Paper ID # AM-TP1672

Challenges of sharing the DSRC band in the U.S.

Bin Cheng[1], Hongsheng Lu[2], Ali Rostami[1], Marco Gruteser[1], John B. Kenney[2*]

1. WINLAB, Rutgers University, U.S.A

2. Toyota Info Technology Center, U.S.A

tel:650-694-4100, email: jkenney@us.toyota-itc.com

Abstract

As DSRC moves towards large-scale deployment in the U.S., the potential coexistence of unlicensed devices such as Wi-Fi with licensed DSRC devices in the 5.9 GHz DSRC spectrum is under discussion. Two approaches have been proposed by the Wi-Fi industry, Detect & Vacate, and Re-channelization. While the former has been fairly analyzed and understood, the Re-channelization proposal requires fundamental changes to DSRC regulations and operations and needs more studies due to its complexity. In this work, we analyse the challenges of spectrum sharing in the 5.9GHz DSRC band by using the Re-channelization proposal and quantitatively evaluate its impact on DSRC performance.

Keywords:

DSRC, Re-channelization, spectrum sharing

I. Introduction

Dedicated Short Range Communications (DSRC) is an Intelligent Transportation System (ITS) technology which enables message exchange among road users to enhance their mutual awareness over several hundred meters. With increased mutual awareness, road safety and efficiency are expected to be largely improved. The U.S. National Highway Traffic Safety Administration (NHTSA) published in 2016 a Notice of Proposed Rule Making (NPRM) [1], which proposes to mandate equipping new light vehicles with DSRC in the U.S. after 2020.

On the other hand, driven by the growing daily communication demand, the Wi-Fi industry seeks access to additional spectrum. The DSRC band, allocated at 5.850-5.925GHz by the U.S. Federal Communications Commission (FCC) in 1999 [2], is arguably useful to Wi-Fi operations. Two methods, Detect & Vacate (D&V) and Re-channelization, proposed by Cisco and Qualcomm respectively, were proposed as candidate solutions to share the band[1]. While the former is straightforward and received a fair amount of studies, the latter, lacked important technical details, preventing the community from developing a full picture of its spectrum sharing performance. Recently, the Re-channelization proponents released updates to some of the missing technical details, creating the opportunity for a

---

[1] Per FCC, sharing of the band is between DSRC and any unlicensed technology, not limited to Wi-Fi.

more complete analysis. Hence, in this paper we study the Re-channelization proposal in realistic scenarios via ns-3 simulations and quantitatively evaluate its impacts on DSRC performance.

II. Background

A. Re-channelization proposal

As shown in Fig. 1, the U.S. DSRC band compromises seven 10 MHz channels between 5855MHz and 5925 MHz, plus a 5 MHz reserved band (5850-5855 MHz). The FCC designated each channel as either a Service Channel (SCH) or as the Control Channel (CCH). Based on these designations and characteristics of DSRC services, industry stakeholders standardised a channel usage plan in the Society of Automotive Engineers (SAE) J2945/0 document [3], which laid out a technical foundation for selection of appropriate channels for vast numbers of DSRC applications.

The Re-channelization proposal looks at reorganization of the DSRC band and channel usage plan. More specifically, it re-designates the seven channels, squeezing all safety-critical services that are currently spread out across all seven channels to the upper 30MHz of the band without acknowledging the possibility of severely elevated DSRC self-interference. In addition, the proposal aligns the lower 45MHz of the DSRC band with existing U-NII-3 Wi-Fi channels and requires DSRC to use two 20 MHz channels instead of four 10 MHz channels. The proponents of Re-channelization assert that by doing so, DSRC can achieve mutual detection with Wi-Fi (neglecting that mutual detection with non-Wi-Fi U-NII will not exist). In an FCC filing [4], Broadcom suggested several possible Wi-Fi channel access priority modes for testing, as shown in Table 1. Each gives Wi-Fi a certain priority relative to DSRC.

