Adjacent Channel WiFi 5 Interference on DSRC Communication at 5.9GHz

Jacob A. Bills
Kahlert School of Computing
University of Utah
Salt Lake City, Utah, USA
jacob.bills@utah.edu

Alex Orange
Kahlert School of Computing
University of Utah
Salt Lake City, Utah, USA
alex.orange@utah.edu

Jacobus Van der Merwe
Kahlert School of Computing
University of Utah
Salt Lake City, Utah, USA
kobus@cs.utah.edu

***Abstract*—Since their controversial decision to adjust the spectrum allocation for intelligent transportation systems in November 2020, the FCC has implemented a wide range of changes. These changes include the removal of 45 MHz from existing spectrum allocations and the transition from DSRC to C-V2X, both of which need to be studied in greater detail. We aimed to explore the effects of these decisions by examining the potential impacts on commercial-grade V2X hardware in a real-world, complex radio environment. This was done by characterizing DSRC and comparing its performance in a complex radio environment with different types of interference present. The results of these experiments indicate that outdoor adjacent band WiFi networks can impact DSRC operations; however, this impact is unlikely to have a measurable effect on current ITS installations.**

***Index Terms*—DSRC, WiFi 5, 802.11ac, adjacent channel interference, ITS, V2X**

I. Introduction

As cars advance in sensing and computing systems, the need for a dedicated communication standard continues to grow due to the unique conditions vehicles face. To respond to this need, in 1999, the Federal Communications Commission (FCC) allocated 75 MHz of bandwidth for Intelligent Transportation Systems (ITS) from 5.85 MHz to 5.925 MHz [1]. This spectrum was dedicated to and intended to be used by ITS to enhance the operational safety of roadways in the United States. In addition to reserving this ITS band, these FCC rules designated this spectrum to Direct Short-Range Communication (DSRC), a WLAN-based V2X solution, making it the preferred ITS communication standard. They also created seven 10 MHz channels to be used by the technology within the band. This early reservation was intended to create an environment that would foster research and innovation within the industry with the goal of widespread adoption of ITS.

V2X describes a family of communication standards. Within that family, there are two dominant technologies in use across the United States: DSRC and Cellular-V2X (C-V2X). These standards control physical links and access layers, defining how messages are composed as well as how and when they are transmitted by the radios. They ensure operational consistency and interoperability across vendors and networks and are similar to existing WiFi and LTE standards. Between these two V2X technologies, the US Department of Transportation has 143 active and pending V2X projects across the country [2]. These implementations serve various purposes in multiple areas, such as a Utah Department of Transportation (UDOT) project using V2X communications to provide preemption for Utah Transit Authority busses at intersections to increase the number of timely arrivals. The protection of this use case provided part of the motivation for this work.

This work was supported by the National Science Foundation under Grant Number 1827940.

In the twenty years since the ITS spectrum reservation, there has been limited investment in V2X communication. A 2019 report from the Congressional research service found that across the United States, only 52 DSRC implementations are in operation [3]. This lack of widespread adoption prompted the FCC to issue a rule change in 2020 [4], which reallocated the lower 45 MHz of the previously allocated band to unlicensed WiFi transmissions. The motivation for this 45 MHz reallocation was to produce an additional 160 MHz block of dedicated spectrum for WiFi when combined with existing 5 GHz allocations. This enables higher throughput when used with the 160 MHz bandwidth channels provided through WiFi 6. This rule change also officially started the transition of the remaining 30 MHz of the band to C-V2X, a cellular solution from 3GPP. This transition to C-V2X is motivated by industry investment and support for the technology. The FCC also indicated in the rule change that they expect C-V2X to provide more robust connectivity for ITS than DSRC.

