The Impact of Redundancy on DSRC Safety Application Reliability under Different Data Rates

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

This paper only addresss V2V safty, so only present the maximum allowable power for some public OBU and RSU

This paper focus on the BSM failure (like, jamming)

***Abstract*—This research addresses reliability issues of safety applications in Intelligent Transportation Systems (ITS) that use Dedicated Short Range Communication (DSRC) in Wireless Access in Vehicular Environments (WAVE) systems. Reliability of such applications is affected not only by the usual environmental effects of wireless communication, but also potentially by malicious act. The case of constant and random jamming and their impact on safety applications are investigated under consideration of the data rates used. It is shown that the most important message, the Basic Safety Message (BSM), which is transmitted on a dedicated safety channel can be jammed, resulting in safety application failure. To mitigate against jamming a communication scheme based on redundant channel is used that utilizes channels with higher power ratings for communicating data with BSM-equivalent content, while not deviating from existing standards. The impact of channel and message redundancy for different data rates is investigated. Considering the two jammer types, it is shown that the introduction of redundancy overcomes the impact of jamming attacks. Furthermore it is demonstrated that application reliability increases inverse to the data rates of the channels. Analysis shows that DSRC safety applications that use redundant communication can overcome jamming attacks if data rates of 3Mbps and 6Mbps are used, while 12Mbps communication is not advisable.**

Keywords: ITS, DSRC, BSM, Vehicular Network, Connected Vehicles

I. Introduction and Background

Intelligent Transportation Systems (ITS) are utilizing technology to increase traffic safety and environmental benefits. For wireless communication ITS uses communications links based on Dedicated Short Range Communication (DSRC) in Wireless Access in Vehicular Environments (WAVE) systems. 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 [1]. Due to the fact that the ITS is a safety critical system, the security and survivability of the services it provides are paramount. Failure could have catastrophic consequences and public trust in the technologies would be undermined.

Well noted Background of the DSRC

A. Channel Allocation and Power Limits

DSRC Channel allocation and the power characteristics are important to the concept of redundant communication for safety applications. The Federal Communication Commission (FCC) licensed 75 MHz of bandwidth at 5.9 GHz (5.850-5.925 GHz) to DSRC [2][3]. There are seven 10 MHz channels from (5.855-5.925 GHz), consisting of one Control Channel (CCH), i.e., channel 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 [1][2][3].

The transmit power levels for public safety RSU and OBU operations in DSRC channels were introduced in the ASTM E2213-03 standard [3]. 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 services [4]. Since this research addresses the reliability of V2V safety applications, we will only present the maximum allowable power for some public safety OBU and RSU operations. According to the standard Public Safety OBU operations in Channel CH172 shall not exceed 28.8 dBm antenna input power and 33 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. RSUs and OBUs shall transmit only the power needed to communicate over the distance required by the application being supported.

B. Jamming in DSRC communications

As stated in ASTM E2213-03 standard [3], DSRC uses Orthogonal Frequency Division Multiplexing (OFDM) and uses binary or quadrature phase shift keying (BPSK/QPSK) and 16-quadrature amplitude modulation (QAM), which support the

Here denote that another papers usually talk about enviornment issues related to signal degradation

mandated data rates of 3Mbps, 6Mbps and 12Mbps. These rates will be subject of our investigations.

Whereas much research has focussed on dealing with the environment issues related to signal degradation, we focus on the impact of jamming as a malicious act. Different jamming types and their associated problems have been identified in [5][6]. These types include *Constant Jammer*, which emits a constant radio signal to interfere with legitimate communication, and *Random Jammer*, which unpredictably jams for t_j and sleeps for t_s seconds. We picked the constant jamming because it can create wide blind spots and induce immense performance degradation [7], whereas random jamming was picked as its impact on reliability is limited, depending on sleeping period. The jammer's capabilities are assumed to be limited to the technical specifications of an OBU. This is due to the fact that our current field implementation, to be published later, uses such device as a jammer.

In our previous work [8][9] we introduced a communication architecture based on dissimilarity of message and channel redundancy to mitigate against jamming attacks. We extend this work to focus on jamming as it impairs OFDM channel data rates.

II. The Reliability of Safety Applications

All DSRC safety applications rely on the Basic Safety Message (BSM), the most important message for safety applications as defined in the SAE J2735 Message Set Dictionary Standard [10]. The BSM is limited to one channel, i.e, the safety channel CH172, to communicate all the data needed by safety applications. This channel represents a single point of failure, which can affect the reliability of all safety applications. The possible faults may originate from simple obstacles to potential malicious act like jamming. The implications of BSM message faults on applications will be demonstrated using a selected safety application, described below.

