On the Reliability of DSRC Safety Applications: A Case of Jamming

Ahmed Serageldin, Hani Alturkostani and Axel Krings
Department of Computer Science
University of Idaho
Moscow, ID 83843-1010
Email: Sera1405@vandals.uidaho.edu, altu2655@vandals.uidaho.edu, krings@uidaho.edu

***Abstract*—Dedicated Short Range Communication (DSRC) is the wireless communication protocol of safety applications in Intelligent Transportation Systems (ITS) using Vehicular ad hoc Networks (VANET). Due to the criticality of the 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, our research considers reliability from the safety application point of view, as it is adversely affected by malicious behavior, thus shedding light on application layer reliability. Specifically, the wireless communication shared medium can be used by jammers to launch Wireless Denial of Service (WDoS) attacks. This has great implications for Basic Safety Message (BSM), which is the most important message for safety applications as defined in the SAE J2735 Message Set Dictionary Standard.**

In this paper we study the impact of different jamming types, constant, random, and intelligent, on the reliability of BSM message exchanges. For the research we selected the Forward Collision Warning (FCW), which is one of the identified critical safety applications by the standard. We introduce survivability mechanisms, utilizing the concept of dissimilarity and redundancy, to increase reliability of the application. These mechanisms are strictly compliant with existing standards, and thus do not require any mechanisms outside of the standards. The impact of the different jamming types and the effectiveness of our solutions on the application reliability are demonstrated.

I. Introduction and Background

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].

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 dealt with concepts and solutions optimized for interoperability between standards, performance of communications, and functionality of services [2]. This led to the adoption of 5.9 GHz Dedicated Short Range Communication (DSRC) over existing 900 MHz DSRC. 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 [3] as approved standard for DSRC operations.

A. DSRC/WAVE Background

In Wireless Access in Vehicular Environments (WAVE) systems the DSRC protocol provides the communication between two devices. One of the devices is the communication support of the vehicle, while the other can be any WAVE device, such as another vehicle, roadside units, or pedestrians. According to the ASTM E2213-03 standard the device in the vehicle is defined as the On-Board Unit (OBU), which is mounted to a vehicle or any portable moving device [4]. For stationary devices the WAVE standards define the Road Side Unit (RSU), which is permanently mounted. The resulting communication scenarios are Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Infrastructure-to-Vehicle (I2V).

For DSRC communication the Federal Communication Commission (FCC) has licensed 75 MHz of bandwidth at 5.9 GHz (5.850-5.925 GHz). The bandwidth is divided into 7 channels, each with a bandwidth of 10 MHz [1][3]. They consist 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 [4]. 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 I shows a summary of information related to channels.

Testing communications related to vehicles was spearheaded by the Vehicle Safety Communications-Applications (VSC-A) team [5]. One of the most important goals in the VSC-A project was to develop and test Basic Safety Message (BSM) for V2V communication that can be used by safety applications to communicate in all directions of the host vehicle. BSM is defined in SAE J2735 standard [6] and

Channel Number		Channel Use	Bitrate (Mbps)		Bandwidth (MHz)		Frequency Range (GHz)
CH170		Reserved	-		5		5.850 - 5.855
CH172		SCH	3-27		10		5.855 - 5.865
CH174	CH175	SCH	3-27	6-54	10	20	5.865 - 5.875
CH176		SCH	3-27		10		5.875 - 5.885
CH178		CCH	3-27		10		5.885 - 5.895
CH180	CH181	SCH	3-27	6-54	10	20	5.895 - 5.905
CH182		SCH	3-27		10		5.905 - 5.915
CH184		SCH	3-27		10		5.915 - 5.925

TABLE I
DSRC CHANNEL ALLOCATION

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.

B. 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 [7] 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 [7][8]. 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 affect 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 [8]. 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 paper, we investigate the safety application reliability as it is affected by constant, random and intelligent jammers. We picked the constant jamming because it can create wide blind spots and induce immense performance degradation [9]. Random jamming was picked as its impact on reliability is limited, depending on sleeping period. Intelligent jamming was selected because it is highly sophisticated.

C. Survivability and its Role in Critical Infrastructures

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 [10]. This implies that the system needs to be designed with survivability considerations in mind. Given the wireless nature of communication, may it be V2V or V2I, 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 [11] 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 of BSM messages. They are in line with the VSC-A project [5] motivation, which considers data reliability to be essential for the robustness of the system.

II. APPLICATION RELIABILITY AND SURVIVABILITY

Application reliability is highly dependent on the message exchanges and requirements of the specific application considered. For our research we selected the Forward Collision Warning (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 [5].