In this paper, we aim to quantify the impact of the 2020 FCC rule change on the quality of communication achievable using DSRC with WiFi in the adjacent band. This required a way to reliably and consistently produce interference in the adjacent band. However, due to the recent nature of this rule change, only a limited number of commercially available WiFi equipment could operate in the newly opened channels. To address this problem, an interference generation system was developed for these experiments that use Software-Defined Radios (SDRs) to capture active WiFi communications and transpose them into the new bands. This allowed for the same interference to be introduced to a DSRC link across numerous tests, along with fine-grain control of the interference signal's center frequency and transmit power. Then through a series of ground truth measurements, the amount of power generated

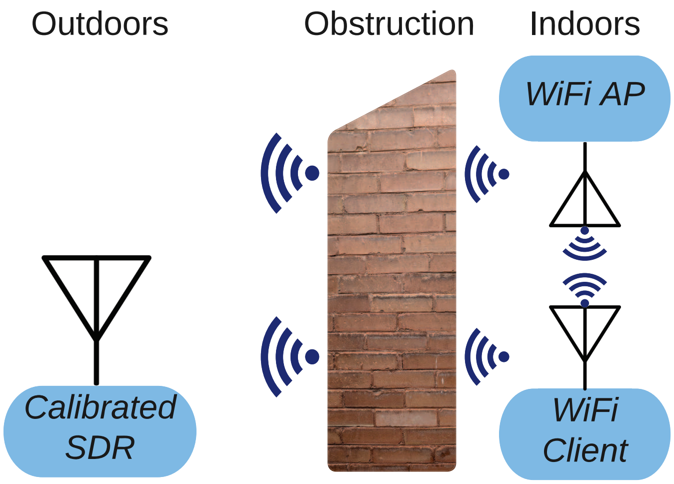

Fig. 1: Escaping WiFi Power Measurement Topography

by a WiFi network inside and outside a structure was characterized using the experimental setup outlined in Figure 1. Where a WiFi 5 network was configured and loaded with traffic within a structure and the power level of escaping WiFi was recorded; allowing for the assessment and comparison of current WiFi operations to our controlled interference. Using resources within the Powder Platform [5], our recordings were introduced to an active DSRC link in a complex Over the Air (OTA) radio environment at realistic power levels, representing a first-of-its-kind study on the technology.

After running numerous interference tests, it appeared that while there are signs of interference in worst-case scenarios, such as a WiFi transceiver operating outside of a structure nearby to an active DSRC channel, in most cases, adjacent band WiFi interference does not pose a significant threat to an ITS system using DSRC. This indicates that the 2020 FCC rule change does not greatly inhibit DSRC's ability to provide communication for ITS applications.

This work's contributions are summarized as:

- First of its kind DSRC reliability study that incorporates WiFi interference in the 5.9GHz band with commercially available equipment operating over the air in a realistic radio environment.
- Provides a set of ground truth measurements as to the expected power levels of WiFi interference in the roadway from a WiFi network setup within a household.

II. Related Works

Since the FCC proposed changes to ITS spectrum allocations, there have been a handful of academic studies into the effects of these modifications and ways of mitigating their impact on these technologies. Studies conducted by Cheng et al. [6], and Choi et al. [7] investigated the impacts of WiFi coexistence within the same band and the possibility of using detect and vacate techniques. While Cheng used computer simulations, Choi used production-level equipment on an attenuator matrix. These works differ from this work in that this work makes use of commercial equipment in an over-the-air environment. Both studies found that even with the detect and vacate tools, there was a noticeable impact on performance. However, Choi claimed that commercial implementations should remain operationally unaffected and perform essential functions, indicating that the performance impact is only pronounced in two scenarios: when the distance between the DSRC transmitter and receiver is greater than 300m or the distance between the WiFi Transmitter and DSRC receiver is less than 15m.