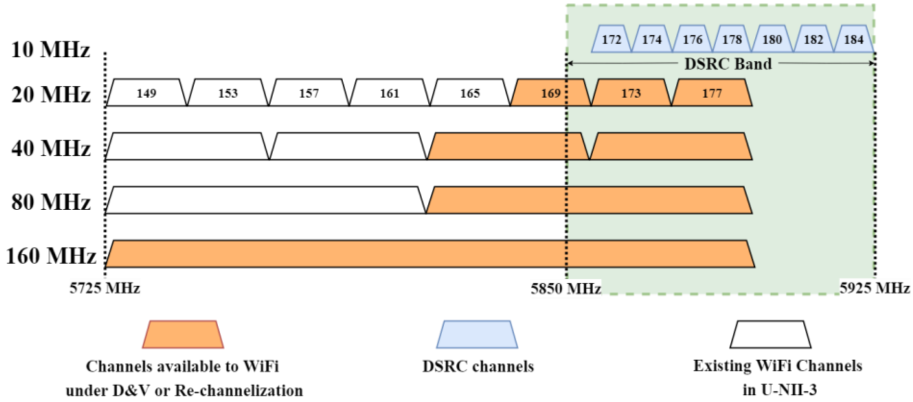

Figure 1 – An illustration of spectrum sharing in DSRC band

B. Wi-Fi carrier sensing

The basic channel access scheme used by the IEEE 802.11 ("Wi-Fi") systems is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), where each Wi-Fi device senses the channel before transmission. Two rules employed to declare the busy state of a channel are Carrier Sensing (CS) and Energy Detection (ED). The CS mechanism tries to match the preamble of a received signal with a known training signal sequence. It is designed primarily to avoid interference among Wi-Fi devices. The ED mechanism monitors the wireless energy on the channel, regardless of the form of the signal. This mechanism is helpful in preventing interference with non-Wi-Fi devices. According to the IEEE 802.11 standard, the minimum ED detection threshold is 20 dB higher than the minimum CS detection level [5].

Table 1 – Enhanced Distributed Channel Access (EDCA) parameters for Re-channelization proposal

Mode	CW_{min}	CW_{max}	AIFSN	TXOP
Mode 1	15	1023	3	0
Mode 2	15	1023	6	0
Mode 3	31	1023	6	0
Mode 4	31	1023	8	0
Mode 5	31	1023	10	0

III. Simulation Configuration & Metric

We evaluate the impact of the Re-channelization proposal on the DSRC's performance via ns-3 network simulations. The main studied scenario is a four-leg intersection, as shown in Fig. 2. The motivation by using this scenario is two-fold: a) Wi-Fi exists within and/or near a building. Portable Wi-Fi devices may be used in vehicles. b) A pivotal set of safety critical scenarios addressed by DSRC, beyond the capability of other vehicle on-board sensors, is related to intersection where victims of a potential vehicle crash come from perpendicular streets. As a result, the simulation configuration in Fig. 2 represents a number of realistic scenarios where Wi-Fi and DSRC may encounter each other. Note that we may not use all the Wi-Fi devices in a particular simulation since we aim to uncover underlying technical characteristics for Re-channelization and a simpler Wi-Fi topology will facilitate this goal. Hence, further specification of usage of these Wi-Fi devices will be provided in corresponding sections to follow. A brief list of other simulation parameters is summarized in Table 2.