A. Forward Collision Warning

The FCW application alerts the driver of the Host Vehicle (HV) of an impeding rear-end collision with a Remote Vehicle (RV) traveling ahead in the same direction in the same lane. Such scenario is depicted in Figure 1, where vehicles are traveling at constant speed. When the RV brakes hard it initiates broadcasting of this event via BSM messages to the surrounding vehicles. The vehicles following the RV use the BSM messages emitted by the RV to alert the driver about a possible collision. This may be especially useful in situations of low visibility or visual obstruction, as shown in the figure, where HV cannot directly see the RV since another vehicle blocks its view.

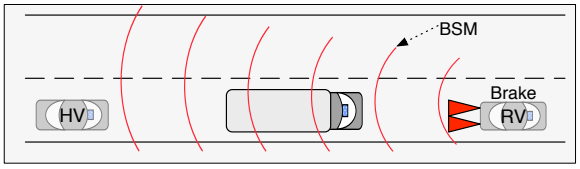

Fig. 1. Forward collision warning scenario with remote and host vehicle

The timing issues related to HV and RV in the scenario of Figure 1 are shown in Figure 2. 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 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}. As seen in Figure 2, this means that HV must receive at least one of the first x BSM messages, i.e., BSM_1, ..., BSM_x. Any BSM message received after that will arrive too late for a driver to be able to react. Typical reaction times are within 0.9s [12].

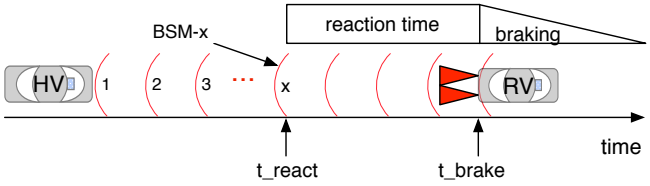

Fig. 2. BSM propagation and impact on application

B. Application Reliability

The FCW application reliability is directly linked to the probability of the HV receiving BSM messages before it is too late to react. In line with the standard definition of reliability, i.e., $R(t)$ is the probability that the system is working to specifications during the entire time interval $[0, t]$ [13], we can define our 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}, 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 packet error probability 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.

C. Impact of Jamming

Figure 3 shows FCW scenarios, where the host vehicle's reception of the BSM messages 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.

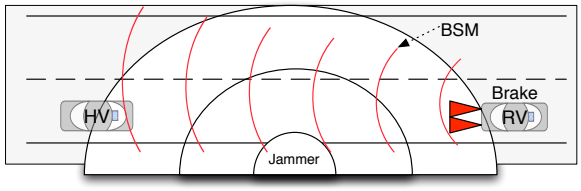

Fig. 3. FCW under jamming

Three interesting jamming scenarios are shown in Figure 4. Whereas the figure shows the timeline, it should be clear that these times relate to distances. In Figure 4a) 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 4b) 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 4c). 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.

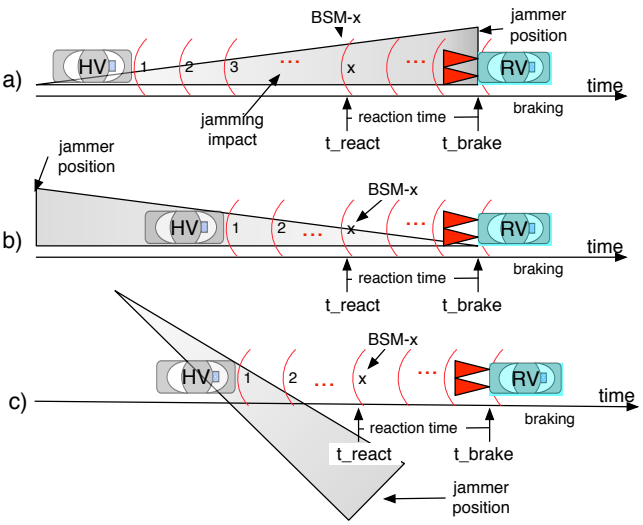

Fig. 4. Jammer positions

III. Reliability Quantification

In order to obtain the application unreliability indicated in Equation 1 we need the values of Q_i, which are the packet

error probabilities at the time BSM$_i$, for $i = 1, ..., x$, is received. Note that these probabilities change as the HV moves towards or away from the jammer.

We first need to compute the Jamming-to-receiver Signal Ratio (JSR), which depends on signal powers and distances, as it applies for each BSM$_i$. The JSR is given in [8] by

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

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.