While the above papers explored the degrees of effectiveness in limiting the interference impact of coexisting WiFi operating in the same band using detect and vacate (D&C) techniques, Khan et al. [8] examined these protocols in more depth in an attempt to identify their weaknesses and possible improvements. Through computer simulations, unlike our study's use of production hardware, Khan found that even though detect and vacate tools are relatively effective at improving performance in ideal conditions, they often fail to recognize a busy channel when presented with weaker relative DSRC transmissions. This means that in the cases where it would be most critical to avoid a collision, the WiFi transceiver often failed to vacate the channel properly and would transmit over the DSRC signal. Khan et al. theorizes the discrepancy in channel bandwidths between WiFi and DSRC likely causes the effect. While DSRC operates in 10 MHz channels, modern WiFi operates in much wider channels ranging from 20 MHz to 160 MHz in width.

The research performed by Mavromatis et al. [9] is the only related work that involves over-the-air testing. This study examined real-world unlicensed transmissions on DSRC. By operating commercial DSRC equipment on existing 2.4 GHz and 5 GHz WiFi channels, they compared the performance to that captured on Europe's dedicated DSRC band. Their findings showed no significant performance penalty when DSRC was operated on the 2.4 GHz band. However, in the 5GHz implementation, the DSRC connection showed some performance degradation, consistent with the earlier findings in WiFi DSRC coexistence. This study differs in that it introduces the interference to the 5.9GHz band, where a production DSRC network would operate.

III. Interference Testing Methods

With the change in spectrum allocation only occurring in 2020, few commonly available WiFi equipment operate adjacent to the ITS space. To this end, several calibrated systems were developed throughout this work to allow for a USRP B210 SDR [10] running with GNU Radio [11] based software to generate signals that share similar properties as WiFi within these bands. This was necessary as these new WiFi bands have yet to gain broad hardware support. This system allows us to conduct and evaluate the impact of these future devices before they are widely adopted and reasonably determine their potential impact.

A. Interference Generation

This investigation into possible interference on the ITS band requires a realistic WiFi-based interference source in the adjacent band. Thus, to provide an accurate understanding of DSRC's behavior in the presence of WiFi interference, a system was developed that captured an active WiFi signal in the 2.4GHz WiFi band commonly supported by modern WiFi equipment. These captured signals were then replayed to replicate the interfering effect of a WiFi network. This was done by transposing this capture to the ITS band and its adjacent channels.

A WiFi 5 network was configured to generate these captures with a COTS AP, a client, and a USRP B210 SDR [10] were placed inside a room, each approximately 2 meters apart. In this layout, the client was able to connect to the AP and the SDR was able to monitor their connection on an otherwise empty WiFi channel(channel 5). Then the WiFi link was saturated using iPerf [12], ensuring it remained active. This allowed an SDR and GNU radio to record this active link at its native frequency. Next, by performing a spectral mask analysis of both an active WiFi link and our replayed WiFi signal, it was determined that the recording represents a reasonable approximation of WiFi, that can be transposed to the newly opened WiFi bands presenting the potential to interfere with ITS operations.

While the creation of this interference generation technique came out of necessity from hardware limitations at the time, it has several advantageous features due to the kind of interference testing done for this work. By replaying the captures using a single SDR, the testing setup's complexity was greatly reduced as it replaced an entire interfering network. Through a recording, the interference signal will produce an identical interference pattern for every run, thus ensuring repeatability and accurate comparisons between different experimental settings, further reducing the number of variables in the interfering signal. This left only an interfering signal's center frequency and transmit power, which can be precisely controlled across test runs.

One potential issue facing this setup is that the recorded signal will not exhibit the same collision avoidance behavior produced by CSMA systems used in WiFi networks. However, since CSMA does not check the adjacent band before transmitting, it would not stop a WiFi transmission from failing to prevent any generation of adjacent band interference. Even in the same band, which is illegal under this rule change, simulation studies conducted by Lansford et al. also indicated that differences in channel width between the technologies prevent CSMA from properly protecting DSRC from WiFi collisions in most cases [13], further indicating that CSMA support was not necessary.