A. Redundancy-Based Architecture

Not really understand this part

The communications architecture that is the basis for this research is described in detail in [8][9]. This architecture uses two main concepts, message dissimilarity and channel redundancy. Message dissimilarity is achieved by selecting other messages from the SAE J2735 standard [10], capable of providing the application with all required data of the BSM. In terms of information content the À la Carte Message (ACM) and Probe Vehicle Data (PVD) messages contain all the required fields to support the functionality of BSM in safety application.

Channel redundancy is based on two criteria, 1) the channel distance in the frequency spectrum, and 2) the maximum allowed channel transmitting power. One suitable candidate for channel redundancy is the control channel CH178, which 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. The other candidate is CH184, offering two advantages. Firstly, it maximizes the spectrum separation to the other channels used in the redundancy scheme, which provides higher resilience to interference. Secondly, the EIRP of CH184 is higher than that of CH172, i.e., 40 dBm and 33 dBm respectively.

As stated above, one candidate for a redundant analog to the BSM messages is the ACM, which is to be sent on the CCH CH178 with higher priority to take precedence over other messages. This, together with CH172, implements a system with dual redundancy utilizing dissimilarity, i.e., two different messages on two different channels, to increase survivability of safety applications. For triple-redundancy the PVD was selected to be sent as unicast from vehicles to the RSU on CH184. The RSU will send alerts to vehicles if the infrastructure detects a hazard using a message called Road Side Alert (RSA).

An OBU is assumed to have two radios, according to the VSC-A project recommendation [11]. One is dedicated to safety channel CH172, whereas the other switches between control channel CH178 and any other service channel. Whereas dual redundancy utilizes two radios, any high redundancy scheme will share radios in a switching fashion.

B. Forward Collision Warning

So, here is the problem may be happened???

The highest ranked safety application based on crash frequency, cost and functional years lost, according to the VSC-A project [11], is the Forward Collision Warning (FCW) application, which will be used in this research. This application scenario is shown in Figure 1a, in which the driver of the Host Vehicle (HV) is alerted of an impending rear-end collision with a Remote Vehicle (RV) traveling ahead in the same direction and on the same lane. As shown in the figure, when the RV brakes hard, it broadcasts this event via BSM messages to the surrounding vehicles. The vehicles following the RV will use this information to alert their drivers about a possible collision. This may be very useful in situations with low visibility, e.g., heavy fog or vision obstruction by large vehicles.

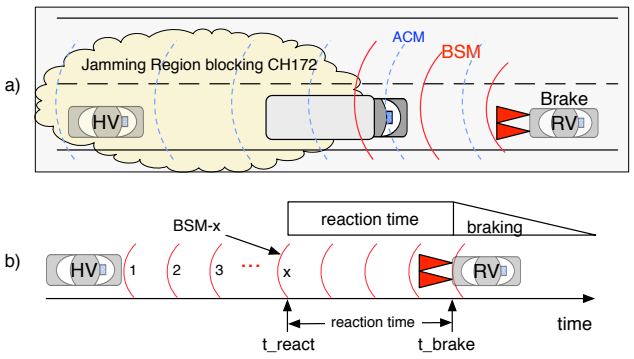

Fig. 1. FCW scenario and BSM propagation diagram

C. Safety 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. Thus the application reliability depends on the packet error ratio (PER), or packet error probability and their impact on message exchanges. The derivation below is based on [9]. 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 $[0, t]$ [12], we can define the FCW application reliability as the probability of receiving at least one BSM message. Specifically, as demonstrated using Figure 1b, at least one BSM message, i.e., one of BSM$_i$, for $i = 1, .., x$, 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. This reaction time is from t_{react} to t_{brake}.

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

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

Here 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. The position of the jammer in this scenario is assumed to be right next to the RV. A hypothetical situation following this logic is where the adversary with the jammer causes the event that leads to braking, e.g., launching an obstacle into the moving traffic.