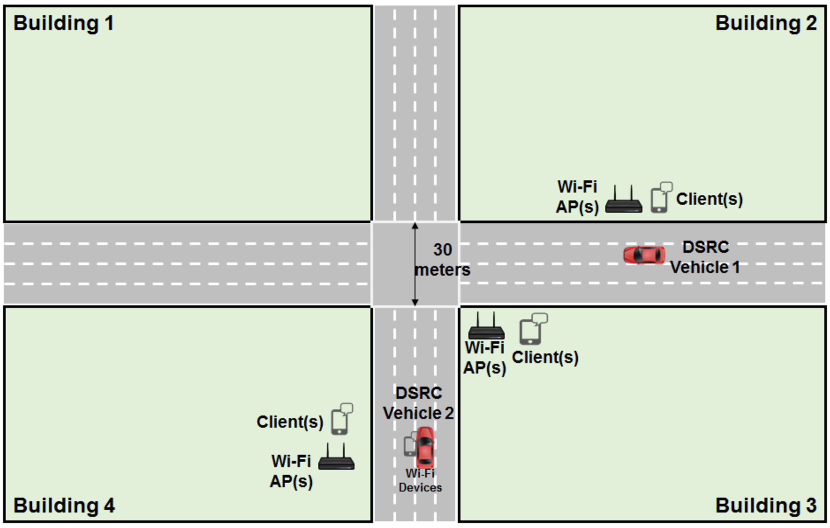

Figure 2 – The main simulation scenarios

In this work, the Packet Error Ratio (PER) is selected as the primary metric to evaluate the impact of the Wi-Fi operation on the DSRC performance. PER is defined for a transmission link as the ratio between the number of received packets at the intended receiver and the number of transmitted packets from the sender vehicle.

Table 2 Simulation Configurations

Configuration items	Values
Network simulator	ns-3.26
DSRC transmit power	20 dBm
Wi-Fi transmit power	20 dBm
DSRC transmit rate	10 Hz
DSRC EDCA parameters	AIFSN=6, CW_{min}=15, CW_{max}=1023
Wi-Fi transmit rate	Generated by Wi-Fi AP and a packet always available to transmit (saturation mode)
Wi-Fi traffic type	UDP or TCP according to specific requirement in different simulations
DSRC to/from DSRC propagation model	VirtualSource11p [6]
Wi-Fi to/from DSRC propagation model	IEEE P802.11 TGn [7] with 15 dBm signal attenuation per wall

IV. Cross-channel Interference from Wi-Fi to DSRC

Under Re-channelization, safety-critical DSRC services would move to channel 180, 182 and 184. There are many concerns over this migration idea which by analysis will cause significant impact to DSRC safety communications [8]. The simulation in this section evaluates one of the concerns, which is the impact of cross-channel interference from Wi-Fi in the shared band on the quality of DSRC safety critical services replaced to channels 180, 182 and 184. The goal is to assess the magnitude of DSRC packet loss due to leaked energy from Wi-Fi transmissions in the shared band.

To set up the simulation, based on what is described in Section III we keep the Wi-Fi devices in vehicle 2 active and turn down the others in the scenario. The rationale behind such a configuration is that the cross-channel interference for vehicle 2 would be dominated by the transmissions of Wi-Fi devices in the vehicle since they are much closer to the DSRC radio. If negligible impact on DSRC performance is observed in this case, there should be a less of concern about Wi-Fi operations in the building. In this simulation, Wi-Fi exchanges data on channel 177 over a 20MHz channel width and DSRC uses channel 180 to send Basic Safety Messages per SAE J2945/1. Evaluation results for other Wi-Fi-DSRC channel choices are not included in the paper due to the space limitation.

We configure the mobility trace of vehicles to mimic one potentially leading to a T-bone accident. More specifically, the two vehicles move towards the intersection center from the same distance on their respective streets with identical speed. They will meet at the intersection as if they were going to collide. Furthermore, we assume that vehicle 1 is the violator of traffic rules, e.g. by running a stop sign or ignoring a traffic light turning from yellow to red. We hope to see that vehicles 2, via BSMs of vehicle 1, can predict the potential of a vehicle crash.

