t)^2$ if we assume that both channels have the same reliabilities. If we extend the redundancy level by one, e.g., by including redundancy using PVD, we have a triple-redundant system, which for equal reliabilities results in $Q_{triple}(t) = Q(t)^3$. The unreliability of a system with redundant channels is unaffected by jamming as long as one channel is unjammed, i.e., jamming has no effect unless it covers all channels. In the case of an intelligent jammer, who is capable of targeting specific message types, e.g., the BSM, this implies that one of the dissimilar message types needs to remain unaffected, as is the case when he is targeting a specific message type.

Now assume that all channels are jammed. Figure 11 shows the impact of redundancy on unreliability of such scenario as a function of the number of BSMs sent before t_{react}, which in our case is 20. It can be seen that as the redundancy level goes up, the unreliability during lower power jamming goes down. However, as expected, redundancy in the presence of all channels jammed at full power has limited benefit. The real benefit is when the power of the jammer is spread over all redundant channels, and that impact will be significant.

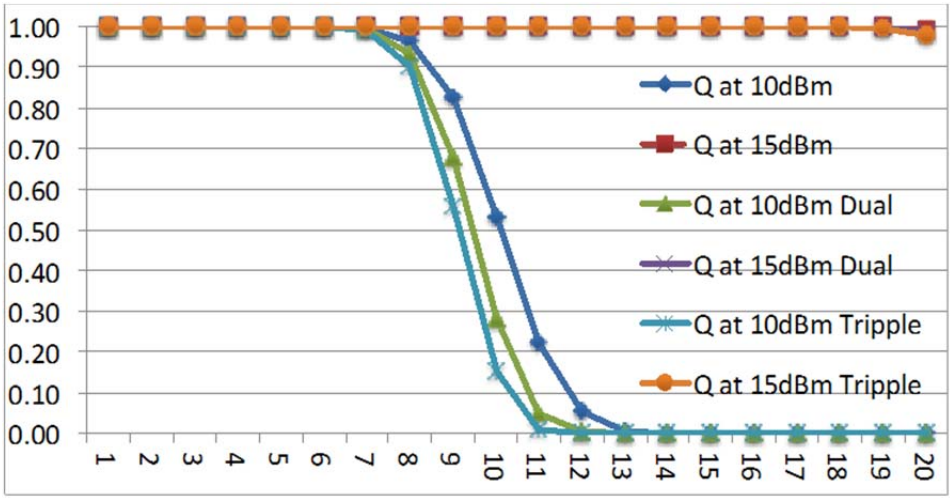


Figure 11: Impact of redundancy on *Q*(*t*) (y-axis) for BSM (x-axis).

7.2 Impact of Jamming Considering Different Power Limits

7.2.1 Considering the Constant Jammer

The impact of constant jamming on the PER of the safety channel, CH172, the first redundant channel, i.e., control channel, CH178, and the second redundant channel, CH184, for 3Mbps communication is shown in Figure 12. As can be seen in the graph, the impact of the jammer increases with the message index, with BSM_1 least affected by jamming.

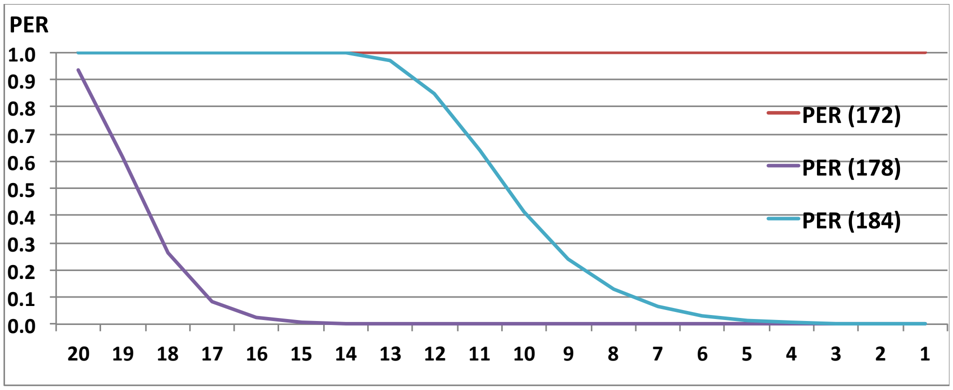


Figure 12: PER for BSM_i during jamming for different channels using 3Mbps.

