Paper: ASAT-16-134-CE

16th International Conference on
AEROSPACE SCIENCES & AVIATION TECHNOLOGY,
ASAT - 16 – May 26 - 28, 2015, E-Mail: asat@mtc.edu.eg
Military Technical College, Kobry Elkobbah, Cairo, Egypt
Tel : +(202) 24025292 – 24036138, Fax: +(202) 22621908

Increasing Survivability of DSRC Safety Applications through Dissimilarity and Redundancy without Altering Existing Standards

Ahmed Serageldin*

Abstract: Intelligent Transportation Systems (ITS) are considered one of the most critical infrastructures. For wireless communication ITS uses communications links based on Dedicated Short Range Communication (DSRC) in Wireless Access in Vehicular Environments (WAVE) systems, which is a promising technology to improve traffic safety and reduce highway fatalities. Much research has focused on supporting WAVE safety applications, which depend on many message types. Most important to safety applications is the Basic Safety Message (BSM) as defined in the SAE J2735 Message Set Dictionary Standard. We investigate the survivability of this message exchange, as the industry is moving to the implementation phase, particularly due to the criticality of the system. Therefore fault-tolerance and survivability considerations have to be designed into the system, rather than addressed in an add-on fashion. In this paper we will first give required information introduced by different standards related to this topic. Then we will investigate data reliability of safety application message exchanges for selected scenarios. Finally we propose survivability solutions based on dissimilarity and message redundancy, which only rely on the existing standards.

Keywords: DSRC, V2V, V2I, Jamming, Survivability, Reliability.

I. Introduction

Intelligent Transportation Systems (ITS) are utilizing technology to increase traffic safety and environmental benefits. For example, according to the U.S. Transportation Department ITS reduce traffic hazards, which cause about 43,000 deaths, 3 million injuries and consume over $230 billion dollars each year [1]. ITS are defined according to the United States Department of Transportation (USDOT), Research and Innovative Technology Administration (RITA), as "the application of information technology to surface transportation in order to achieve enhanced safety and mobility while reducing the environmental impact of transportation". The ITS program was initialized and created by the U.S Congress as a national program to incorporate technology and advanced systems into the transportation infrastructure, e.g., to increase traffic safety and decrease pollution and fuel consumption. It was administered by the Department of Transportation in the Intermodal Surface Transportation Efficiency Act of 1991 (ISTEA) which originally named ITS as Intelligent Vehicle Highway Systems (IVHS) [1].

* Ph.D., Egyptian Armed Forces, Egypt

At the core of the ITS are safety applications, which require wireless communications, i.e. wireless signals. It should be obvious that the safety applications are directly affected by any degradation of communication reliability. Such degradation may be the result of adverse effects on the signals implementing communication, but it may also be the result of malicious act. Given that the ITS is a critical infrastructure, that it is a safety critical application, and that any fault, may it be of benign or malicious nature, could have far-reaching consequences, security and survivability are of paramount importance. Security addresses the standard concerns associated with confidentiality, integrity, and authentication, and often includes access control, nonrepudiation, availability, and privacy. Survivability on the other hand takes a more mission-oriented view, in that the "mission must survive", i.e., essential functionalities must perform to specification even in the presence of faults or malicious act [2]. This implies that the system needs to be designed with survivability considerations in mind. Given the wireless nature of communication, may it be vehicle to vehicle or between vehicles and the fixed infrastructure, communication inherits the entire spectrum of potential threats. Furthermore the attack vector cannot be fully predicted. For example, targeted jamming has been shown to be able to introduce Byzantine faults in wireless networks [3] and the safety applications of the ITS are not immune to such attacks either. The mechanisms to increase survivability of ITS safety applications that will be presented in this paper are based on data redundancy associated with applications using a specific kind of message, i.e., the Basic Safety Message (BSM) message described below. They are in line with the Vehicle Safety Communications - Applications (VSC-A) project [4] motivation, which considers data reliability to be essential for the robustness of the system.

The rest of this paper is structured as follows. Section II will provide detailed background on ITS communications and will categorize related work. Section III presents the necessary information from Wireless Access in Vehicular Environments (WAVE) as they apply to the survivability investigation. Safety application scenarios are described in Section IV. Several of these scenarios will be used to describe the solutions to increase survivability of Section V. Finally; conclusions are given in Section VI.