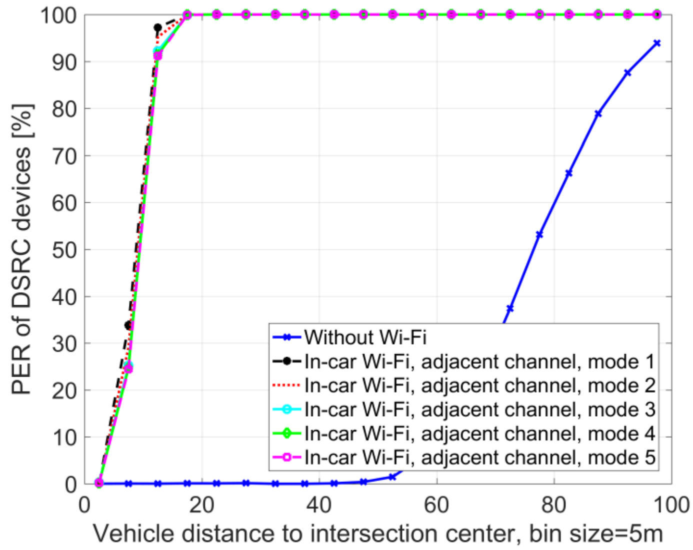

Figure 3 - PER for vehicle 1's BSMs sent to vehicle 2, with/without Wi-Fi present on adjacent channels

Fig. 3 shows the packet reception performance for vehicle 1's BSMs at vehicle 2, with and without Wi-Fi operations. It is starkly clear that Wi-Fi usage causes devastating impact to DSRC performance. In particular, all BSMs from vehicle 1 are lost before the two vehicles proceed to around 15 meters away from the intersection center when Wi-Fi is enabled. Considering that the width of the intersection is 30 meters, this means that vehicle 2 is not aware of vehicle 1 until they become Line-Of-Sight (LOS), too late for vehicle 2 to take appropriate actions to avoid a collision. In contrast, without Wi-Fi there are plenty of chances for vehicle 2 to receive vehicle 1's BSMs that will facilitate vehicle 2 to infer the likelihood of a vehicular collision and plan accordingly.

The harmful impact as reflected in Fig. 3 is particularly concerning. It proves that one fundamental assumption of the Re-channelization proposal, i.e., DSRC safety critical service would have a better communication environment after the migration to channel 180 and above, is not always true. Meanwhile, Fig. 3 suggests that the cross-channel interference significantly discounts the core value of DSRC for road safety, which is to expand drivers' awareness of the traffic situation from LOS to None Line-of-Sight (NLOS). It is shown that the NLOS communication performance of DSRC has largely degraded due to Wi-Fi sharing the adjacent channels.

One additional thing to note in Fig. 3 is that the impact on BSM communication performance by different EDCA options, suggested in Table 1, is very similar. This should be straightforward to understand since these EDCA modes intend to prioritize DSRC channel access in the shared band and have no consideration of cross-channel interference. In the following section, we will evaluate their impact on the performance of DSRC transmissions carried out in the shared band.

V. Co-channel interference from Wi-Fi to DSRC

Another key point of the Re-channelization proposal is that it can enable mutual detection (through CS and ED as explained in Section II.B) between Wi-Fi and DSRC. The supporters of the proposal assert that this mutual detection will facilitate protection of DSRC traffic from harmful interference in the shared band. However, it needs to be recognized that this mutual detection assumption violates the spirit of technology neutrality. Any non-Wi-Fi U-NII technology (e.g, Long Term Evolution-Advanced) will not sense the presence of DSRC on the shared band like the CS mechanism enables for Wi-Fi devices. However, even in the context where Wi-Fi is the sole unlicensed technology in the shared band, we need to evaluate the level of protection the Re-channelization proposal provides for DSRC traffic.

A. Hidden terminal

It is a well-known fact that hidden terminals degrade the performance of a communication system. The hidden terminal problem, in one of its simplest forms, reflects a communication topology where two transmitter nodes without knowing the existence of the other are transmitting to the same receiving node. This is called mutual hidden in the paper. A packet reception may fail if two transmitter nodes have their transmissions overlapped.