The assumptions for the graph are as follows: the EIRP of the transmitter and jammer are 33dBm, R_{tr} is set to the safety distance between vehicles of 3s, or 46.9m, corresponding to a vehicle speed of 35mph, with an assumed reaction time of 1s. R_{jr} is the varying distance from the jammer as the HV moves. The impact of thermal noise compared to the large jamming power is assumed negligible. We assume a BSM length of 300 Bytes, giving $N = 2400$ bits. If we assume a total safety distance of 3s and subtract 1s of reaction time, this only leaves the first 2 seconds to receive a BSM before it is too late to react. Since the interval between two BSMs is 0.1s, i.e., BSMs are broadcast every 100ms [16], a maximum of 20 BSMs could possibly be received, and thus the last message that may be received in Figure 5 is BSM_{20}. A summary of the parameter used in the derivation of the application reliabilities is shown in Table 4 and Table 5. This data was extracted from ASTM E2213-03 standard [6].

As can be seen in Figure 12, CH172 is completely jammed, i.e., PER = 1, and thus any safety application only relying on this channel will fail. For CH184, the PER only starts deteriorating starting with message 6, implying that the lower numbered messages are unlikely to be corrupted. CH178 however is mostly resilient to jamming as corruption begins with message 16, i.e., all lower numbered message have very high probability of being delivered uncorrupted. The impact of constant jamming on the PER of the safety channels using 3Mbps and 6Mbps rates is shown in Figure 13.

It can be seen in the graph that the impact of the jammer increases with the message index, with BSM_1 least affected by jamming. However, the exponential deterioration affects channels differently. CH172 is (for all practical purposes) completely jammed for 3Mbps, with even worse results for 6Mbps and 12Mbps (not shown in the figure). CH184 for 3Mpbs has very low PER (less than 10−3) for the first 4 messages, and only starts showing practical impact with message 5. For 6Mbps however, even the best PER achieved for message 1 is already slightly over 0.3, which is violating the acceptable rate of the standard [6]. The most reliable channel is CH178, which only starts seeing deterioration for 3Mbps and 6Mbps starting with messages 15 and 9 respectively. All channels with 12Mbps experienced unacceptable PER for all messages, and they were not depicted in the figure.

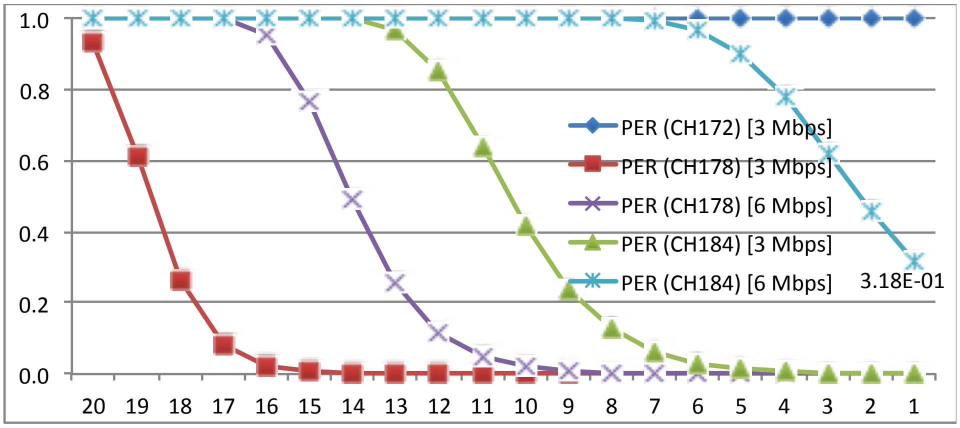


Figure 13: PER of safety message *i* (x-axis) using 3Mbps and 6Mbps for different channels affected by constant jamming.

By using Redundant approach, the unreliability of a system with redundant channels is unaffected by jamming as long as one channel is unjammed, i.e., jamming has no effect unless it covers all channels.