To obtain the application unreliability indicated in Equation 1 we need the values of Q_i, which are the PER at the time BSM$_i$, for $i = 1, ..., x$, is received. Packet error probabilities are derived from the receiver Signal-to-Jamming Ratio (SJR), which depend on signal powers and distances, as it applies for each BSM$_i$. The SJR is given in [5] 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, i.e., for 3Mbps using BPSK 1/2, for 6Mbps using QPSK 1/2, and for 12Mbps 16-QAM 1/2, as defined in [3] and shown in Table II. Assuming Additive white Gaussian noise (AWGN) channel model, the Bit Error Rate (BER), or bit error probability, $P_{b(PSK)}$ for BPSK and QPSK can be expressed using the complementary error function *erfc*() as

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

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. This assumes that jamming noise dominates other noise.

The PER P_p is now approximated by $P_p = 1 - (1 - P_b)^N$, 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., [13].

III. Experimental results for FCW

The impact of jamming on the redundancy schemes for FCW using channels CH172, CH178 and CH184 will be presented for the case of a constant and random jammer. As stated previously, the jammer is assumed to be positioned next to the remote vehicle in Figure 1b. Further assumptions are: 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 [10], a maximum of 20 BSM messages could possibly be received, and thus the last message that may be received in Figure 1b is BSM$_{20}$. The parameters of the analysis are shown in Table I and Table II, which were extracted from ASTM E2213-03 standard [3].

A. Considering Constant Jammer

The impact of constant jamming on the PER of the safety channel CH172, the first redundant channel, i.e., control channel CH178, and the second redundant channel CH184, is shown in Figure 2. As the HV approaches the jammer the PER of the safety messages increases. It can be seen in the

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

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

Given the packet error rates of Figure 2 the FCW unreliabilities were derived for triple-redundant configurations, as shown in Figure 3. The unreliabilities shown reflect the number of messages, i.e., terms, used in Equation 1. Thus,

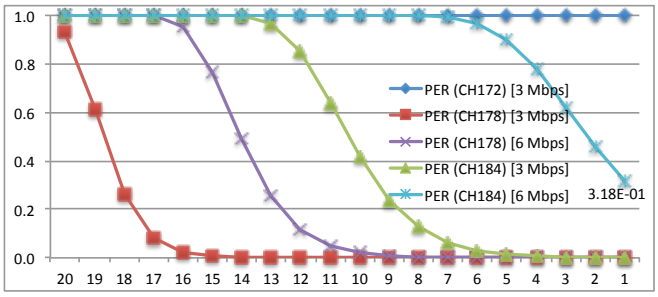

Fig. 2. PER of safety message i (x-axis) using 3Mbps and 6Mbps for different channels affected by constant jamming

the best unreliabilities are achieved when all 20 messages are used, where the dominating messages are the first ones received, i.e., the message with lowest PER in Figure 2, which is message 1. Most importantly, for 12Mbps even the triple-redundant implementation results in unacceptable unreliability close to one. When using lower data rates, i.e., 3Mbps and 6Mbps, all triple configurations can, for all practical purposes, completely overcome jamming.

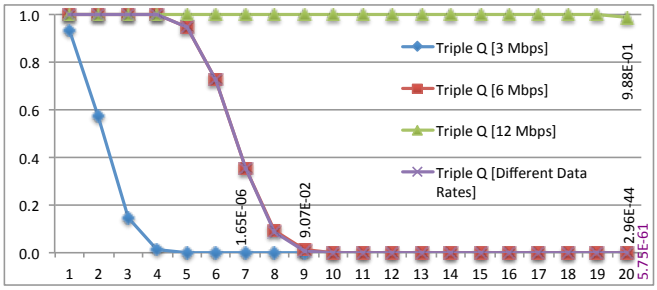

Fig. 3. Unreliability Q of different triple redundant configurations, constant jammer, over total number of BSM sent

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

B. Considering Random Jammer

The unreliabilities of random jamming for different sleep ratios are shown in Figure 4 for CH172 using 3Mbps, and for different triple redundant scenarios in Figures 5 and 6. The most important observation is that the unreliabilities now are dominated by the sleep ratios. All scenarios, no matter whether the data rates are 3, 6, or 12Mbps, are unaffected by jamming unless the sleeping times are small, e.g., less than 25% in Figures 4 and 5. The justification for this is that as the sleeping times increase the probability for messages to not experiencing jamming is high. Thus even the 12Mbps scenario, which was not usable in the constant jammer case, is immune to random jamming, if the sleep ratio is above 25%.