The hidden terminal problem is commonly observed in daily communication scenarios. In fact, the Wi-Fi community invented Request-to-Send and Clear-to-Send messages to mitigate the impact of the hidden terminal problem. However, these messages are not suitable for broadcast services. In addition, they may not be used even for unicast links because in Wireless Local Area Networks (WLAN), a receiver device may be much closer to its desired transmitter than to the hidden interfering nodes. In that case where a packet reception involves interference from the hidden nodes, the desired signal may be strong enough to overcome the interference, leading to a success packet reception.

Within the context of the Re-channelization proposal, Wi-Fi devices could well play as hidden terminals to DSRC transmissions due to signal attenuation caused by concrete walls and/or obstructing metal car body. To understand the impact of these hidden Wi-Fi devices on the performance of DSRC broadcasting services, we configure, in Fig. 2, a pair of Wi-Fi devices in Building 4 to be mutually hidden to the DSRC transmitter in vehicle 1. The other Wi-Fi devices are turned off in this evaluation.

Fig. 4 shows the PER of vehicle 1’s packets at vehicle 2 (Both vehicles are stationary during the evaluation). Independent of the EDCA mode in Table 1, all of vehicle 1’s transmissions failed. The reason is two-fold: a) Lack of mutual detection between the two technologies in this case makes the Wi-Fi interference always present at vehicle 2 (as listed in Table 2, Wi-Fi operates in saturation mode) when vehicle 1’s transmissions occurs. b) Vehicle 2 is closer to Wi-Fi interferer than to vehicle 1. In a packet collision, the strength of a DSRC packet cannot overcome the stronger Wi-Fi interference.

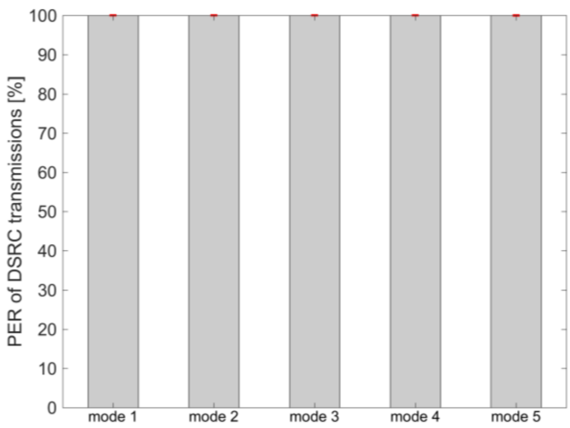

Figure 4 – PER of vehicle 1's transmissions due to hidden terminal problem

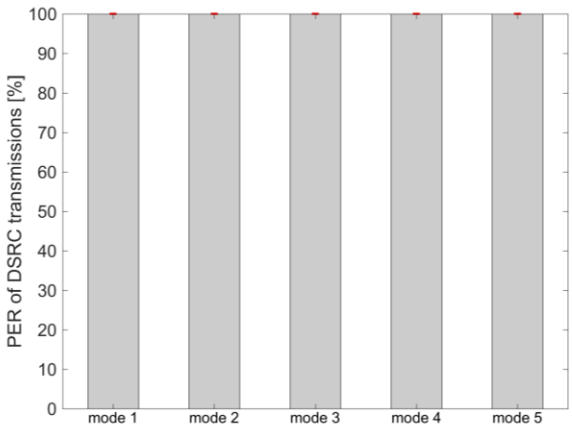

Figure 5 – PER of vehicle 1's transmissions due to unilateral hidden terminal problem

Unfortunately, this second aspect of the reason is commonly seen for vehicular communications. More specifically, a sender vehicle and its receiver vehicles are often spread out across a space much wider than that for a WLAN where communicating nodes are constrained to a few meters. This topology difference leads receiver vehicles more likely (than Wi-Fi users in a WLAN) to observe hidden interfering source (e.g., Wi-Fi devices transmitting on the shared band) at a distance much closer than that to the desired transmitter. As an effort to illustrate the region in which hidden Wi-Fi devices may exist, we moved around the Wi-Fi devices in Fig. 2 to evaluate where signal strength of packets from vehicle 1 falls under the CS threshold of Wi-Fi, and vice versa. The results are plotted in Fig. 6. Note that to not overcomplicate the evaluation, we turned off the fading component in our channel models.