The unreliability of the FCW safety application, defined in Equation 1 and Equation 9, for 3Mbps communication, is shown in Figure 14. Note that the product of the equation is dominated by the product terms with smallest unreliability. Only using safety channel, CH172, the FCW application fails totally, as no error-free packets were received. On the other hand, the first redundant channel, i.e., control channel, CH178, is extremely robust. This can be observed when one considers the time window in which safety messages could be potentially received, which is given in the x-axis of Figure 14. When the safety distance between the HV and the RV in Figure 5 allows a message window greater than three messages, the FCW receives messages with very high probability. This point is reached for CH184 when the message window grows beyond thirteen. Since CH178 is used in the dual and triple redundant schemes, its unreliability dominates that of the schemes, resulting in FCW to work reliably.

Table 4: Configuration Parameters

Parameter	Value	Parameter	Value
Number of Subcarriers, Total (N_{ST})	52 (48 Data Subcarrier + 4 Pilot Subcarrier)	Information Data Rate	3, 4.5, 6, 9, 12, 18, 24, and 27 Mbit/s (3, 6, and 12 Mbit/s are Mandatory)
Subcarrier Frequency Spacing (ΔF)	156.25 KHz (10 MHz / 64 total OFDM subcarriers)	Modulation	BPSK OFDM, QPSK OFDM, 16-QAM OFDM, 64-QAM OFDM
T_{FFT}	6.4 µs (1/ΔF)	Coding Rate	1/2, 2/3, 3/4
Guard Interval (T_{GI})	1.6 µs (T_{FFT} /4)	Channel Bandwidth	10 MHz (Occupied Bandwidth 8.3 MHz)
OFDM Symbol Duration	8 µs (T_{GI} + T_{FFT})	CH172 Transmit Power Level	33 dBm EIRP, 28.8 dBm i/p power
PLCP preamble duration (T_{PR})	32 µs	CH178 Transmit Power Level	44.8 dBm EIRP, 28.8 dBm i/p power
Duration of the SIGNAL BPSK-OFDM symbol (T_{SIG})	8 µs (T_{GI} + T_{FFT})	CH184 Transmit Power Level	40 dBm EIRP, 28.8 dBm i/p power
Packet Size	300 bytes (2400 bits)	Jammer Transmit Power Level	33 dBm EIRP, 28.8 dBm i/p power

Table 5: Data Rate and Modulation Parameters.

Information Data Rate (Mbits/s)	Modulation	Coding Rate	Coded bits per Subcarrier N_{BPSC}	Coded bits per OFDM symbol N_{CBPS}	Data□bits per OFDM symbol N_{DBPS}
3	BPSK	1/2	1	48	24
6	QPSK	1/2	2	96	48
12	16-QAM	1/2	4	192	96

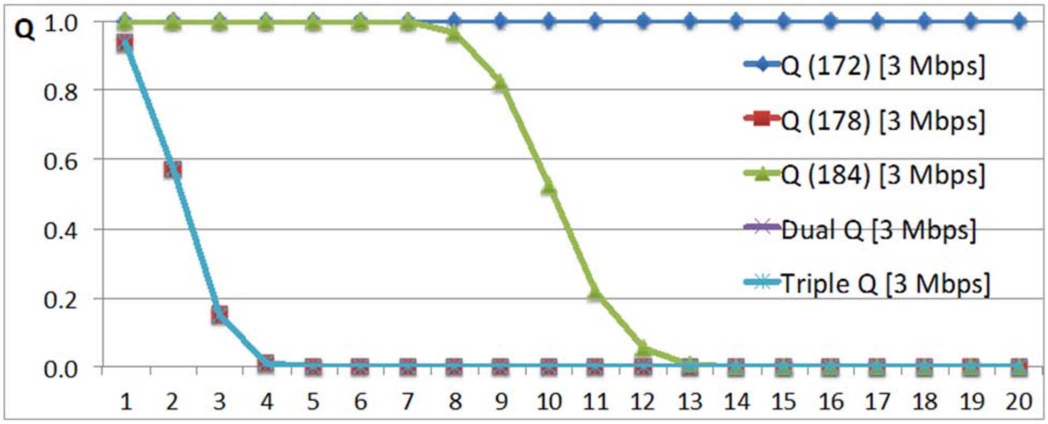


Figure 14: Unreliability *Q*(*t*) of different 3Mbps jammed configurations.

In Figure 15, which considers 6Mbps communication, similar behavior can be observed. However, only CH178, and the redundancy schemes using it, allows FCW to work reliably. In the figure, the plot for the unreliability of CH178 dual and triple-redundancy overlap. CH184 is borderline, as only one BSM provides reasonable unreliability of 0.06, i.e., the BSM at x-axis label 20. Therefore, in general, we suggest to not use this channel for 6Mbps or higher.