B. Power Measurements

Using the systems ability to transmit WiFi-like signals at frequencies of concern for ITS operations, this experimental setup needed to represent WiFi power levels at the roadway accurately. For this to realistically represent what a DSRC link

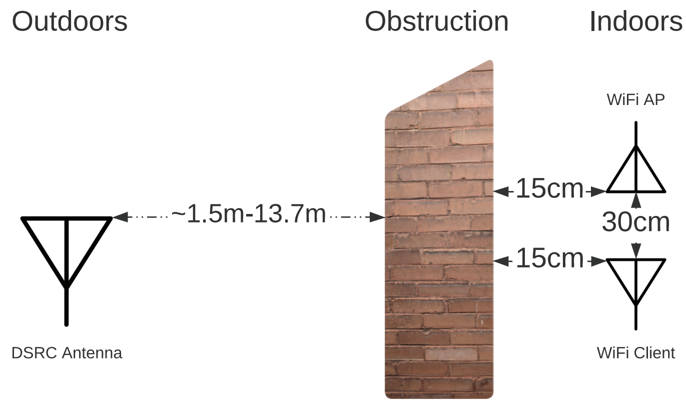

Fig. 2: Escaping WiFi Power Measurement Dimensions

could experience, several ground-truth measurements were taken, allowing any results to be accurately compared to real-world situations. The same B210 SDR ran another GNU Radio script in this set of experiments to collect the average power level across a configurable 20MHz WiFi band. Together with our calibration results, these measurements gave a series of power levels from residential WiFi equipment.

To achieve our goal of determining the impact a residential WiFi network will have on a nearby roadway, a series of measurements were collected. Four measurement sites were selected at three residences constructed from various materials, outlined in table I, were selected as measurement sites. At each site, a WiFi network was configured at channel 165, the highest frequency channel supported by our equipment. The AP and client were co-located along the interior of an exterior wall, as shown in Figure 1. Additionally the AP was configured to performance mode, where it continuously broadcasts using its maximum gain setting, preventing any power scaling from occurring based on the proximity of the connected devices. Then iPerf was used to saturate the connection before power measurements on the channel were collected at distances between approximately 1.5 and 13.7 meters from the exterior wall, covering a range typical of North American building setbacks [14], with the WiFi client and AP being placed 30 centimeters apart and 15 centimeters from the exterior wall as shown in Figure 2. All exterior walls selected also had a window within 61 centimeters of the AP that varied in size at each location listed in Table I, and the measurements were repeated with the window closed, open with a screen(if present), and open without a screen; the test was also conducted with a large sliding glass door. Additionally, a test was conducted without a building acting as an obstruction, representing a worst-case scenario, even though direct outdoor operation is prohibited under the 2020 rule change.

The results of these power measurement tests are illustrated in Figure 3. In this figure the results from each of the different obstruction materials has been averaged as they exhibited extremely similar characteristics, except for the location that included a sliding glass door which exhibited WiFi signal

TABLE I: Obstruction Materials with Window Dimensions

Obstruction Material	Window Width (cm)	Window Height (cm)
Metal(Steel) Siding	61.0	101.6
Brick	81.3	101.6
Vinyl Siding	111.8	111.8
Glass Door	182.9	203.2