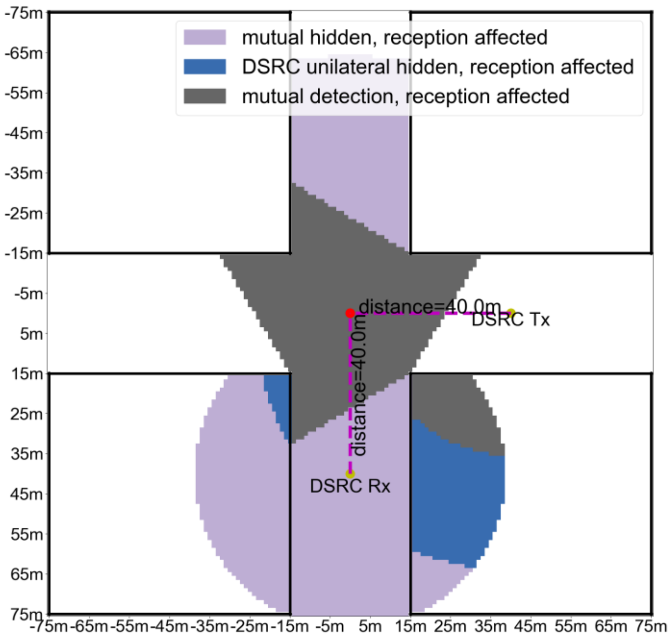

Figure 6 - Potential impact regions on the DSRC performance with Wi-Fi device at various locations

Fig. 6 plots several different zones, describing the mutual detection relationship between Wi-Fi devices and vehicle 1 when the former appear at different locations in the scenario. The first type of zone is called mutual hidden zone. It represents the set of locations at which appeared Wi-Fi devices are mutually hidden to the DSRC device in vehicle 1. Note that this zone only includes places from which Wi-Fi signal is strong enough to fail vehicle 1's packet reception at vehicle 2 during a packet collision. Other mutual hidden places are painted white since they are less interesting to the discussion. As we can see, the mutual hidden zone occupies a sizable portion of the scenario in Fig. 2, including places inside and outside the buildings. Wi-Fi devices present in this zone cause significant DSRC packet loss as shown in Fig. 4.

As we test different locations, we observe another set of places at which appeared Wi-Fi devices could not sense the transmission of vehicle 1 but the reverse is false. In other words, vehicle 1 could sense Wi-Fi activities. This happens because the CS mechanisms of the two technologies use different thresholds, -92dBm for DSRC and -82dBm for Wi-Fi. Such a mismatching provides a unique relationship among the two technologies which we call unilateral hidden terminal. From vehicle 2's perspective, this means that when Wi-Fi transmissions are on the air, vehicle 1 could sense them and defer its transmission according to CSMA. However, when vehicle 1 starts a transmission, the Wi-Fi devices will not sense that and therefore could potentially cause interference. In Fig. 6, we marked out a region where the unilateral hidden terminal exits as "DSRC unilateral hidden". Again, this region only includes places from which Wi-Fi transmission's signal is strong to fail a DSRC packet reception at vehicle 2 during a packet collision.