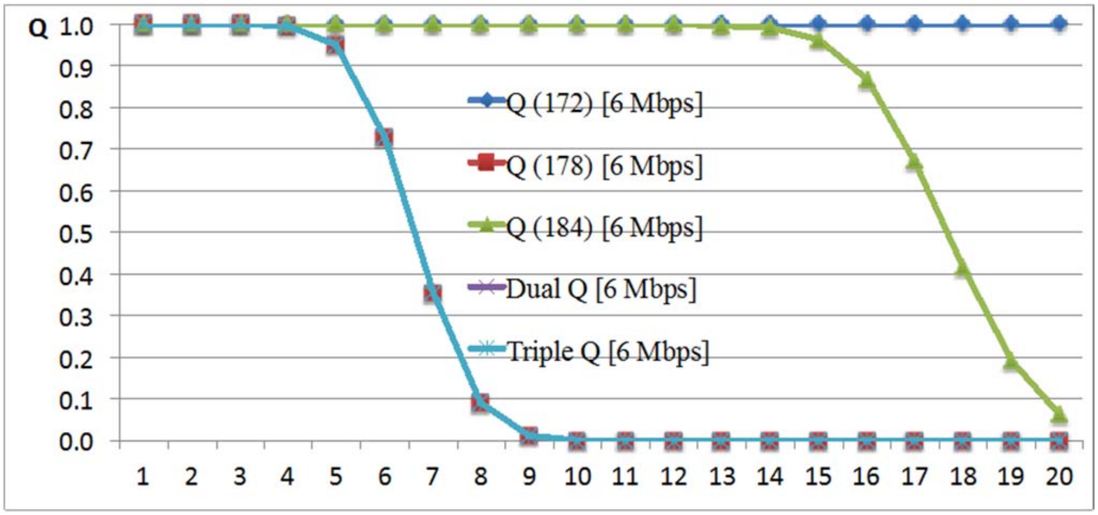


Figure 15: Unreliability *Q*(*t*) of different 6Mbps jammed configurations.

The dual-redundant schemes for different data rates are compared in Figure 16. For the FCW application the 3Mbps and 6Mbps communication is not affected by jamming, i.e., given the assumed minimal safety distance between the vehicles the unreliability of jamming of both falls below 10^{-43}. The 12Mbps communication however fails as unreliability remains close to one. This is a very important observation, which makes us conclude that safety applications should not use this data rate, as communication fails under jamming, i.e., in the figure the application unreliability stays close to one during the entire time before it is too late to react.

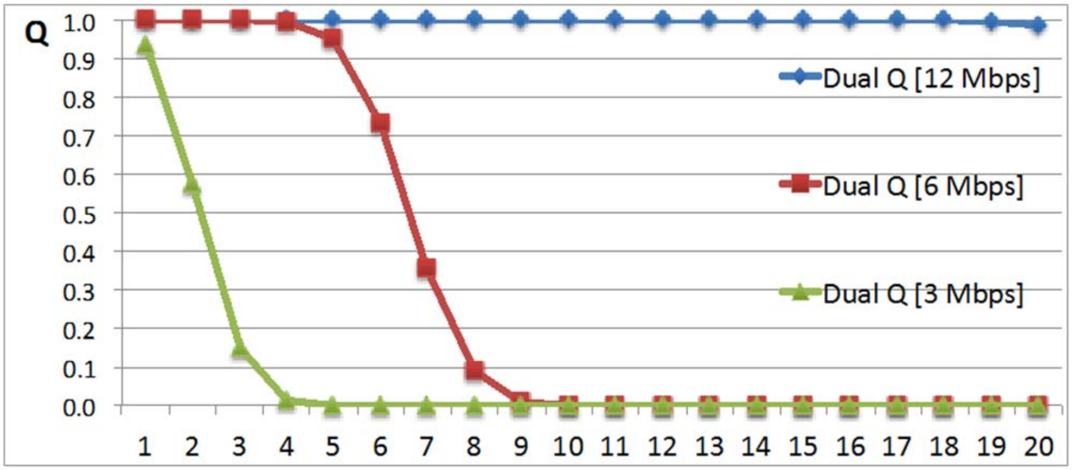


Figure 16: Impact of data rate of dual configuration on unreliability Q during jamming.