II. 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 FHWA entered into cooperative agreement with ASTM, leading to the publication of the ASTM E2213-03 standard [6] as approved standard for DSRC operations.

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, 5-7]. 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 CH 178), 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 shows a summary of information related to channels.

Table 1. DSRC Channel Allocation

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

Note: “na” = not applicable

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 Vehicular ad hoc Networks (VANET). Research either focused on 1) applications with mechanisms utilizing the BSM messages, or 2) applications that use new messages to increase the functionality of BSM messages.

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 messages 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 messages 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 BSM messages. Such 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.

As it is not possible to give a comprehensive overview of all related work in general, we only gave representative examples. However, to be best of our knowledge, there is no research to date that uses redundant messages from the standard alone to overcome reliability issues or malicious act. We will show an approach that uses BSM messages together with redundant messages from the existing standards to overcome BSM reliability issues.

III. 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 1.

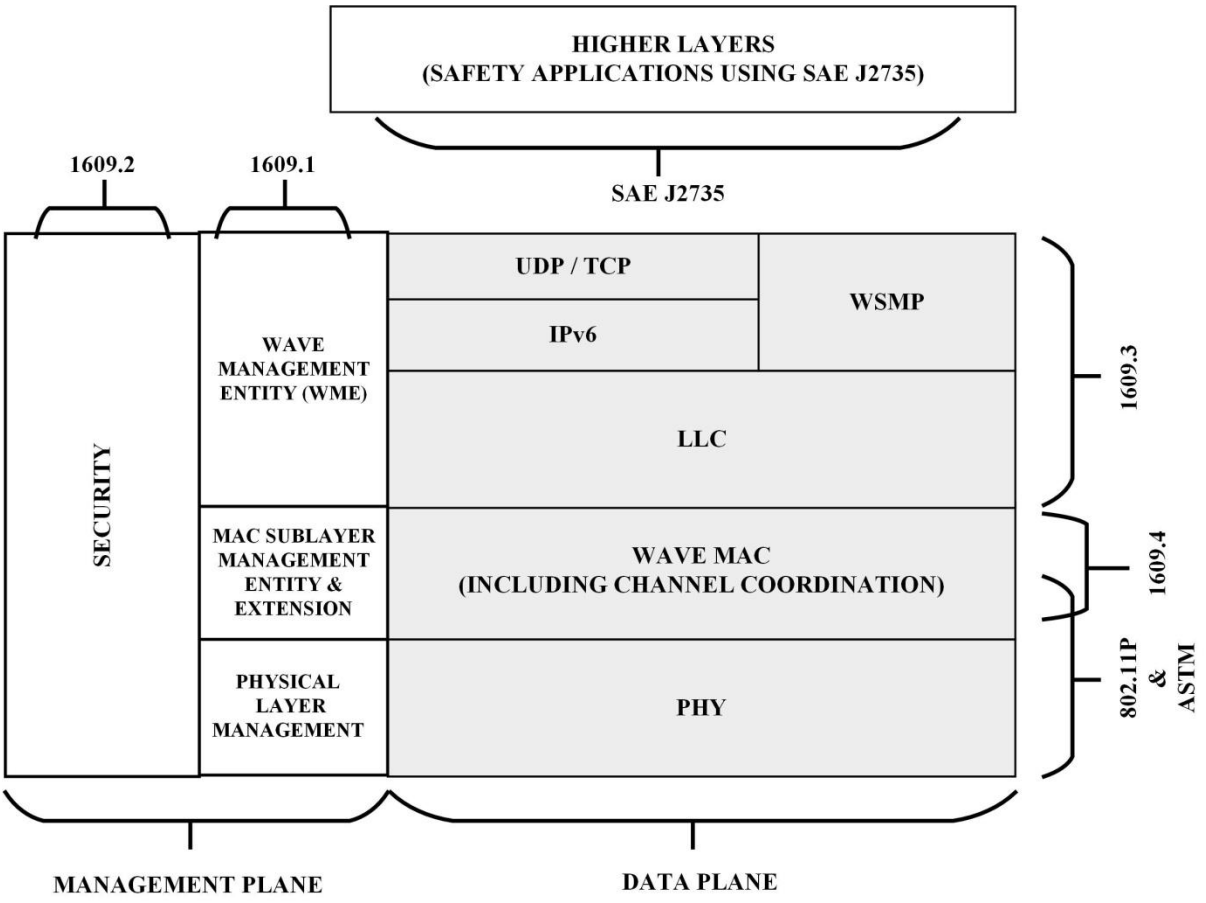

Fig. 1. DSRC Protocol Architecture related to WAVE standards

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], which is an amendment to include the specifications discussed by ASTM E2213-03 standard to support WAVE systems.