The JSR for two constant jammers is plotted in Figure 5, for the scenario of Figure 4a). The assumptions for the graph are as follows: P_t was set to 20dBm, P_j to 10 dBm 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 BSM messages before it is too late to react. Since the interval between two BSM messages is 0.1s, a maximum of 20 BSM messages could possibly be received, and thus the last message that may be received in Figure 4a) 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.

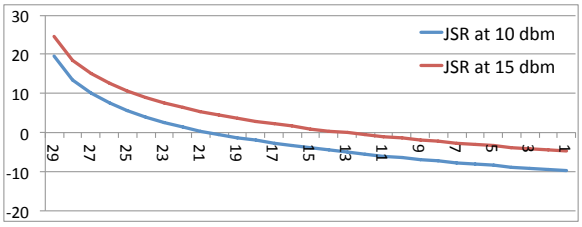

Fig. 5. Jamming-to-signal ratio in dB related to messages BSM$_i$

A. Packet Error Probability

The impact of the JSR is now used to calculate the packet error ratio (PER), or packet error probability. The BSM messages are sent on the 6Mbps Channel CH172 using QPSK 1/2 encoding [3][4]. Assuming Additive white Gaussian noise (AWGN) channel model, the bit error probability P_b for QPSK can be expressed using the complementary error function *erfc*()

$$P_b = \frac{1}{2} erfc\left(\sqrt{\frac{E_b}{N_0}}\right) \tag{3}$$

This is related to the JSR by

$$\frac{E_b}{N_0} = \left(\frac{1}{JSR}\right)\frac{B}{R} \tag{4}$$

where R is the channel information data rate, here 6Mbps, and B is the channel bandwidth, here the 8.3MHz occupied bandwidth of the 10MHz channel [3].

The packet error probability P_p is now approximated by

$$P_p = 1 - (1 - P_b)^N \tag{5}$$

where N is the number of bits of the BSM message. It should be noted that Equation 5 however assumes independence of faults. The rational behind the approximation is that the effect of jamming is considered constant over the jamming time and is reflected in the bit error probability. For details about the impact of bit-to-bit dependence on packet error rate the reader is referred to the literature, e.g., [14]. We assume a BSM message 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 6. The x-axis labels i indicate the total number of BSM messages that were sent by t_i and may be received before t_{react}, whereas the y-axis is the corresponding unreliability $Q(t) = \prod_1^x Q_j(t_j)$ 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 BSM messages 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 BSM messages due to jamming was 10^{-18}.

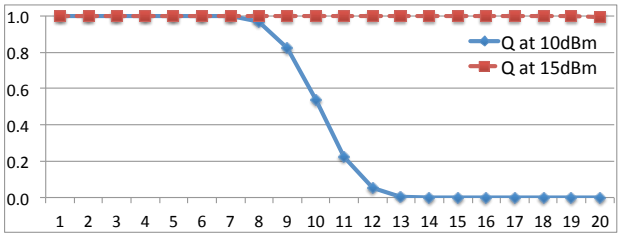

Fig. 6. $Q(t)$ under constant jamming over number of BSM messages sent

B. Impact of Random Jammer on $Q(t)$

Figure 6 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 message 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 message. Thus, the application unreliability as it is affected by random jamming is

$$Q_{rand}(t) = \prod_1^x (1 - P_s) Q_i(t_i) \tag{6}$$

where $Q_i(t_i)$ is the unreliability of BSM reception at t_i during jamming. Equation 6 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 7. For the 15dBm jamming scenario the unreliability, which was unacceptable in Figure 6, 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 6 was 10^{-18} for the 20 messages.

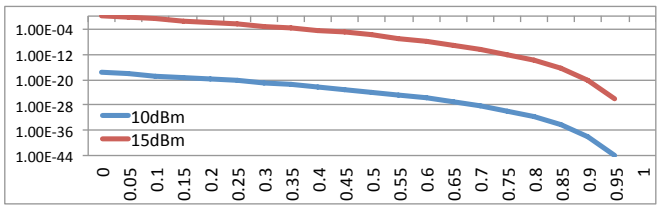

Fig. 7. Impact of sleeping probability (x-axis) on Q(t) (y-axis)

IV. Application survivability based on redundancy

Reliability of safety applications depends on BSM message exchanges. The BSM messages use the safety channel, CH172. Thus for any safety applications, as they depend on the BSM, this channel constitutes a single point of failure. Failure sources include obstacles, congestions, simple and sophisticated jamming, to name a few [15]. We want to introduce channel redundancy and message dissimilarity as mitigation techniques. In the first case we utilize alternative channels in addition to CH172, and in the latter we use alternate messages from the SAE J2735 standard capable of proving the application with all the required data to support the functionality of BSM.