The FCW unreliabilities were derived for triple redundant configurations, as shown in Figure 17. The unreliabilities shown reflect the number of messages, i.e., terms, used in Equation 1. Thus, the best unreliabilities are achieved when all 20 messages are used, where the dominating messages are the first ones received, i.e., the message with lowest PER in Figure 13, which is message 1. Most importantly, for 12Mbps even the triple redundant implementation results in unacceptable unreliability close to one. When using lower data rates, i.e., 3Mbps and 6Mbps, all triple configurations can, for all practical purposes, completely overcome jamming.

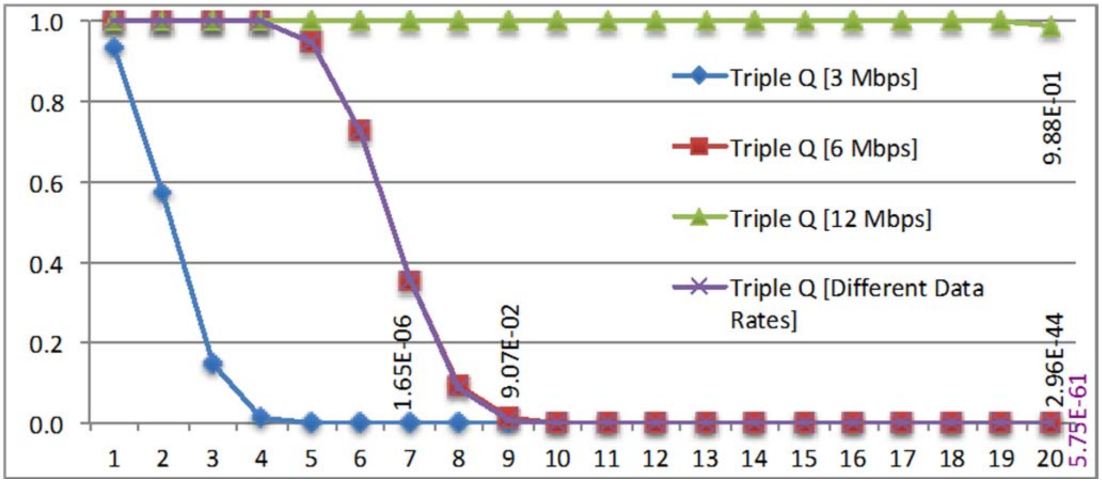


Figure 17: Unreliability *Q*(*t*) of different triple redundant configurations, constant jammer, over total number of BSMs sent.

Figure 17 also shows the unreliability of a triple redundant configuration using different data rates, which overlap with the 6Mbps plot. Here CH172 and CH184 use 3Mbps, but CH178 uses 6Mbps. The rational for using a higher rate for control channel, CH178, is that this channel is used by all applications and thus bandwidth is precious. CH178, even with the higher rate, is providing the dominating terms for Equation 1 and Equation 9, which result in extremely low unreliabilities.

7.2.2 Considering the Random Jammer

The unreliabilities of random jamming for different sleep ratios are shown in Figure 18 for CH172 using 3Mbps, and for different triple redundant scenarios in Figures 19 and 20. The most important observation is that the unreliabilities now are dominated by the sleep ratios. All scenarios, no matter whether the data rates are 3, 6, or 12Mbps, are unaffected by jamming unless the sleeping times are small, e.g., less than 25% in Figures 18 and 19. The justification for this is that as the sleeping times increase the probability for messages to not experiencing jamming is high. Thus even the 12Mbps scenario, which was not usable in the constant jammer case, is immune to random jamming, if the sleep ratio is above 25%.

