Impact of 5.9 GHz Spectrum Sharing on DSRC Performance

Bin Cheng*, Hongsheng Lu†, Ali Rostami*, Marco Gruteser*, John B. Kenney†
*WINLAB, Rutgers University, USA
†Toyota Info Technology Center, USA
Email: cb3974@winlab.rutgers.edu, hlu@us.toyota-itc.com,
{rostami, gruteser}@winlab.rutgers.edu, jkenney@us.toyota-itc.com

***Abstract*—To increase the amount of contiguous spectrum available for unlicensed use, there is interest in both the United States and Europe to allow secondary users on the 5.9 GHz band allocated for Intelligent Transportation Services. Under standard spectrum sharing rules, secondary users such as Wi-Fi are required to avoid harmful interference to primary users such as DSRC devices. Compared to conventional spectrum sharing scenarios, such as unlicensed devices sharing TV whitespaces, the safety-critical nature of DSRC transmissions places stricter requirements on the effectiveness of spectrum sharing mechanisms.**

In this paper, we analyze this spectrum sharing problem to identify its fundamental challenges and derive interesting network sharing scenarios. We also evaluate two recently proposed spectrum sharing mechanisms, Detect & Vacate and Detect & Mitigate, to understand their performance in these challenging scenarios. We identify that both mechanisms suffer from a delayed detection problem, which can be effectively improved by extending interframe idle periods. We further find that due to the unilateral hidden terminal problem, Detect & Mitigate can introduce up to 30% extra packet loss to DSRC transmissions after detecting the presence of DSRC devices. However, Detect & Vacate leaves the band after detecting DSRC, minimizing the impacts on DSRC transmissions.

I. Introduction

Due to increasing congestion in available unlicensed bands, strong interest exists in letting Wi-Fi exploit the 5.850–5.925 GHz (5.9 GHz) band [1], [2]. In the US, this would allow access to three additional 20 MHz channels, two 40 MHz channels or, perhaps more importantly, allow creating an additional contiguous 80 or 160 MHz Wi-Fi channel, as shown in Fig. 1. In Europe, where the 5.8 GHz band is generally not available for Wi-Fi, opening the 5.9 GHz band would add much needed spectrum for Wi-Fi. This motivated proposals to open the 5.9 GHz band for spectrum sharing in both regions.

However, the primary applications of Dedicated Short Range Communications (DSRC) [1] systems in the 5.9 GHz band are safety-critical, which places stricter requirements on network performance, e.g., lower packet loss rate and inter-packet reception delay, than in other spectrum sharing scenarios such as TV whitespaces. DSRC is an Intelligent Transportation System (ITS) technology that enables direct vehicle-to-vehicle and vehicle-to/from-infrastructure communication. It allows a vehicle to share trajectory, driving status as well prevailing road and traffic conditions with other vehicles and roadside devices. With this shared information, significant improvements in road safety and efficiency are expected. This potential impact motivated the U.S. Federal Communications Commission (FCC) to designate DSRC as a primary service in the licensed 5.9 GHz band in 1999 [3]. Such safety-related applications of primary users raise deep questions about the interference avoidance guarantees that spectrum sharing protocols offer and how such protocols can be evaluated—not just in the average case but also under challenging, near-worst case conditions.

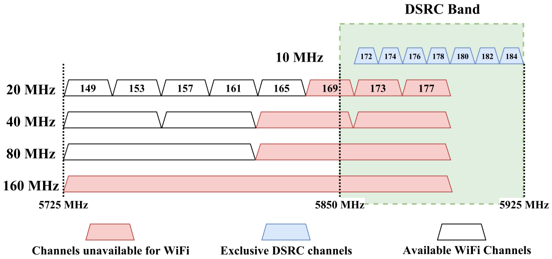


Fig. 1: DSRC and Wi-Fi Channelization in US 5.7-5.9 GHz band

While significant work has been conducted on spectrum sharing protocols (e.g., [4]–[6]), the previous work has primarily focused on sharing with non-safety related applications, i.e., assuming applications with modest loss and latency requirements. For safety-related communications in the 5.9 GHz band, two spectrum sharing mechanisms have been proposed by the Wi-Fi industry in the European Telecommunications Standards Institute (ETSI): Detect & Vacate (D&V) and Detect & Mitigate (D&M). These are defined and their performance is studied in ETSI TR 103 319 [7]. Prior work has studied the performance gains that Wi-Fi can achieve through spectrum sharing with DSRC [8], [9]. However, we are not aware of any publications that carefully evaluate the impact of Wi-Fi on DSRC and, in particular, any analysis of challenging and near-worst case scenarios.