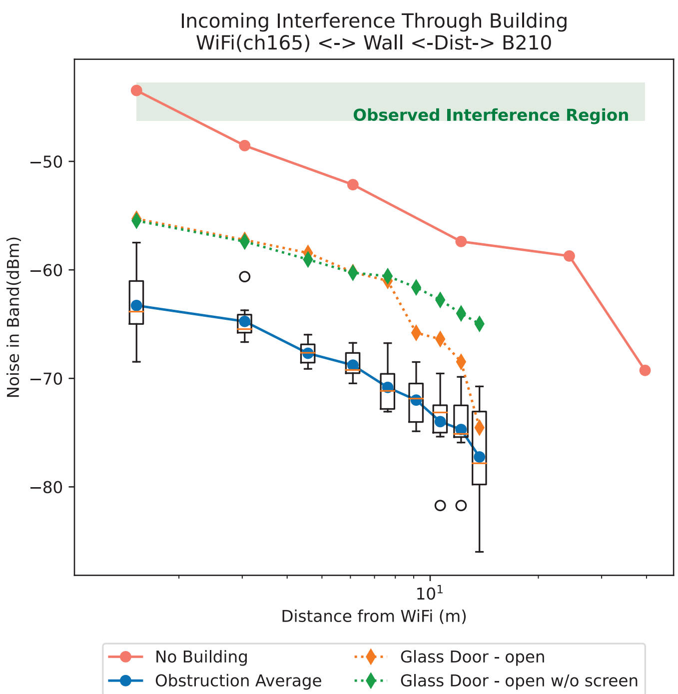

Fig. 3: Escaping WiFi Power. Observed interference region corresponds to green box shown in Figure 6

leakages between 10 and 15 dB above the average case when the glass door was open at all distances. However, even in the worst-case scenario: where there is an open glass door, the free-space measurements collected without an obstruction are only around 10 dB greater than any of those with an obstruction. This indicates that even with a large opening—like in the case of an open sliding glass door—having the network within a structure greatly decreases the power leakage from an active WiFi network. With these results, a realistic frame of reference for our interference testing was created. These results allowed us to target our interference generation system and determine the expected impact of various residential networks on a DSRC network.

C. Calibration

Calibration data was collected to allow for consistent and accurate comparison across all stages of this experiment, allowing for earlier dB results to be grounded and compared in dBm. This calibration data for the TX and RX ports used in the interference generation and power measurements, respectively, were collected.

For the output calibration, the RF A TX/RX port of our B210 SDR was attached to a Keysight N1913A power meter [15] paired with a Keysight N8482A power sensor [16]. Then using the interference generation GNU radio previously developed for this work, the TX gain was swept from 0 dB to 89 dB. The resulting power was then recorded from the power meter in dBm. This allowed a conversion factor between our interference generator's relative gain dB setting and the expected dBm power output. The expected power output in dBm can be calculated by adding an offset of -91dB to the TX gain. Additionally, given the RX output from the SDR is piped to the on-board unit (OBU) with a directional coupler as shown in figure4, a -40dB coupling factor will need to be added to any power.

To calibrate the inputs on our SDR, a similar procedure was followed. The RF A-RX2 port was attached to a signal generator configured to the same frequency as the channel 165(5825 MHz) WiFi signals that were being monitored in the power testing phase of this work. By determining the difference between the relative dBA (dB arbitrary) of the SDR to the absolute dBm input from the signal generator, an offset was determined and in this case was found to be -3.4.

Combining these two offsets makes it possible to directly calculate the expected power output from our interference generation system in dBm by adding -88dB from the configured TX_Gain. This allowed the interference generation system to be easily configured to match output power levels from the ground truth measurement series.

D. DSRC Testing

To start DSRC testing, the equipment was installed in a simple configuration to validate its functionality. In this layout, the road side unit (RSU) was pole mounted to the William Browning Building (WBB) rooftop co-located with existing POWDER infrastructure that allowed for remote access and control of the RSU. The OBU was set up outside the Warnock Engineering Building (WEB) and directly accessed via Ethernet. With this setup, it was discovered that many radio layer statistics and logs were locked behind accounts with elevated privileges that the equipment vendor was unwilling to provide for this work. In response to these limitations, the DSRC units had to be treated as "black boxes," a workaround was found by exploring UDOT's current deployment. This workaround allowed artificially generated traffic to be sent over the link in a controlled manner while providing results that would be particularly relevant to UDOT's current implementation. UDOT used a message forwarding function called immediate forward [17], which enabled pre-generated messages to be sent to a specific port on the RSU, which using the immediate forward function would send them to the OBU over a DSRC connection. The OBU then forwarded those messages to an open controller port. Considering this, a testing framework was developed to work with this traffic generation technique in a configuration that can be seen in Figure 4. In this framework, packets were sent to the RSU on the WBB rooftop using a UDP socket on the RSU side controller node(Dell r740) located within POWDER in the Merrill Engineering Building (MEB), which recorded how many and how often the messages were sent. Then using another UDP socket on the OBU side