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 [13] 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 allow 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.

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 V:

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

IV. Safety Application Scenarios

In order to discuss how one can increase survivability (in Section V), we have 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, which includes 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 2, 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 in Section V and are depicted in Figure 2.

Table 2. 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

Scenario 1: Lead Vehicle Stopped

This scenario, shown in Figure 2a, 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 travelling 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 message 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.

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 2b the RV travelling in the opposite direction occupies the passing zone of HV.

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 2c such warning is issued if the data in the BSM of the RV suggests to the HV that the RV is not stopping.

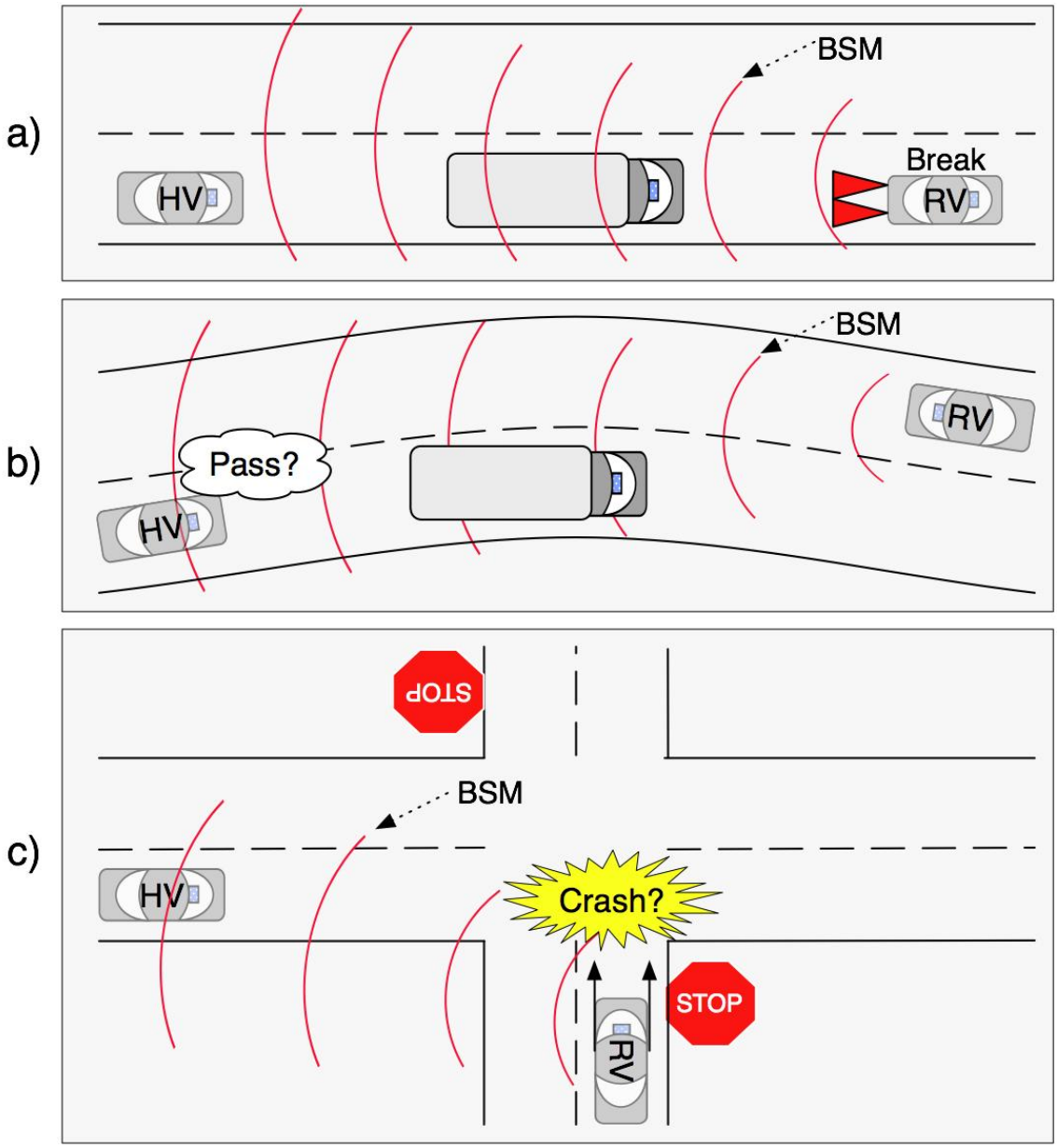

Fig. 2. Selected Crash Scenarios

V. Reliability Consideration and Survivability Solutions

The discussion above has the common thread that the BSM message is the main mechanism used by all safety applications. This message is limited to one specific channel, as will be indicated, 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" [15], to name a few.