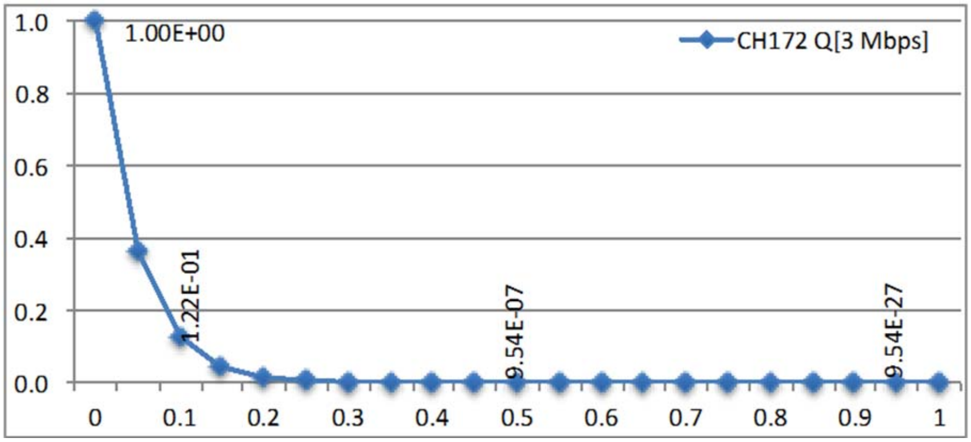


Figure 18: Unreliability *Q*(*t*) of CHI72 using 3 Mbps under random jamming over sleeping ratio.

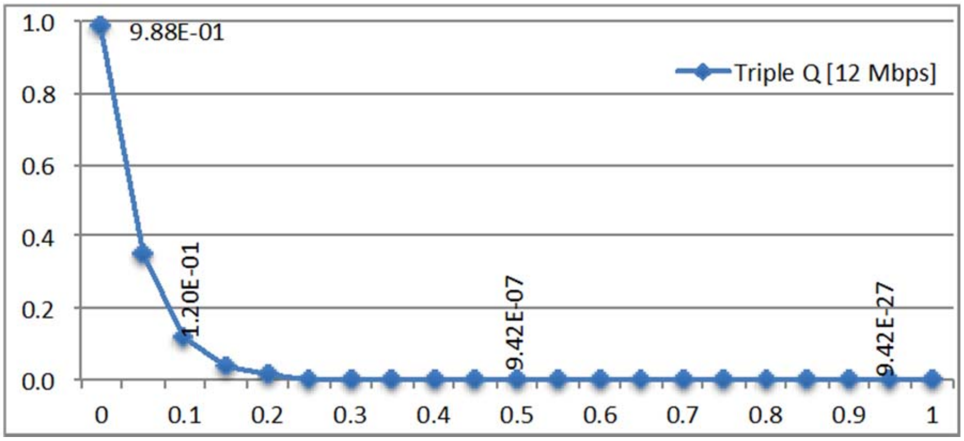


Figure 19: Unreliability *Q*(*t*) of 12Mbps configuration under random jamming over sleeping ratio.

Extreme resilience against random jamming can be observed in Figure 20 for triple redundant configurations using 3 and 6Mbps. One should note that the unreliabilities are insignificantly low, as even the constant jammer, which is a special case of random jammer with sleeping time zero, could cope in this configuration. All results for random jammers do not even consider the time the jammer would need to switch channels, e.g., to switch between CH178 and CH184, which is bound by 2ms [6]. In spite of message delays of approximately 6.3ms, 3.5ms and 2.3ms for 3Mbps, 6Mbps and 12Mbps rates respectively, considering maximum message length, such channel switching would effectively count as non-jamming time.