In this paper, we conduct such an analysis by identifying fundamental challenges, providing guidance on challenging scenarios, and simulating D&V and D&M under such two challenging scenarios. In particular, our analysis identifies the delayed detection problem and the unilateral hidden terminal

[1] In Europe the communication referred to in this paper as DSRC is typically called Cooperative-ITS or ITS G5.

problem as key issues. Delayed detection arises because conventional primary user detection mechanisms on secondary user devices are typically only effective when the secondary devices are idle. In other words, a Wi-Fi device can usually detect the presence of DSRC transmissions only when it itself is not transmitting. While not unique to the DSRC scenario, the detection delay is more relevant due to fast moving vehicles and the safety-related nature of applications. The unilateral hidden terminal problem arises due to DSRC and Wi-Fi using different channel bandwidths, which means that DSRC devices can not effectively detect and defer to Wi-Fi transmissions even if the Wi-Fi device has a DSRC detector. When DSRC transmits on a channel already busy with a Wi-Fi transmission, the DSRC packet is usually lost.

These insights provide guidance for identifying challenging spectrum sharing scenarios. They also motivate an extended idle period technique that we introduce and evaluate to mitigate the detection delay problem.. We further construct two such scenarios and study the performance of D&V and D&M in these settings via ns-3 simulations. We find that even in benign channel conditions, it can take an average of 20 DSRC transmissions (which translates to a minimum of 2 seconds delay, depending on DSRC transmission rates) before Wi-Fi detects the DSRC devices, and that this delay can be effectively reduced with extra idle periods between Wi-Fi transmissions. We further find that D&M can induce up to 30% extra packet loss (comparing to a ”no Wi-Fi” case) on DSRC transmissions even after detecting the presence of DSRC devices, while D&V protects DSRC transmissions by leaving the ITS band after detection.

II. Background

This section reviews popular spectrum sharing techniques in the wireless communication community and briefly introduces the technical background of D&V and D&M.

A. Listen-before-talk

Listen-before-talk (LBT) is a spectrum sharing technique that requires devices to monitor channel status and only transmit packets when the channel is assessed to be idle (clear). This Clear Channel Assessment (CCA) is achieved through two methods, Carrier Sensing (CS) and Energy Detection (ED).

TABLE I: Channel busy thresholds defined in the IEEE 802.11 standard

Channel bandwidth	CS threshold (dBm)	ED threshold (dBm)
10 MHz	-85	-65
20 MHz	-82	-62

The CS mechanism matches the preamble of the received signal with a known training symbol sequence. It is primarily designed to avoid interference from other devices using the same technology (i.e., with same preamble). The ED mechanism detects whether the energy on the channel is above a certain threshold, regardless of the form of the signal. The ED mechanism can be used to reduce interference between devices using different technologies. In the IEEE 802.11 standard, the ED detection threshold is 20 dB higher than the CS detection level, see Table I.

LBT is the primary technique used to resolve backward compatibility issue between a newer version of Wi-Fi protocols and legacy Wi-Fi protocols. For example, IEEE 802.11ac [10] transmissions begin with a legacy IEEE 802.11a preamble so that a 802.11ac transmission can be detected by legacy Wi-Fi receivers via CCA. LBT is also typically used to share with low power (e.g. Wi-Fi) devices, and each device performs its own LBT detection. After a busy channel is detected, the LBT function reassesses the availability of the channel when it is detected to be idle again, typically after a few milliseconds. LBT is generally not considered to be robust enough to protect primary users from harmful secondary interference.