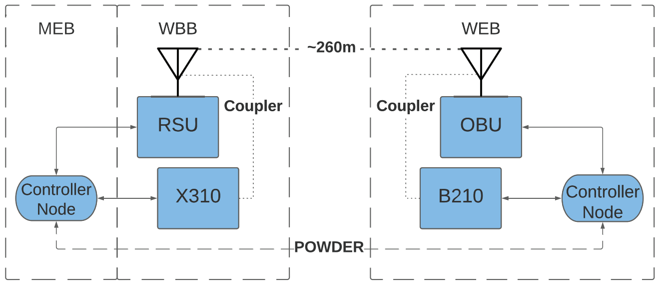

Fig. 4: Topology for DSRC Testing

controller node(Intel NUC) located at WEB with the OBU approximately 260 meters away from the RSU at WBB, the number of messages the OBU received and forwarded along with when they were received were recorded. This allowed the packet delivery ratio (PDR) to be determined for the link in a setup that could be precisely controlled and replicated.

The last step of the process was to construct a mechanism to control the interference generation system described previously, allowing us to programmatically inject the interference signal into the receiver on the OBU. To do this, GNU Radio [11] was installed on the OBU side controller and was used to generate interference that was introduced to the introduced to the antennas on the OBU via the attached USRP B210 SDR [10] and coupler, located at WEB as shown in Figure 4. A USRP X310 [18] was located on the WBB rooftop and used to monitor the RSU output power levels. Testing started using Gaussian noise to ensure that the setup allowed enough interference to jam the DSRC link effectively. This test confirmed that an input signal with a sufficient TX gain would be able to halt successful DSRC transmissions completely. We then used our interference generation system to introduce interference to the ITS band and its adjacent channels. We also conducted an in-depth analysis of our interference system in WiFi channel 165, the nearest channel to the ITS space, representing a worst-case legal scenario under the 2020 FCC rule change.

IV. Results

In the first set of DSRC tests, a broad spectrum area needed to be covered—a special emphasis was placed on the blue highlighted region in Figure 5. By moving the center frequency of the interference signal, different channel and interference configurations were imitated, as the channel settings were predetermined by the vendor. A series of tests were then run, sweeping the interference center frequency from 5.8 GHz to 5.9 GHz, covering the current ITS spectrum and several adjacent bands. This sweep test was done using 1 MHz increments at ten different TX gain settings between 51 and 60 dB. The results of this test can be seen in Figure 5, where the TX center frequency is shown along the X-axis, and the resulting packet delivery ratio is shown along the Y-axis.

As shown in Figure 5, interfering signals in the bands directly adjacent to the operating DSRC channel do not sub-

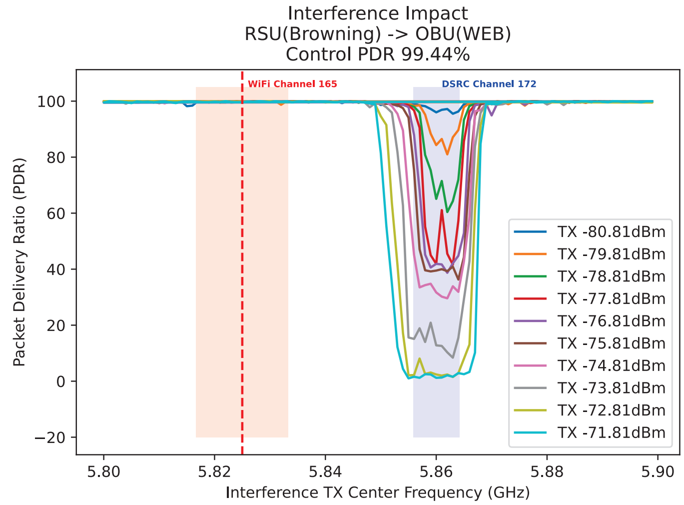

Fig. 5: Band Sweep Results. Red WiFi Channel 165 line corresponds to solid red line in Figure 6