A. Message Dissimilarity

BSM is defined in SAE J2735 and it 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 [6] BSM messages are transmitted on a pre-agreed channel, i.e., CH172, using the WAVE Short Message Protocol (WSMP). Two message types will be introduced next that can provide a safety application with the same information as contained in the BSM.

1) Redundancy using A la Carte Message: The first message is the A la Carte Message (ACM), 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) [6], 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 Probe Vehicle Data: The second message is Probe Vehicle Data (PVD). It is a V2I message, a unicast from the OBUs to an RSU using the WSMP 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 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.

B. Channel Redundancy

In the standards [1], [4] it is stated that any safety application can be licensed on all channels. This makes it possible to use any of the control or service channels as safety channels in an attempt to eliminate the aforementioned single point of failure (BSM is limited to CH172).

As for the placement of the channels we suggest the redundant channels to be far apart, to increase resilience against natural and malicious external interference such as shadowing or jamming. This is in line with the VSC-A project's cross-channel interference (CCI) field test results [5].

Related to our technical report [16] we suggest that each vehicle should use two separate radio devices, as suggested by VSC-A. The first radio will be dedicated to CH172 for BSM exchange [5]. The second radio will be a switching radio device that exchanges information on other service channels while participating on the control channel [15]. Since the control channel CH178 is the default channel that every device listens to, and this channel is optimally spaced from CH172 in terms of interference isolation, it lends itself as optimal candidate for the redundant channel.

For the third redundant channel we suggest CH184 because its advantage is twofold. First it maximizes the spectrum separations for the other channels used in the redundancy scheme, which provides higher resilience to interference, and second the high power has the potential to increase the signal-to-jamming ratio.

We suggest to use ACM with CH178 and the PVD with CH184, with the support of other messages, as described in detail in [16].

C. The Impact of Redundancy

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 [13]. The unreliability of such system is therefore the product of the unreliabilities of the subsystems. In our case the application unreliability $Q_{C_j}(t)$ of each channel C_j is defined by Equation 1 and thus

$$Q_N(t) = \prod_{j=1}^{N} Q_{C_j}(t) = \prod_{j=1}^{N} \prod_{i=1}^{x} Q_i(t_i) \quad (7)$$

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 in Subsection IV-A. 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 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 8 shows the impact of redundancy on unreliability of such scenario as a function of the number of BSM messages 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.

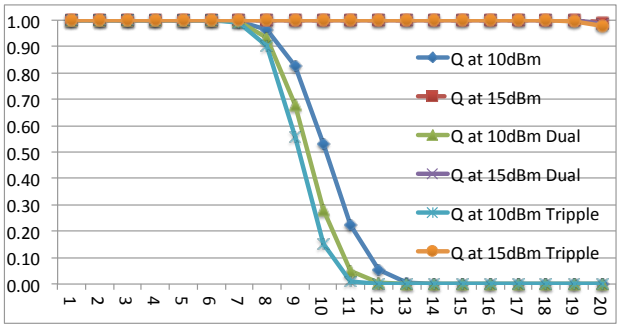

Fig. 8. Impact of redundancy on $Q(t)$ (y-axis) for BSM messages (x-axis)

V. Conclusion

This paper addresses reliability of DSRC safety applications, considering jamming, which has the potential to adversely affect the applications to the point of rendering them useless. The application reliability has been derived for the FCW application as it is impacted by three kinds of jamming: constant, random and intelligent jammer. Jamming has not impact on any redundant schemes if it is limited to a single channel. For multi-channel jamming we show that for a constant jammer the application reliability is strongly reduced unless the jamming power is low or the distance to the jammer is large. In the case of random jammer the sleeping time probability dominates the reliability. Channel and message redundancy has been introduced without using mechanisms outside of standards for applications relying on BSM messages. The impact of channel redundancy is that unless all channels are jammed, the safety applications is unaffected.

References

[1] 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.

[2] Makaya, C., S. Pierre., *Emerging Wireless Networks: Concepts, Techniques, and Applications*, CRC Press, Taylor & Francis, New York, 2011.

[3] 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.

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

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

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

[7] 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.

[8] 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.

[9] 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.

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

[11] 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.

[12] 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.

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

[14] 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.

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

[16] Ahmed Serageldin, Axel Krings and Ahmed Abdel-Rahim, *Increasing Survivability of DSRC Safety Applications Through Dissimilarity and Redundancy Without Altering Existing Standards*, Technical Report TR-UI-2013-0801, Computer Science Department, University of Idaho, 2013.