B. Dynamic frequency selection

The second solution is Dynamic Frequency Selection (DFS). The purpose of DFS is to ensure that secondary users do not interfere with primary radar systems [11]. As required by various spectrum regulations, a secondary user (e.g. Wi-Fi local area network) operating in the radar band should passively scan for and select a channel not occupied by radars. If the radar waveform is detected, Wi-Fi devices must cease using the channel, and will most often execute a channel switching procedure [12].

Comparing LBT and DFS, we realize that both approaches require detection of and deferral to other users in order to avoid interference. However, LBT does not differentiate channel users while DFS aims to detect the primary user of the channel. LBT is typically implemented in each device to detect low power transmissions from near neighbors. By contrast, DFS detects high power radar signals, so one detector can operate on behalf of the entire secondary network. Also, LBT only defers to other transmissions over a short term (milliseconds). But the deferral from transmissions in DFS is for a relatively long term (at least 30 min) [11].

While elements of LBT and DFS can be applied to the Wi-Fi and DSRC coexistence scenario, neither technique would be sufficient on its own. It is mainly because: 1) LBT require mutual detection between users, is not designed to prevent all interference, and so is insufficient to protect DSRC safety applications adequately. Also, by definition DSRC cannot use LBT to detect and defer to every unspecified unlicensed technology; 2) DSRC is a low power short range technology used by highly mobile devices, in contrast to fixed location high-power radar, so DFS techniques cannot apply directly to protection of DSRC.

C. DSRC detector for Wi-Fi devices

The DSRC Physical (PHY) and Medium Access Control (MAC) protocols are a variation of the IEEE 802.11a standard, referred to as Wireless Access in Vehicular Environments

(WAVE). This variation, which typically uses 10 MHz channels, is specified in the IEEE 802.11p amendment [13]. The similarity of Wi-Fi and DSRC suggests a simplified DSRC detection function that leverages a Wi-Fi CCA modified to search for 10 MHz preambles. On the other hand, DSRC devices do not detect 20 MHz Wi-Fi preambles, so spectrum sharing that relies on mutual carrier sensing will be ineffective. The two sharing approaches below both utilize detection of DSRC, but take different views of the lack of mutual sensing.

D. Details of D&V and D&M

D&V approach, proposed by Cisco, requires Wi-Fi devices to be equipped with DSRC detectors. If a Wi-Fi device operating in the DSRC band detects a DSRC transmission, it needs to vacate the entire DSRC band for a few seconds. A premise of D&V is that, since DSRC cannot detect Wi-Fi transmissions it is not safe for Wi-Fi to use the band when DSRC activity has been detected. The precise detection sensitivity threshold and length of vacate period are parameters of the proposal.

Similar to D&V, D&M [2], proposed by Broadcom, relies on the DSRC detector to monitor the appearance of DSRC transmissions. However, instead of leaving the ITS band, D&M allows a packet-by-packet spectrum sharing after the detection of DSRC transmissions. More specifically, the D&M approach adjusts the medium access parameters of the IEEE 802.11 Enhanced Distributed Channel Access (EDCA) mechanism. In EDCA, Arbitration Interframe Space Number(AIFSN), minimum and maximum size of Contention Window (CW_{min} and CW_{max}) control the timing with which a device accesses the channel when it becomes idle, and thus provide different levels of channel access priority to traffic using different EDCA parameters. Four EDCA access categories, in ascending order of priority, are: background (AC_BK), best effort (AC_BE), video (AC_VI), and voice (AC_VO). Upon detection of DSRC transmissions, D&M increases the EDCA parameters of each access category, such that the minimum gap between two consecutive Wi-Fi transmissions is prolonged as compared to that enabled by the default EDCA, see Table II.

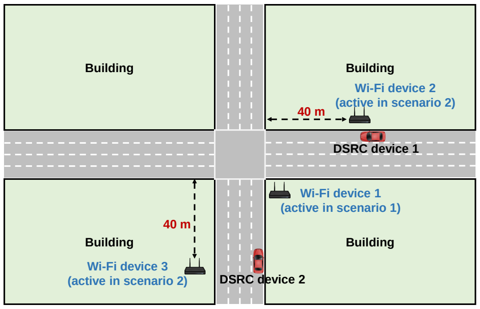
TABLE II: EDCA parameters in D&M after DSRC detection