stantially impact DSRC robustness until the TX gain reaches -75.81dBm. This is in contrast to interference operating in the same band, which has a noticeable impact at all but the lowest tested levels of interference. Of particular interest in Figure 5, is the region highlighted in red as it represents the closest WiFi band in which a legally operating WiFi network could actively transmit. Given the importance of this specific channel configuration scenario, additional tests were done highlighting the impact of interference in this region. In this test with a fixed frequency channel, granulated measurements were collected every quarter dB of interference for transmit power settings from 0 dB to 89 dB, the full range available on a B210 SDR [10]. The results of this more targeted test can be seen in Figure 6, where the TX gain is shown along the X-axis, and the PDR is along the Y-axis. Looking at Figure 6, it can be observed that the PDR does not deviate greatly from the control until about -46 dBm. However, after -46 dBm, it began to drop quickly to a PDR of 80; this region of observed interference is highlighted in green in Figure 6. These results indicate that even in the worst-case legally allowed scenario, DSRC would only see approximately 20% performance reduction. Together, the band sweep and single band test findings demonstrate that DSRC remains reasonably robust with interference in the adjacent bands.

Superimposed on the single band sweep results in Figure 6 is a subset of data points from Figure 3. Each of these measurements is a different scenario where the data was collected 1.5 meters from the structure's exterior, along with the 1.5 meter free space results. Only the free space results fall within the observed interference region. All scenarios in which the WiFi network was within a structure failed to push the power level into the region with observed interference. This is shown in green on both Figure 3 and Figure 6. These findings support that the indoor operation requirement from the 2020 FCC rule change is sufficient to prevent WiFi adjacent-band interference from impacting DSRC operations.

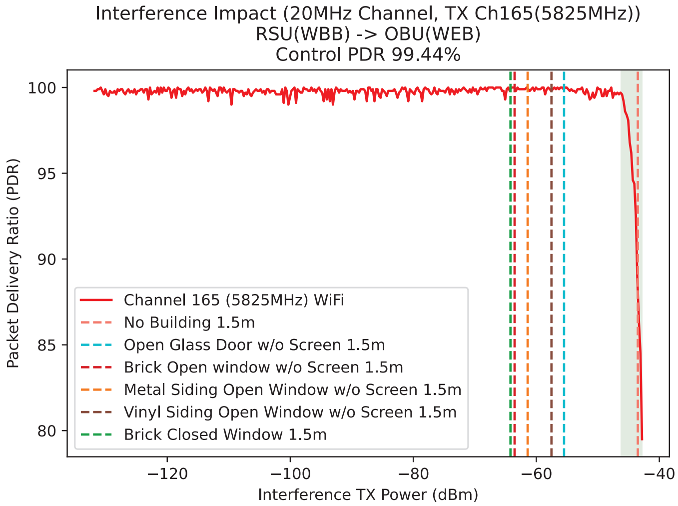

Fig. 6: Single Band Results. Dashed lines correspond to WiFi power leakage values from Figure 3

V. Conclusion

The controversial nature of the FCC's decision to modify large portions of the ITS spectrum has intensified the need for academic research into its impacts. Understanding what impacts this change has on the ability of V2X platforms is paramount. After establishing a way to constantly produce interference in a controlled manner and running it in a realistic over-the-air environment, these experiments began to characterize the exact impacts of unlicensed transmission on potentially lifesaving ITS applications. This knowledge and data will inform policymakers of weaknesses in the existing spectrum allocations or placate early V2X adopters by quantifying the impact on their operations.

In the DSRC testing phase, it was observed that there is a potential for WiFi interference when broadcast outside a structure near a DSRC receiver. However, WiFi is not likely to pose a threat to current implementations. This means that for the FCC to ensure the continued efficacy of V2X communications in the ITS band relying on DSRC radio technology, some level of monitoring will be needed to ensure that current and future installations remain unaffected. In addition, the FCC should ensure that commercially available radio equipment capable of operating in bands adjacent to ITS should not be ruggedized to dissuade end users from configuring outdoor networks. Conducting regular compliance checks along critical sections of ITS-enabled roadways for other sources of interference, like misconfigured or malicious equipment operating in the newly unlicensed bands, will be crucial.