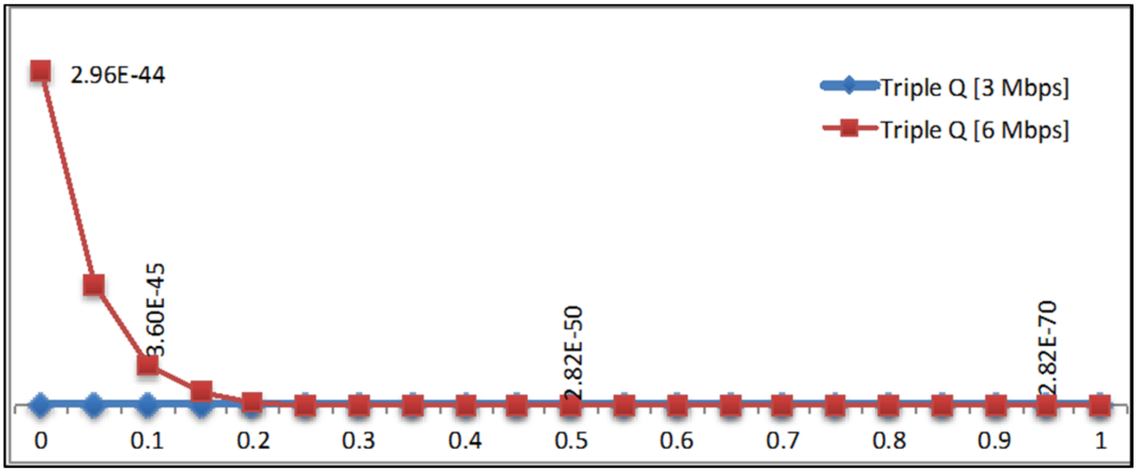


Figure 20: Unreliability *Q*(*t*) of 3 and 6Mbps configuration under random jamming over sleeping ratio.

8 Findings, Conclusions, and Recommendations

A new approach to increase survivability of safety applications using DSRC has been presented. It is based on the concept of Design for Survivability, i.e., the survivability mechanisms are built into the infrastructure and application, rather than as an add-on.

The key concepts, observations, and recommendations are as follows:

1. The concept of dissimilarity of communication mechanisms has been used to increase resilience against interference as the result of natural phenomena and malicious act.
2. The dual or triple redundant mechanisms do not introduce concepts that deviate from existing standards. Thus, no changes to existing standards are necessary to implement the concepts.
3. Reliability of communication in the presence of jamming was greatly affected by the jamming power, the distances between jammer and host vehicle, and the data rate/encoding of the communication.
4. The redundancy schemes introduced overcome the impact of jamming assuming that the jammer capabilities do not exceed the technical specifications similar to that of the vehicles OBU transmission power model.
5. For higher-powered jamming detection, and consequent fail-safe behavior must be assumed, as beyond certain levels of jamming mediation is infeasible.
6. The dual-redundant scheme using channels CH172 and CH178 can provide sufficient FCW application reliability in the presence of jamming. This is the case for either using 3Mbps or 6Mbps communication.
7. In triple redundant approaches we suggest using CH184 for data rates no higher than 3Mbps for DSRC safety applications.
8. Furthermore, given the results for the unreliability of 12Mbps communication, we conclude that the use of this data rate is also not advisable for DSRC safety applications that may be exposed to jamming attacks.
9. The findings of the research are also described in [26][27] and [28].

9 References

1. Federal Communications Commission FCC 03-324–2004, Amendment of the Commission’s Rules Regarding Dedicated Short-Range Communication Services in the 5.850-5.925 GHz Band (5.9 GHz Band).
2. Krings, A., Survivable Systems, in Information Assurance: Dependability and Security in Networked Systems, Morgan Kaufmann Publishers, 2008.
3. Balogun, V. and A. Krings. On The Impact of Jamming Attacks on Cooperative Spectrum Sensing in Cognitive Radio Networks, in Proc. 8th Annual Cyber Security and Information Intelligence Research Workshop, January 8 - 10, 2013.
4. Vehicle Safety Communications-Applications (VSC-A) Final Report. DOT HS 811 492 A. U.S. Department of Transportation, NHTSA. September 2011.
5. Makaya, C., and S. Pierre. Emerging Wireless Networks: Concepts, Techniques, and Applications. CRC Press, Taylor & Francis Group, New York, 2011.
6. ASTM E2213-03(2010) 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.
7. IEEE P1609.0™/D5, September 2012, IEEE Draft Guide for Wireless Access in Vehicular Environments (WAVE) –Architecture.
8. Crescenzo, G., L. Yibei, S. Pietrowicz and T. Zhang. Non-interactive malicious behavior detection in vehicular networks, Proceedings of the IEEE International Conference on Vehicular Networking Conference (VNC), pp. 278–285, 13-15 Dec. 2010, Jersey City, NJ, USA.
9. Harit, S.K., G. Singh, and N. Tyagi. Fox-Hole Model for Data-centric Misbehavior Detection in VANETs, Third International Conference on Computer and Communication Technology (ICCCT), pp. 271-277, 23-25 Nov., Allahabad, India 2012.
10. Abumansoor O., and A. Boukerche. A secure cooperative approach for nonline-of-sight location verification in VANET, IEEE Trans. Vehicular Technology, vol. 61, no. 1, pp. 275–285, Jan. 2012.
11. Tung L. C., and M. Gerla. An efficient road-based directional broadcast protocol for urban VANETs, Proceedings of the IEEE International Conference on Vehicular Networking Conference (VNC), pp. 9–16, 13-15 Dec. 2010, Jersey City, NJ, USA.
12. IEEE Std 802.11p - 2010 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.
13. IEEE Std 1609.2™-2013, IEEE Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages.
14. IEEE Std 1609.3™-2010, IEEE Standard for Wireless Access in Vehicular Environments (WAVE) –Networking Services.
15. IEEE Std 1609.4™-2010, IEEE Standard for Wireless Access in Vehicular Environments (WAVE) –Multi-Channel Operation.