AC	CW_{min}	CW_{max}	AIFSN	Max TxOp
AC_BK	31	2047	2065	2.258 ms
AC_BE	31	2047	2059	2.258 ms
AC_VI	15	31	1029	3.008 ms
AC_VO	7	15	515	1.504 ms

The rationale behind the increased inter-packet gap is to enable an improved probability for DSRC packets to be sent before Wi-Fi packets when DSRC and Wi-Fi devices observe the same channel-busy conditions. However, as noted, since DSRC does not detect Wi-Fi transmissions (unless they are very close, such that they trigger DSRC's CCA-ED), this rationale is only weakly fulfilled. Rather than providing strict priority, as EDCA is designed to do, the mitigation of interference under D&M is only a function of the extent to which Wi-Fi channel utilization is reduced after detection. This is evident in the simulations in Section V below.

III. Methodology Overview

This paper, to our best knowledge, is the first to investigate the performance of D&V and D&M from the perspective of ITS safety applications through a combination of systematic analysis and detailed simulations. For better clarity, the investigation begins with separating each algorithm into a pre-detection phase and a post-detection phase. The former is defined as the time interval that starts from the moment at which DSRC activities appear on the channel and ends when an interfering Wi-Fi device engages its mitigation mechanism. During this phase, we are interested in understanding how fast a Wi-Fi device may detect the presence of DSRC transmissions since delay in detection could cause interference to DSRC operations. By contrast, the analysis for the post-detection phase focuses on studying if a Wi-Fi device can protect DSRC transmissions after being detected. Insights obtained in these analysis will be used to guide design of simulation configurations. The performance of D&V and D&M are then evaluated with these challenging configurations via ns-3 simulations.



Scenario 1: Pre-Detection with Wi-Fi device 1;
Scenario 2: Post-Detection with Wi-Fi device 2 and Wi-Fi device 3

Fig. 2: The simulation scenarios at an intersection

A. Simulation Configurations

Our main simulation scenario is a four-leg intersection, shown in Fig. 2. Selection of the intersection scenario is driven by: 1) Wi-Fi is commonly available near urban intersections; 2) communications between DSRC devices for collision avoidance at intersections can be non-line-of-sight (NLOS). Compared with line-of-sight (LOS) communications, for a given transmitter-receiver distance a NLOS signal is normally weaker, making NLOS communications more vulnerable to interference [14], [15]. In this work, we assume a closed intersection which has a building at each of its corners. Two vehicles will be transmitting DSRC packets from perpendicular approaches to the intersection. The position and traffic volume of each Wi-Fi device are carefully configured in order to create near-worst scenarios.

We rely on network simulations to verify the theoretical observations and evaluate the performance of the studied

[2] Note: two variations of D&M are studied in TR 103 319. In this paper we focus on the more conservative variation, called ”Decreased EDCA”.

mechanisms. The key simulation parameters used in our simulations are listed in Table III.

TABLE III: Simulation configurations

Configuration items	Values
Network simulator	ns-3.25 [16]
DSRC transmit power	20 dBm
Wi-Fi transmit power	20 dBm
DSRC transmit rate	2.5 Hz
Wi-Fi transmit rate	MAC always has a packet (saturation mode)
DSRC transmission duration	0.5 ms
Wi-Fi transmission duration	limited by maximum TxOp
Threshold for detection of DSRC by Wi-Fi	-85 dBm
DSRC reception sensitivity	-92 dBm
Wi-Fi ED threshold	-62 dBm
DSRC ED threshold	-65 dBm
DSRC to/from DSRC propagation model	VirtualSource11p [17]
Wi-Fi to/from DSRC propagation model	IEEE P802.11 TGn [18] with 15dB signal attenuation per wall

B. Evaluation Metrics

Two metrics are primarily used to evaluate the impact of Wi-Fi transmissions on DSRC performance:

The first contact distance to the intersection center. It is defined as the distance to the intersection center at which the two DSRC devices start to receive packets from each other (the DSRC devices are equi-distant from the intersection in this paper). Generally, a larger first contact distance is preferred, since it offers longer time for the two cars to take necessary actions to prevent collisions.