Acknowledgment

We acknowledge the support of Blaine Leonard and his colleagues at the Utah Department of Transportation, who made this work possible. Further, this material is based upon work supported by the National Science Foundation under Grant Number 1827940.

References

[1] Federal Communications Commission (FCC), "FCC Allocates Spectrum in 5.9GHz Range for Intelligent Transportation System Uses," October 1999.
[2] United States Department of Transportation (USDOT), "Operational Connected Vehicle Deployments in the U.S." https://www.transportation.gov/research-and-technology/operational-connected-vehicle-deployments-us, July 2020.
[3] Congressional Research Service (CRS), "Smart Cars and Trucks: Spectrum Use for Vehicle Safety," https://crsreports.congress.gov/product/pdf/IF/IF11260, December 2019.
[4] Federal Communications Commission (FCC), "FCC Modernizes 5.9 GHz Band to Improve Wi-Fi and Automotive Safety," https://docs.fcc.gov/public/attachments/DOC-368228A1.pdf, November 2020.
[5] Flux Research Group, "POWDER: Platform for open wireless data-driven experimental research," https://powderwireless.net/, 2020.
[6] B. Cheng, H. Lu, A. Rostami, M. Gruteser, and J. B. Kenney, "Impact of 5.9 ghz spectrum sharing on dsrc performance," in *2017 IEEE Vehicular Networking Conference (VNC)*, 2017, pp. 215–222.
[7] J. Choi, V. Marojevic, R. Nealy, J. H. Reed, and C. B. Dietrich, "Dsrc and ieee 802.11ac adjacent channel interference assessment for the 5.9 ghz band," in *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, 2019, pp. 1–5.
[8] I. Khan and J. Härri, "Can ieee 802.11p and wi-fi coexist in the 5.9ghz its band?" in *2017 IEEE 18th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2017, pp. 1–6.
[9] I. Mavromatis, A. Tassi, and R. J. Piechocki, "Operating its-g5 dsrc over unlicensed bands: A city-scale performance evaluation," in *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2019, pp. 1–7.
[10] Ettus Research, "USRP B210: Universal Software Radio Peripheral B210," https://www.ettus.com/all-products/ub210-kit/, 2020.
[11] GNU Radio Project, "GNU Radio," https://https://www.gnuradio.org/, 2020.
[12] J. Dugan, S. Elliot, B. Mah, J. Poskanzer, and K. Prabhu, "iPerf: The ultimate speed test tool for tcp, udp and sctp," https://https://www.iperf.fr/, 2020.
[13] J. Lansford, J. B. Kenney, and P. Ecclesine, "Coexistence of unlicensed devices with dsrc systems in the 5.9 ghz its band," in *2013 IEEE Vehicular Networking Conference*, 2013, pp. 9–16.
[14] A. Vialard, A. Wir-Konas, and A. Araldi, "Frontage and setbacks: a comparison of english and north american suburban houses," in *2020 Conference of the International Seminar on Urban Form*, 02 2021.
[15] Keysight Technologies, "N1913A EPM Series Single-Channel Power Meter," https://www.keysight.com/us/en/product/N1913A/epm-series-single-channel-power-meter.html, 2022.
[16] Keysight Technologies , "N8482A Thermocouple Power Sensors," https://www.keysight.com/us/en/product/N8482A/thermocouple-power-sensor-100-khz-6-ghz-35-dbm-20-dbm.html, 2022.
[17] United States Department of Transportation (USDOT), "Dsrc roadside unit (rsu) specifications document v4.1," October 2016.
[18] Ettus Research, "USRP X310: Universal Software Radio Platform X310," https://www.ettus.com/all-products/x310-kit/, 2020.