16. SAE J2735 Dedicated Short Range Communications (DSRC) Message Set Dictionary. Society of Automotive Engineers, DSRC Committee. November 2009.
17. Maile M., and L. Delgrossi. Cooperative Intersection Collision Avoidance System for Violations (CICAS-V) for Avoidance of Violation-Based Intersection Crashes, Paper Number 09-0118. Enhanced Safety of Vehicles, 2009.
18. Sahner R., S. Trivedi and A. Puliafito. Performance and Reliability Analysis of Computer Systems: An Example-Based Approach Using the SHARPE Software Package, Kluwer Academic Publishers, 1996.
19. S. Zhanshan and A. Krings. Multivariate Survival Analysis (I): Shared Frailty Approaches to Reliability and Dependence Modeling, Proc. IEEE Aerospace Conference, March 1-8, Big Sky, MT, 2008.
20. Xu, W., Trappe, W., Zhang, Y., Wood, T. *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, pp. 46-57. ACM, 2005.
21. Pelechrinis, K.; Iliofotou, M.; Krishnamurthy, S.V., *Denial of Service Attacks in Wireless Networks: The Case of Jammers*, Communications Surveys & Tutorials, IEEE, vol.13, no.2, pp.245,257, 2nd Quarter 2011.
22. Punal, O., Aguiar, A., Gross, J., *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, pp. 83-92. ACM, 2012.
23. Johansson, G., Rumar, K., *Drivers' brake reaction times*, Human Factors: The Journal of the Human Factors and Ergonomics Society 13, no. 1, pp. 23-27, 1971.
24. W. B. Johnson, *Design and Analysis of Fault-Tolerant Digital Systems*, Addison-Wesley Publishing Company, New York, 1989.
25. Trabelsi C., and A. Yongacoglu, *Effect of Bit-to-Bit Dependence on Packet Error Rate Using Asynchronous DC-CDMA for Mobile Packet Radio Networks*, International Journal of Wireless Information Networks, Vol.2, No.3, 1995.
26. Serageldin A., H. Alturkostani, and A. Krings, *On the Reliability of DSRC Safety Applications: A Case of Jamming*, in Proc. International Conference on Connected Vehicles & Expo (ICCVE 2013), December 2-6, 2013.
27. Serageldin A., and A. Krings, *The Impact of Redundancy on DSRC Safety Application Reliability under Different Data Rates*, in Proc. 6th International Conference on New Technologies, Mobility & Security (NTMS-2014) Dubai, UAE, March 30 –April 2, 2014.
28. Serageldin A., and A. Krings, *The Impact of Dissimilarity and Redundancy on the Reliability of DSRC Safety Applications*, in Proc. Tenth International Symposium on Frontiers of Information Systems and Network Applications, (FINA/AINA 2014), Victoria, Canada, May 13-16, 2014

10 Appendix

The following are publications that resulted from this research:

Ahmed Serageldin, Hani Alturkostani, and Axel Krings, “On the Reliability of DSRC Safety Applications: A Case of Jamming”, in Proc. Intl. Conference on Connected Vehicles and Expo, (ICCVE 2013), Dec. 2-6, 2013, Las Vegas.

Ahmed Serageldin, and Axel Krings, “The Impact of Redundancy on DSRC Safety Application Reliability under Different Data Rates”, in the 6th International Conference on New Technologies, Mobility and Security, (NTMS 2014), Dubai, March 30 - April 2, 2014.

Ahmed Serageldin, and Axel Krings, “The Impact of Dissimilarity and Redundancy on the Reliability of DSRC Safety Applications”, in the 28th IEEE International Conference on Advanced Information Networking and Applications (AINA-2014) Victoria, Canada, May 13-16, 2014.