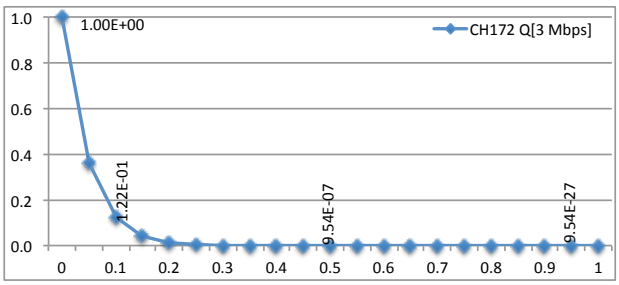

Fig. 4. Unreliability Q of CH172 using 3Mbps under random jamming, over sleeping ratio

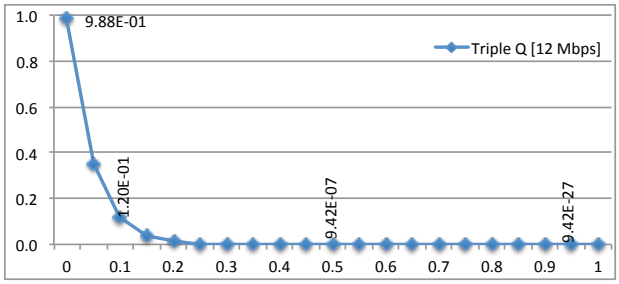

Fig. 5. Unreliability Q of 12Mbps configuration under random jamming, over sleeping ratio

Extreme resilience against random jamming can be observed in Figure 6 for triple redundant configurations using 3 and 6Mbps. One should note that the unreliabilities are insignificantly low, as even the constant jammer, which is a special case of random jammer with sleeping time zero, could cope in this configuration. All results for random jammers

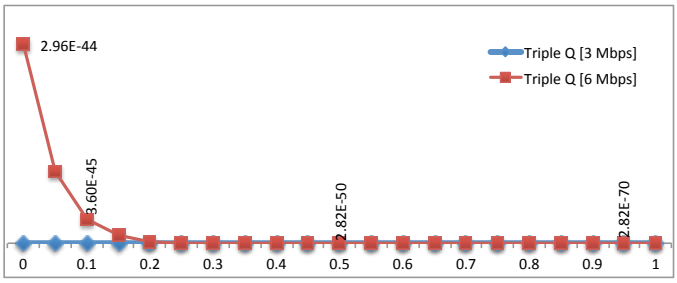

Fig. 6. Unreliability Q of 3 and 6Mbps configurations under random jamming, over sleeping ratio

do not even consider the time the jammer would need to switch channels, e.g., to switch between CH178 and CH184, which is bound by 2ms [3]. In site of message delays of approximately 6.3ms, 3.5ms and 2.3ms for 3Mbps, 6Mbps and 12Mbps rates respectively, considering maximum message length, such channel switching would effectively count as non-jamming time.

IV. Conclusions

This paper addressed the reliability of DSRC safety applications in site of jamming attack, considering constant and random jammers. It is shown how different data rates were affected by jamming, and that for 3Mbps and 6Mbps both jamming types are ineffective if redundancy is used. For constant jamming it was observed that the control channel dominates the reliability due to its high power. As a result it allowed to use higher data rates on that channel, up to 6Mbps. This in turn would allow the usage of higher data rates in other channels, as the control channel reliability has greatest effect on the application reliability. Channel rates of 12 Mbps were found to be unreliable for the case of constant jamming. For random jamming it could be shown that reliability is highly dependent on the sleeping ratios. For sleeping ratios above 25% random jamming has no effect on reliability on all data rates. However, for lower sleeping rates, random jamming causes reliability characteristics closer to that of constant jamming.

As also stated in our previous work, 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 Draft Guide for Wireless Access in Vehicular Environments (WAVE) -Architecture, IEEE P1609.0/D5, September 2012.

[2] 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.

[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 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.

[5] 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.

[6] 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.

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

[9] Serageldin A., and A. Krings, *The Impact of Dissimilarity and Redundancy on the Reliability of DSRC Safety Applications*, in Proc. 10^{th} International Symposium on Frontiers of Information Systems and Network Applications, (FINA 2014), Victoria, Canada, May 13-16, 2014.

[10] SAE J2735 Dedicated Short Range Communications (DSRC) Message Set Dictionary, SAE, DSRC Committee, Nov. 2009.

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

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

[13] Trabelsi C., et.al, *Effect of Bit-to-Bit Dependence on Packet Error Rate Using Asynchronous DC-CDMA for Mobile Packet Radio Networks*, Intl. Journal of Wireless Information Networks, Vol.2, No.3, 1995.