The DSRC PER in the post-detection phase. This evaluates how well a Wi-Fi device can provide protection to DSRC transmissions after it detects the presence of DSRC devices. Ideally, once the DSRC devices are detected by the Wi-Fi devices, the DSRC devices are expected to perform as well as when no Wi-Fi devices share the spectrum.

IV. Analysis of Pre-detection Phase

We explore in this section the challenges for Wi-Fi devices to detect the presence of DSRC devices. It has been observed that interference from a Wi-Fi device's transmission prevents its DSRC detector from working until the transmission completes. This observation leads to identification of a near-worst setting for D&V and D&M by making a Wi-Fi device transmit with a saturated load, i.e., the Wi-Fi device always has a packet to be sent.

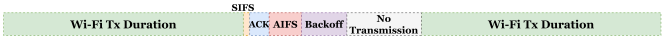


Fig. 3: Wi-Fi transmission sequence

A. Challenge: self-interference on DSRC Detector

A DSRC detector, upon detecting a DSRC transmission, will report a channel busy event to the host Wi-Fi device. We focus on the case of detection based on the DSRC preamble (CCA-CS), since CCA-ED requires very close proximity to the DSRC transmitter. It is generally only possible to detect the DSRC preamble if it begins at a moment when the host Wi-Fi device and other nearby Wi-Fi devices are not transmitting in the same DSRC channel. The interference from such a Wi-Fi transmission would prevent an incoming DSRC preamble from being decoded at the DSRC detector. Fig. 3 shows an example channel access time-line for a Wi-Fi LAN. We can see that a Wi-Fi device releases the channel for a Short Interframe Space (”SIFS”) after it finishes one transmission. If an acknowledgement (ACK) is received successfully, the Wi-Fi device will start an idle interframe period, consisting of an Arbitration Interframe Space (AIFS) and a backoff time period whose length is random within a certain range, before it can send another packet. The lengths of the AIFS and the backoff time period are controlled by AIFSN and CW_{min}, respectively. The ”No-packet” period in the figure represents the time duration when none of the Wi-Fi devices have packets ready to be sent and the channel remains idle. In this example, if we further assume that the signal strength of the ACK packet is strong enough to interfere with the detection of DSRC transmissions, the probability for a DSRC preamble to be detected then equals to the probability that the start of the DSRC preamble falls into any of ”SIFS”, ”AIFS”, ”Backoff” and ”No-packet” periods, i.e., the periods when the Wi-Fi devices are not transmitting [3]. We define the sum of the four periods as an idle period. Therefore, the expected DSRC detection probability can be estimated as $Prob_{detection} = \frac{idle\ period}{idle\ period + WiFi\ Tx\ duration}$

B. Near-worst case study

The above analysis shows a way to identify a near-worst case for detecting DSRC transmissions. That is to reduce the length of ”No-packet” period to zero, or, in other words, to make a Wi-Fi device transmit in saturation. With the default Wi-Fi channel access parameters (AIFS = 43 μs, SIFS = 16 μs, the average length of the backoff duration = 67.5 μs and the length of an ACK = 44 μs) and 2 ms Wi-Fi transmission duration, the average idle period in the equation above is 126.5 μs long and a DSRC preamble can be detected, on average, with a probability of only 5% in a near-worst case.

One implicit assumption behind this 5% detection probability is that the arrival time of DSRC packets at a DSRC detector is independent of the host Wi-Fi device's transmission timing. This assumption is valid in this study because the interval between two consecutive DSRC transmissions is typically a few hundred milliseconds. This is long enough to witness many 2 ms Wi-Fi transmissions. The backoff period with a random length can randomize the Wi-Fi transmission phase at which a DSRC packet arrives. With this observation, we model the DSRC detection as a Bernoulli experiment, whose trial is considered successful when a DSRC transmission is initiated at a time when no Wi-Fi transmission is active. Given the above analysis, the probability of a successful trial, noted by p, is 5% for the Wi-Fi saturation case. With this model,

[3] While detection of a preamble actually requires that the first 8 microseconds be free of interference, in the following analysis we ignore that short interval and model detection as successful if the start of the preamble occurs when the channel is otherwise idle.

we can then calculate the average number of trials to the first successful one, noted by n, i.e., with $n-1$ failures, the trial n is successful. The expected value of n is defined by $\frac{1}{p}$. Given $p = 5\%$, the expected value of n is 20, which means approximately 20 DSRC transmissions are required before one DSRC transmission can be detected by the Wi-Fi device.

