The Impact of Dissimilarity and Redundancy on the Reliability of DSRC Safety Applications

Ahmed Serageldin
Department of Computer Science
University of Idaho
Moscow, ID 83843-1010
Email: Sera1405@vandals.uidaho.edu

Axel Krings
Department of Computer Science
University of Idaho
Moscow, ID 83843-1010
Email: krings@uidaho.edu

Abstract—**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, 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. The most important message related to safety applications is the Basic Safety Message (BSM), as defined in the SAE J2735 Message Set Dictionary Standard. Thus, this paper focuses on the reliability of safety applications in the presence of jamming attacks affecting BSM. The case of a constant jammer is considered under the assumption that its capabilities are limited to the technical specifications of the vehicles On-Board Unit (OBU), a device that is readily available for purchase. A communications architecture for safety applications is defined that considers dissimilarity and redundancy to overcome the effects of jamming. The dual and triple-redundant schemes presented enable channels with higher power ratings to communicate the needed BSM data to safety applications. This is accomplished without making any assumptions deviating from the existing standards. Using the Forward Collision Warning safety application, it is shown that the redundancy schemes can effectively overcome the impact of jamming. Furthermore, it is shown that the use of 12 Mbps communication speed is not advisable under the adversary model.**

I. Introduction and Background

Intelligent Transportation Systems (ITS) are utilizing technology to increase traffic safety and environmental benefits. 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 [1]. 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) described below. The redundancy schemes 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.

Whereas communications are affected by many aspects of benign environmental phenomena, the adversarial model addressed in this research is malicious act, specifically jamming. Many different jammer types have been introduced and characterized in [5] [6], ranging from constant jammers, which constantly disrupt communication brute force, to intelligent jammers that are protocol-aware and able to target specific data or control packets.

In this research we picked the constant jamming because it can create wide blind spots and induce immense performance degradation [7], also constant jammers are generally considered the worst case jammers in that their effect is indiscriminatory, even though they are easy to detect compared to more sophisticated jammers [5]. One important factor in jamming is the power that the adversary uses to disrupt. We assume that the jammer capabilities are limited to the technical specifications of the vehicles On-Board Unit (OBU), which is the device installed in vehicles and is readily available for purchase, i.e., its jamming effect is limited by the transmission power model of such devices as specified in the ASTM E2213-03 standard [8].

A. Safety Applications

Since the focus of this research is the reliability of Dedicated Short Range Communication (DSRC) safety applications, we first briefly describe three applications, i.e., realword scenarios listed by the VSC-A project. These scenarios have been tested and analyzed by the VSC-A project, which includes the vehicle manufacturers, and have led to the development of the safety applications [4]. The scenarios described 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. The applications associated with crash scenarios based on [4] are: Emergency Electronic Brake Lights, Forward Collision Warning, Blind Spot Warning+Lane Change Warning, Do Not Pass Warning, Intersection Movement Assist, and Control Loss Warning.

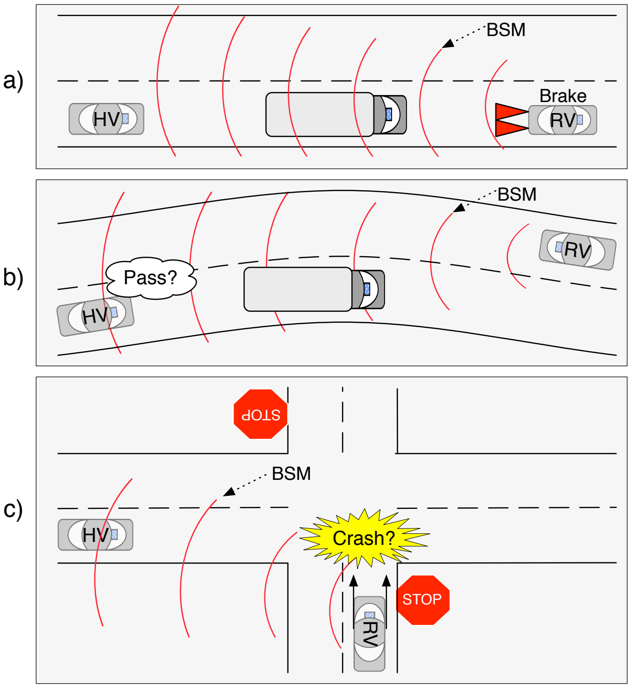

Fig. 1. Selected crash scenarios identified in [4]