To understand the scale of impact of unilateral hidden terminal on DSRC performance, we leverage a pair of Wi-Fi devices in Building 3 in Fig. 2. We place them at a place in the building where they form a unilateral hidden terminal relationship with vehicle 1, and we turn off the other Wi-Fi devices in the scenario. Note that channel fading is re-adopted in the evaluation and both vehicles are stationary. The performance results are shown in Fig. 5. One can observe that unilateral hidden terminal leads to 100% PER for vehicle 1's transmissions, independent of the EDCA modes used, as in the case of mutual hidden terminal. The reason is that although vehicle 1 can adjust its transmission timing based on CSMA and Wi-Fi activities, Wi-Fi devices may continue usage of the channel since they are not aware of the presence of the DSRC device in vehicle 1.

The third type of zone in Fig. 6 is called mutual detection zone which means Wi-Fi devices, if present in the zone, could form a mutual detection with vehicle 1. This zone, as compared to others, is closer to the location of vehicle 1. We will evaluate in the next subsection if and how much of DSRC communication would be impacted.

B. Impact of mutual detection on DSRC communications

In this subsection, we will show that even the assumption of mutual detection between DSRC and Wi-Fi is able to achieve, the impact of Wi-Fi traffic on DSRC transmissions is not negligible. In the IEEE 802.11 based on MAC protocols, one key component to avoid packet collision is to let stations wait for a period of time before they can start a transmission. The length of the waiting time is randomly selected based on the EDCA parameter, Contention Window (CW). However, it is possible that different stations choose the same length of the waiting time. As a result, two stations start the transmissions at the same time, leading to a packet collision. We call this problem as countdown collision which may apply to coexistence of Wi-Fi and DSRC . For example, a Wi-Fi transmitter and a DSRC transmitter choose the same length of the waiting time after a channel busy period. The packet collision between DSRC and Wi-Fi may result in a packet loss at the DSRC receiver. Note that the probability of the packet collision increases with the Wi-Fi traffic load. Therefore, with the saturated Wi-Fi traffic, it is possible to create the near-worst case of the DSRC packet losses.

Our simulation employs some of the Wi-Fi devices in Building 3 to generate Wi-Fi traffic in the scenario. The devices (one Access Point (AP) and one user) are placed at a location inside the building where they can detect vehicle 1, and vice versa. Evaluation results are shown in Fig. 7. One can observe that as the less aggressive mode is applied (from mode 1 to mode 5, the level of aggressiveness of Wi-Fi channel access decreases), the impact of Wi-Fi traffic on DSRC transmissions is decreased. In addition, it can be noticed that the PER of DSRC transmissions is dramatically increased as the Wi-Fi devices switch from UDP traffic to TCP traffic. The main reason is that according to the TCP protocol, the transmitted data packets by the Wi-Fi AP will be acknowledged by the Wi-Fi client. These TCP ACK packets, as compared to UDP traffic, will compete for the channel access with DSRC and generate additional backoff countdown collisions with DSRC packets, leading to more packet losses.

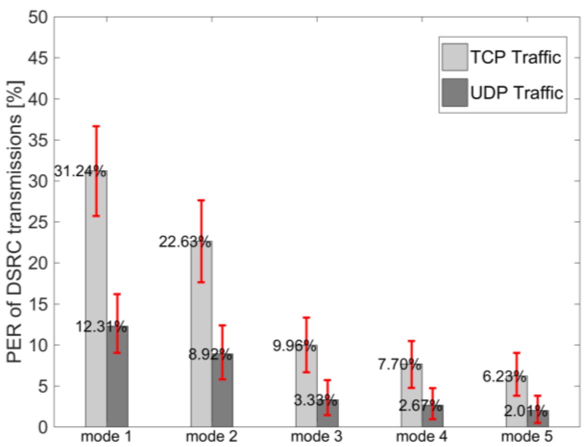

Figure 7 - Packet loss of DSRC transmissions due to backoff countdown collisions between DSRC and Wi-Fi, *TCP and UDP traffic*