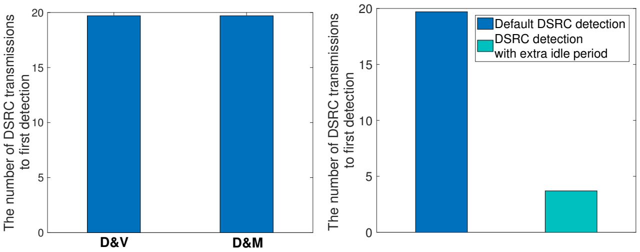
To validate the above assumptions, the identified near-worst case is also created in the ns-3 simulator where two DSRC devices in Fig. 2 remain stationary, each 25 m away from the stop line in their respective lane. One Wi-Fi device, located indoors near the intersection, generates all Wi-Fi traffic in this scenario (see Wi-Fi device 1 in Fig. 2). When a car approaches the intersection, its risk of colliding with another car approaching in the perpendicular road grows and thus communication between the two cars becomes increasingly important. Comparing to a Wi-Fi device located far from the intersection, Wi-Fi device 1 has higher potential to interfere with the transmissions between two DSRC devices, and consequently results in more severe threats to driving safety.

Fig. 4a shows that the average number of DSRC transmissions to the first detection for D&V and D&M is similar since they share the same detection function. Both mechanisms require about 20 DSRC transmissions on average before a successful DSRC detection. The simulation results agree with the theoretical analysis, which validate our modeling assumptions.

C. *Adding an additional idle period*

Without a fast and effective DSRC detection mechanism, many DSRC packets can collide with Wi-Fi packets, resulting in significant performance degradation of DSRC systems. The ETSI Cooperative Awareness Message (CAM) is typically sent when a vehicle travels at least 4 meters, so 20 unsuccessful CAM transmissions corresponds to at least 80 meters of travel toward the intersection by both vehicles in this scenario. We argue that an average of 20 DSRC transmissions may impose too long a detection delay. However, we observe that by adding an additional idle period to the Wi-Fi interframe idle periods, the detection performance can be significant improved. Fig 4b shows the results of the simulation where we experimentally add 266 μs to each AIFS period (the value 266 μs was introduced in [19]). Then, the expected number of DSRC transmissions to the first detection decreases from 20 to approximately 4. Given the significant improvement, the ETSI technical report incorporated this extended idle period into the definition of D&V [7]. Since the extra idle period is short, its impact on the Wi-Fi performance is marginal.

D. *Performance evaluation in a mobile scenario*

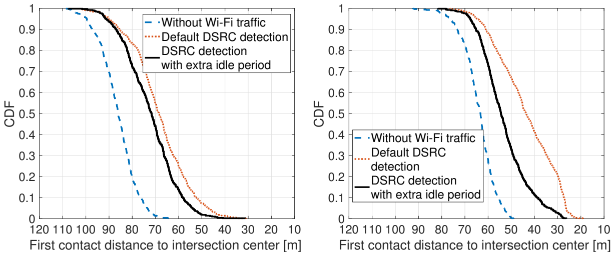


(a)

(b)

Fig. 4: The average number of DSRC transmissions to the first detection with Wi-Fi transmission duration as 2 ms (a) D&V v.s. D&M; (b) with v.s. without extra idle period

The detection performance of D&V and D&M with saturated Wi-Fi traffic is also studied in a mobile scenario, where the two DSRC devices in Fig. 2 are moving at speed 10 m/s towards the intersection center from 200 m away. Note that in order to create a car collision threat, the two cars move symmetrically towards the intersection. Fig. 5a and Fig. 5b depict the distribution of the first DSRC contact distance to the intersection center for two DSRC signal propagation conditions. From Fig. 5a, it can be observed that without Wi-Fi traffic, the two DSRC devices can communicate with each other before they are 65 m from the intersection center. However, with Wi-Fi traffic, it is possible that the first contact between DSRC devices does not occur until they are 30 m from the intersection center. A similar trend is also shown in Fig. 5b, except in this harsher DSRC propagation environment [4], the DSRC devices have to be closer before they can communicate. Therefore, even without Wi-Fi traffic, the minimum value of the first contact distance decreases to 50 m. However, with Wi-Fi traffic, the two DSRC devices may not achieve first contact until they are only 20 m away from the intersection center. A collision avoidance application will likely fail with such a small first contact distance.