Three of the scenarios are depicted in Figure 1. The scenario shown in Figure 1a is 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 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. The Do Not Pass Warning (DNPW) Application alerts a host vehicle attempting a passing maneuver that is not safe. In Figure 1b the passing zone of HV is occupied by the RV traveling in the opposite direction. Figure 1c shows crossing or turning at non-signalized junctions, which uses the Intersection Movement Assist (IMA) application. This application 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. Such warning is issued if the data in the BSM of the RV suggests to the HV that the RV is not stopping.

B. *Related Work*

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 [9], where a non-interactive voting algorithm performed by the vehicle was introduced to detect malicious behavior. The algorithm depends on BSM message broadcasts from other vehicles' reaction to an event to infer on the truth in that event. A different redundancy approach was taken in [10], 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 [11] 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 [12] 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 the 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.

C. *Channel Allocation and Power Limits*

Channel allocation and the power characteristics are important to the concept of redundant communication for safety applications. The DSRC Wireless Access in Vehicular Environments (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 OBU, which is mounted to a vehicle or any portable moving device [13]. The Federal Communication Commission (FCC) licensed 75 MHz of bandwidth at 5.9 GHz (5.850-5.925 GHz) to DSRC [8][14]. 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 [8][13][14]. 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 [14].

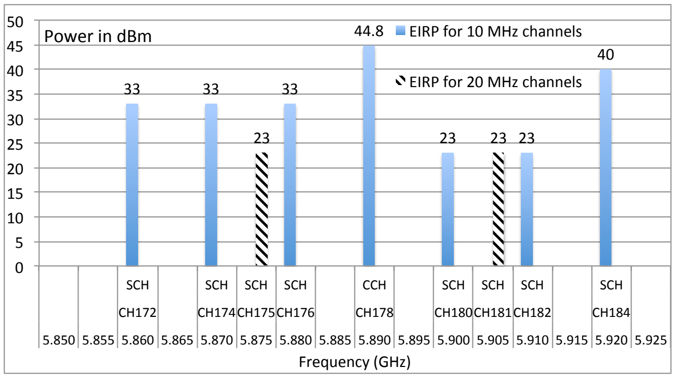

Fig. 2. DSRC channel allocation and power limits

Since the power levels associated with different channels will 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 [8]. 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 non-government [15]. 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 Channel CH175 shall not exceed 10 dBm antenna input power and 23 dBm EIRP. Public Safety OBU operations in Channel CH178 shall not exceed 28.8 dBm antenna input power and 44.8 dBm EIRP. Public Safety RSU and OBU operations in Channel 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 Channels 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 [8], 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 2 shows a summary of information related to channels.

This paper describes how redundancy and dissimilarity can be used to mitigate effectively against jamming. Whereas the research in [16] assumed a homogeneous simplified channel power model, this research is extended to consider the real impact of the inhomogeneous channels with dissimilar power ratings, as defined in [8]. It will be shown how the redundancy scheme utilizes channels that have higher power ratings and how jamming, that would otherwise cause failure of the safety application, becomes largely ineffective. This is without introducing any mechanisms outside of the defined standards. The rest of this paper is organized as follows: Section II will describe the architecture of the redundancy and dissimilarity-based communications architecture. The impact of jamming on the architecture will be analyzed in Section III. Finally, Section IV discusses conclusions and future work.

II. Redundancy-based Survivability Architecture

The BSM message 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 [17][18], 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 [19] capable of providing the application with all required data as 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.

A. 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 message is about 300 meters which depends on the transmitting power on the used channel. 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 [19] BSM messages are transmitted on a pre-agreed channel, i.e., CH172, using the WAVE Short Messages (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.

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 message, i.e., (BSMblob) [19], 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.

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 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). 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 from using the Sample field, and 4) indicate the frequency OBUs will send data using the TxInterval field.

B. 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 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 [14] it was stated that "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 [13], 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.