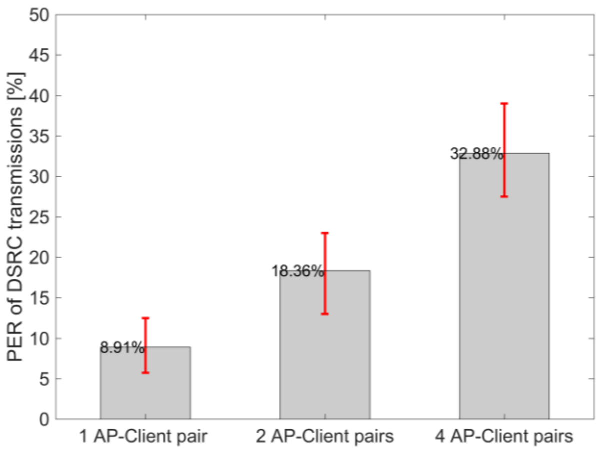

Figure 8 - Packet loss of DSRC transmissions due to backoff countdown collisions between DSRC and Wi-Fi for the Re-channelization mode 2 with different numbers of AP-Client pairs, *UDP traffic*

We also evaluated the impact of different number of Wi-Fi users on DSRC's performance, as shown in Fig. 8. More specifically, we increased the number of Wi-Fi devices in Building 3 from one pair of AP and user to 4 pairs and adopted mode 2 in Table 1 as Wi-Fi's EDCA parameters. One can observe that as the number of AP-Client pairs increases, more and more DSRC packets are lost due to the packet collision. These packet losses as well as those in Fig. 7 show Wi-Fi cause harmful inference to DSRC operations even in contexts where mutual detection is achieved for both technologies.

VI. Conclusion

In this work, we studied the Re-channelization spectrum sharing proposal that aims to support the operation of unlicensed Wi-Fi devices in DSRC's licensed band by overhauling current DSRC channelization. We showed that Wi-Fi transmissions, if sharing DSRC band, could harmfully impact safety-critical DSRC transmissions in channels 180, 182, and 184, due to cross-chanenl intference. This study proves false the claims of Re-channelization proponents that those three channels will be interference-free from Wi-Fi operations. The second question we investigated is if the mutual detection between DSRC and Wi-Fi claimed by Re-channelization proponents protects DSRC from harmful interference. Our study shows that in many scenarios DSRC and Wi-Fi devices will suffer from mutual and unilateral hidden terminal problems, which means that the claimed benefits of mutual detection will not generally be realized. Furthermore, even in an ideal scenario where no hidden terminals are present, backoff countdown collisions that are inherent to the IEEE 802.11 MAC protocol can still lead to a noticeable amount of packet collisions between DSRC and Wi-Fi. We also note that TCP Wi-Fi traffic creates more interference than UDP Wi-Fi traffic.

References

1. National Highway Traffic Safety Administration. Notice of Proposed Rulemaking, CFR 49 CFR 571, Docket No. NHTSA-2016-0126.
2. Federal Communication Commission (2003), *FCC 03-324 Report and Order*.
3. SAE International, Dedicated Short Range Communication (DSRC) System Engineering Process, *Guidance for J2945/x Documents and Common Design Concepts*, Dec. 2017.
4. FCC docket 13-49, Broadcom ex parte of April 6, 2017
5. IEEE (2016). *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*, IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012), pp. 1-3534
6. T. Mangel, F. Schweizer, T. Kosch, and H. Hartenstein, *Vehicular safety communication at intersections: Buildings, non-line-of-sight and representative scenarios*, in 2011 International Conference on Wireless On-Demand Network Systems and Services, Jan 2011, pp. 35–41.
7. IEEE (2014). *IEEE P802.11 Wireless LANs TGn Channel Models*, Technique Report
8. J. Kenney, H. Lu and B. Cheng, *Technical challenges of sharing DSRC band at 5.9GHz in US*, ITS WC 2017, Montreal