To increase the message exchange reliability in the ITS safety applications, we propose an alternative, redundant approach. Specifically we propose the use of other messages from the SAE J2735 standard that are transmitted on different channels from the BSM's safety channel. But first we need to discuss BSM messages in more detail.

Primary Mechanism Using BSM

BSM is defined in SAE J2735 [16] 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 message is about 300 meters. A BSM message 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] BSM messages are transmitted on a pre-agreed channel, i.e., CH172, using the WSM. 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 facility 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.

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 message, i.e., (BSMblob) [16], to get an ACM message containing equivalent information. The message has all the flexibility of the BSM and can even support more data than BSM if desired by an application.

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 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 vehicle type, and most importantly, it has a vector of snapshots, which define the vehicle's travelling 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 message 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). 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 from using the Sample field, and 4) indicate the frequency OBUs will send data using the TxInterval field.
In terms of information content the ACM and PVD messages contain all the required fields to support the functionality of BSM in 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 interferer 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.

Redundant Channel Selection

It is important 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].
For the reasons stated above, we also suggest using at least two WAVE radio devices per OBU for best performance. Dual dissimilar redundancy can be achieved by using the first device dedicated to CH172, the always-on safety channel, for exchanging BSM with full performance. The second device will be a switching radio device that exchanges information on other SCH while participating on CCH. Any device listens to control channel CH178 by default [15] and furthermore, this channel is optimally spaced from CH172 in terms of interference isolation. Therefore CH178 lends itself as 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) [14]. 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 messages, which should take precedence over lower priority messages.

Redundancy Utilizing V2V Communication

For the reasons described above, one candidate for a redundant analog to the BSM messages 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.

Redundancy Involving the ITS 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 to 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 broadcast.
The RSA is an I2V message sent from the RSU to OBUs to alert travellers 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 by Emergency Vehicle Alert message. 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. 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 high power increases the alert range.

Selected Case Study

To demonstrate the redundancy scheme a triple redundant application of Scenario 3 in Section IV, i.e., the Straight Crossing Paths or Turning at Non-signalized Junctions, will be used. Consider the Intersection Movement Assist application used in the host vehicle and the scenario shown in Figure 3a.
In the tradition scenario, which only uses BSM messages, the host vehicle would receive a BSM message from a remote vehicle crossing in its path. If an obstacle blocks the BSM message 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 3a the redundant schemes are provided using the ACM and the PVD involving the RSU.
The communication associated with Scenario 1, i.e., Lead Vehicle Stopped, is depicted in Figure 3b. Assume that channel CH172 is the target of a jamming attack. This will prevent the host vehicle from receiving BSM messages indicating that the remote vehicle is breaking 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 Scenario 2, 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.

Survivability of 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 unreliabilities 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.
This paper describes how redundancy and dissimilarity can be used to mitigate effectively against jamming. Whereas the results for this research had been presented in [20] assuming a homogeneous simplified channel power model, the research in [21, 22] was extended to consider the real impact of the inhomogeneous channels with dissimilar power ratings, as defined in the ASTM E2213-03 standard [36]. In [22] the effect of jamming on the packet delivery ratio was considered for different modulation techniques and diverse data rates.