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 [13] [18] 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 [14] 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 BSM with full performance. The second device will be a switching radio device that exchanges information on any M other SCH while participating on CCH. Below we will present solutions that implement redundancy for the special cases of $M = 2$ and 3, i.e., dual and triple channel redundancy. With a total of 6 service channels, in addition to the control channel, the maximum redundancy level is 7. However, it should be noted that the message overhead will grow linear with the number of redundant channels, imposing extra usage of the dedicated limited bandwidth.

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 2. As stated in [18] 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 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) [18]. 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 sent over CCH.

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.

2) Triple Redundancy Involving the ITS Infrastructure: As shown in Figure 2, the most applicable choice for the third redundant channel is using CH184. The advantages of using CH184 is 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 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 [20] 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 [19]. 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 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 as discussed in the beginning of the subsection.

3) Implication of Triple Redundancy: To demonstrate this redundancy scheme a triple redundant application of the scenario in Figure 1c, 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 3a.

In the traditional scenario, which only uses BSM messages, the host vehicle would receive a BSM message from a remote vehicle crossing in its path. If the BSM message is blocked by an obstacle 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.

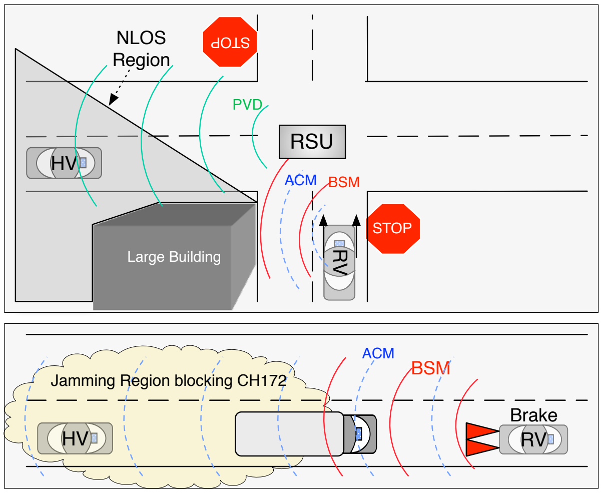

Fig. 3. Demonstration of triple redundancy mechanism

The communication associated with FCW of Figure 1a 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 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.

III. 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 [4].

The timing issues related to the FCW application host and remote vehicles of Figure 1a are shown in Figure 4. 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 BSM messages 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 message from the RV, which is the minimum the application requires to detect the event, before t_{react}. Specifically, as demonstrated using Figure 4, the HV must receive at least one of the first x BSM messages, i.e., BSM$_1$, ..., BSM$_x$, must be received 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 message received after that will arrive too late for the driver to react.

The FCW application reliability is directly linked to the probability of the HV receiving BSM messages 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

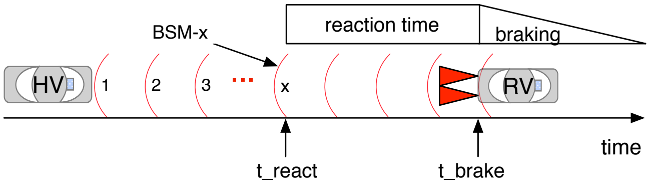

Fig. 4. BSM propagation during FCW

standard definition of reliability, i.e., $R(t)$ is the probability that the system is working to specifications during the entire time interval $[0, t]$ [21], we can define the FCW application reliability as the probability of receiving at least one BSM message before t_{react}, i.e., one of BSM$_i$, for $i = 1, .., x$. Since the application fails only if no BSM message 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 message 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 [6] by

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

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 $SJR_{dB} =$

$$EIRP(t)_{dB} - EIRP(j)_{dB} + 20 \log R_{jr} - 20 \log R_{tr} \tag{3}$$

The impact of the SJR is now used to calculate the PER. However, we need to consider modulation for different bit rates. As stated in ASTM E2213-03 standard [8], 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 [8] and shown in Table II. Assuming Additive white Gaussian noise (AWGN) channel model, the Bit Error Rate (BER), or Bit Error Ratio $P_{b(PSK)}$ for BPSK and QPSK can be expressed using the complementary error function *erfc*() as

$$P_{b(PSK)} = \frac{1}{2} erfc\left(\sqrt{\frac{E_b}{N}}\right) \tag{4}$$

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 $k = \log_2 16 = 4$

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

This is related to the SJR by

$$\frac{E_b}{N} = SJR\frac{B}{R} \tag{6}$$

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

The packet error probability P_p is now approximated by

$$P_p = 1 - (1 - P_b)^N \tag{7}$$

where N is the number of bits of the BSM message. 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 BER. For details about the impact of bit-to-bit dependence on packet error rate the reader is referred to the literature, e.g., [22].

The impact of jamming on the PER of the safety channel CH172, the first redundant channel, i.e., control channel CH178, and the second redundant channel CH184 is shown in Figure 5. As can be seen in the graph, the impact of the jammer increases with the message index, with BSM$_1$ least affected by jamming.

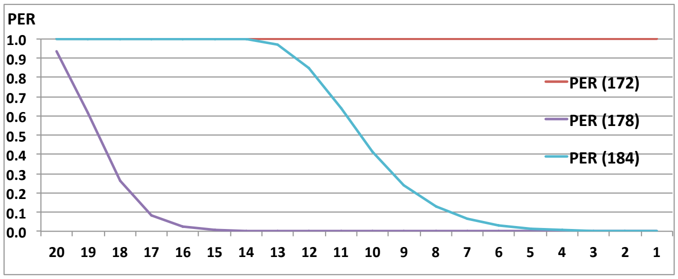

Fig. 5. PER for BSM$_i$ during jamming for different channels

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 message 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 BSM messages before it is too late to react. Since the interval between two

BSM messages is 0.1s, i.e., BSM messages are broadcast every 100ms [19], a maximum of 20 BSM messages could possibly be received, and thus the last message that may be received in Figure 4 is BSM$_{20}$. A summary of the parameter used in the derivation of the application reliabilities is shown in Table I and Table II. This data was extracted from ASTM E2213-03 standard [8].

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	32 μs	CH178 Transmit Power Level	44.8 dBm EIRP, 28.8 dBm i/p power
Duration of the SIGNAL BPSK-OFDM symbol	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 I. Configuration Parameters.

Information Data Rate (Mbits/s)	Modulation	Coding Rate	Coded bits per Sub-carrier 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

TABLE II. Data Rate and Modulation Parameters.

As can be seen in Figure 5, channel CH172 is completely jammed, i.e., PER = 1, and thus any safety application only relying on this channel will fail. For channel CH184 the PER only starts deteriorating starting with message 6, implying that the lower numbered messages are unlikely to be corrupted. Channel 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. 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.

Considering only benign faults, a system consisting of N redundant subsystems C_j, $j = 1,..,N$, fails only if all N subsystems fail, i.e., it functions as long as at least one subsystem functions up to specifications [21]. The unreliability of such system is therefore the product of the unreliabilities of the subsystems. In our case the application unreliability Q_{C_j} of each channel $C_j(t)$ is defined by Equation 1 and thus

$$Q_N(t) = \prod_{j=1}^{N} Q_{C_j}(t) = \prod_{j=1}^{N} \prod_{i=1}^{x} Q_i(t_i) \qquad (8)$$

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.

The unreliability of the FCW safety application, defined in Equation 1 and Equation 8, for 3Mbps communication, is shown in Figure 6. 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 6. When the safety distance between the HV and the RV in Figure 4 allows a message window greater than three messages, the FCW receives messages with very high probability. This point is reached for channel CH184 when the message window grows beyond thirteen. Since channel CH178 is used in the dual and triple redundant schemes, its unreliability dominates that of the schemes, resulting in FCW to work reliably.

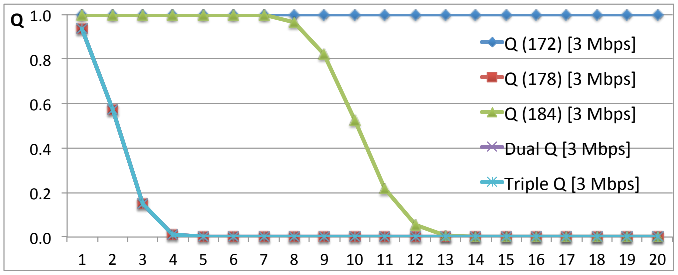

Fig. 6. Unreliability Q of different 3Mbps jammed configurations

In Figure 7, which considers 6Mbps communication, similar behavior can be observed. However, only channel 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. Channel 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.