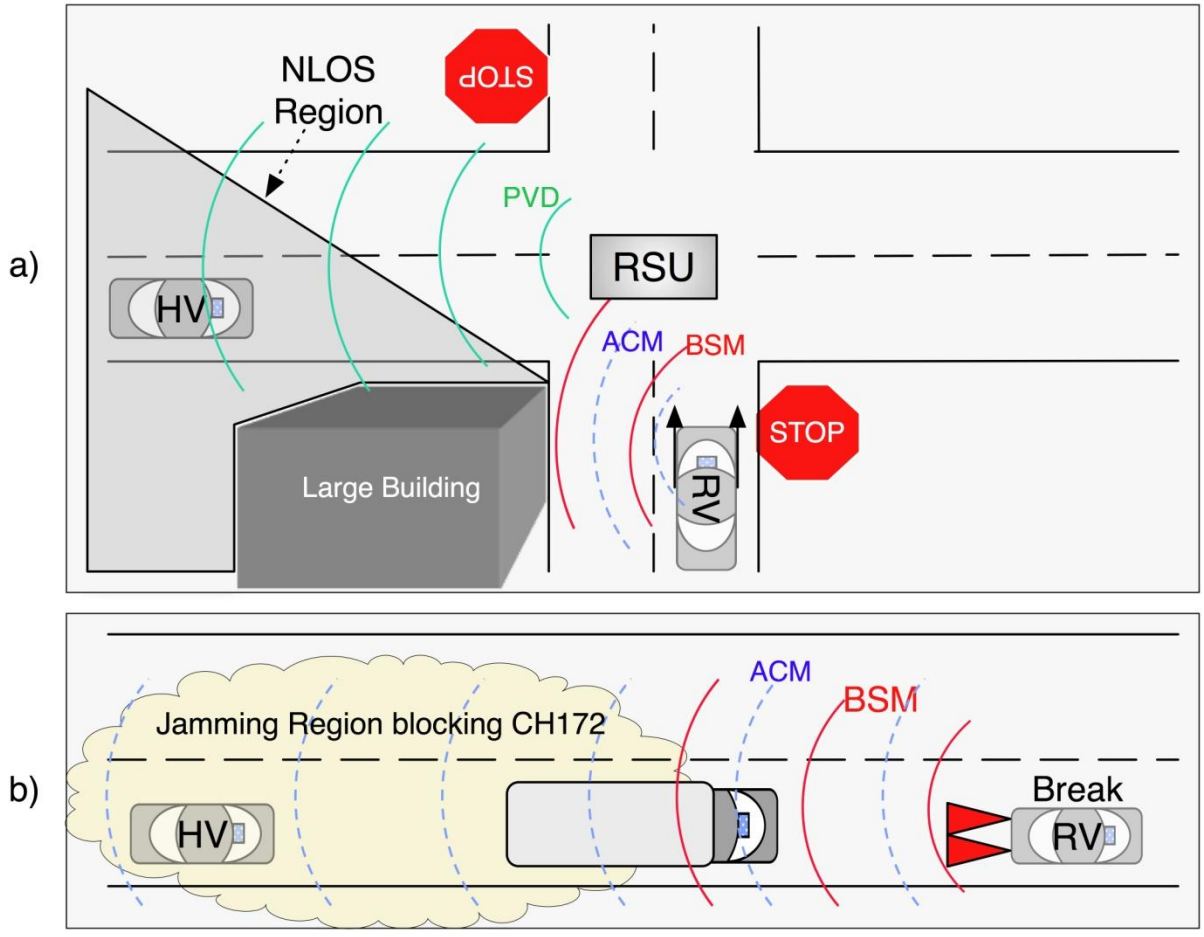

Fig. 3. Demonstrations of Triple Redundancy Mechanism

VI. Conclusion

A new approach to increase survivability of safety applications using DSRC has been presented. The concept of dissimilarity of communication mechanisms has been utilized to increase resilience against interference as the result of natural phenomena and malicious act. The dual or triple redundant mechanisms do not introduce concepts that deviate from existing standards. They only use already defined and established message exchanges that relay on different message types using channels maximally spaced in the spectrum. The information in the standards relevant to the suggested mechanisms is presented to support and justify the decisions taken. The results related to the performance of the proposed solutions had been reported in separate publications [20 - 22].

VII. 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 Misbehaviour 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] 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, 2-6 Dec. 2013, pp. 501 - 506.
[21] A. Serageldin, and A. Krings, The Impact of Dissimilarity and Redundancy on the Reliability of DSRC Safety Applications, in IEEE 28th International Conference on Advanced Information Networking and Applications Workshops (WAINA), Victoria, BC, Canada, 13-16 May 2014, pp. 417 - 424.
[22] A. Serageldin, and A. Krings, The Impact of Redundancy on DSRC Safety Application Reliability under Different Data Rates, in IEEE 6th International Conference on New Technologies, Mobility and Security, (NTMS), Dubai, United Arab Emirates, March 30 - April 2, 2014, pp. 1-5.