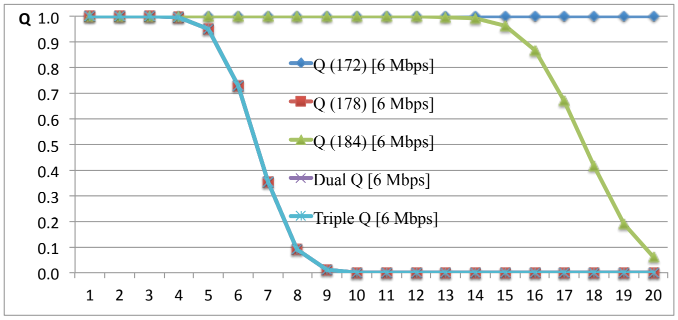

Fig. 7. Unreliability Q of different 6Mbps jammed configurations

The dual-redundant schemes for different data rates are compared in Figure 8. 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.

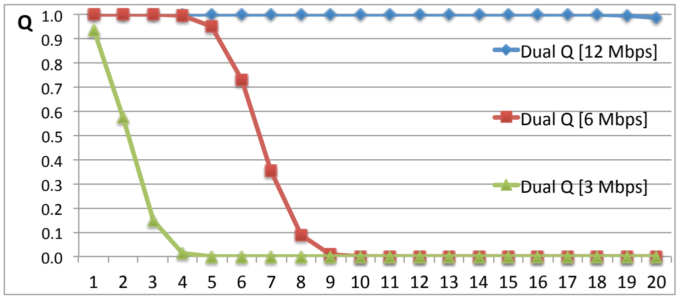

Fig. 8. Impact of data rate of dual configuration on unreliability Q during jamming

IV. Conclusions

A new approach to increase survivability of safety applications using DSRC has been presented. The concept of dissimilarity of communication mechanisms has been used 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 redundancy schemes introduced overcome the impact of jamming assuming that the jammer capabilities are limited to the technical specifications of the vehicles OBU transmission power model. In fact 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. In triple redundancy we suggest using channel CH184 for data rates no higher than 3Mbps for DSRC safety applications. 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.

We acknowledge that using redundancy imposes extra overhead/usage of the dedicated limited bandwidth, which is intended to be used by multiple DSRC applications. However, our main concern is to give high priority consideration to safety applications over any other type of application.

References

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

[2] Krings, A., *Survivable Systems, in Information Assurance: Dependability and Security in Networked Systems*,Morgan Kaufmann Publishers, 2008.

[3] Balogun, V., 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] Vehical Safety Communications-Applications (VSC-A) Final Report. DOT HS 811 492 A. U.S. DoT, NHTSA. September 2011.

[5] 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.

[6] 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, 2^{nd} Quarter 2011.

[7] Puñal, 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.

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

[9] 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. 278285, 13-15 Dec. 2010, Jersey City, NJ, USA.

[10] 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.

[11] 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. 275285, Jan. 2012.

[12] 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. 916, 13-15 Dec. 2010, Jersey City, NJ, USA.

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

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

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

[16] Serageldin A., H. Alturkostani, and A. Krings, *On the Reliability of DSRC Safety Applications: A Case of Jamming*, to appear in Proc. International Conference on Connected Vehicles & Expo (ICCVE 2013), December 2-6, 2013.

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

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

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

[20] Maile M., and L. Delgrossi, *Cooperative Intersection Collision Avoidance System for Violations (CICAS-V) for Avoidance of Violation-Based Intersection Crashes*, paper # 09-0118. Enhanced Safety of Vehicles, 2009.

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

[22] Trabelsi C., and A. Yongacoglu, *Effect of Bit-to-Bit Dependence on Packet Error Rate Using Asynchronous DC-CDMA for Mobile Packet Radio Networks*, Intl. J. of Wireless Information Networks, Vol.2, No.3, 1995.