(a)

(b)

Fig. 5: The CDF of DSRC first contact distance to the intersection center with different DSRC propagation environments: (a) less harsh environment [17]; (b) harsher environment

Comparing Fig. 5a with Fig. 5b, we notice that the effect of adding an additional idle period is sensitive to the DSRC propagation conditions. The advantages of the longer idle period are more evident in the harsher propagation environment (Fig. 5b) than in the less harsh propagation environment (Fig. 5a), e.g., in Fig. 5b, the probability that the first contact distance is at least 50 m increases from 30% to 70% with the longer idle period. By contrast, in Fig. 5a, the probability improvement is less than 10%. We believe the main reason for

[4] The harsher propagation environment is created by increasing the propagation exponent of the signal propagation model from 2.69 to 2.85. Therefore, at a given distance, the harsher environment produces stronger signal loss

such a difference is: 1) adding an additional idle period is expected to primarily improve the DSRC detection performance; 2) in a less harsh DSRC signal propagation environment, the signal strength of a DSRC link may be strong enough to overcome the interference from Wi-Fi transmissions at the DSRC receiver, which means even with less effective DSRC detection, the DSRC devices have a better chance for first contact at these higher distances; 3) in a harsher DSRC signal propagation environment, the DSRC link is more vulnerable to the interference, such that in this environment, the first contact of DSRC devices depends more on first achieving successful DSRC detection, where the additional idle period is comparatively more useful. The DSRC signal propagation at an intersection relies heavily on the building configurations at the corner. Several harsh propagation environments have been reported in field experiments [15]. Nevertheless, even in the less harsh environment, the additional crashes that can be prevented when the longer idle period is used are important relative to the modest reduction in maximum Wi-Fi channel utilization associated with that idle period.

V. Analysis of Post-detection Phase

In this section, we identify the challenges for Wi-Fi devices to protect DSRC transmissions after they detect the presence of DSRC devices. We observe that due to lack of mutual detection, D&M can cause extra packet losses in DSRC transmissions, while D&V requires Wi-Fi devices to leave the band, minimizing its impact on DSRC performance.

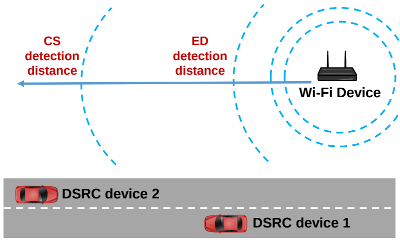


Fig. 6: Illustration of the unilateral hidden terminal problem

A. Challenge: unilateral hidden terminal

Wi-Fi devices use the carrier sense mechanism for DSRC detection via the integrated DSRC detector. However, DSRC devices can sense unlicensed device(e.g. Wi-Fi) transmissions only through the energy detection mechanism. Given the higher threshold for the ED mechanism (see Table I), in many cases, DSRC devices may not be able to sense and defer to Wi-Fi transmissions. This leads to a unilateral hidden terminal problem. As an example shown in Fig. 6, DSRC device 2 generates a new packet and the packet is ready to be sent before a Wi-Fi transmission completes. Since there is no other ongoing DSRC transmissions and the Wi-Fi signal is not strong enough to be detected through the ED mechanism, DSRC device 2 considers the channel idle and starts its transmission, leading to a packet collision between DSRC device 2 and the Wi-Fi device. As a result of the Wi-Fi interference, DSRC device 1 will not be able to successfully decode the packets from DSRC device 2. Until DSRC device 2 becomes close enough to the Wi-Fi device, i.e., when the ED detection becomes available, DSRC device 2 then starts to defer to the Wi-Fi transmissions. This is called the unilateral hidden terminal problem because the Wi-Fi device is hidden from the DSRC device, even though the DSRC device is not hidden from the Wi-Fi device.

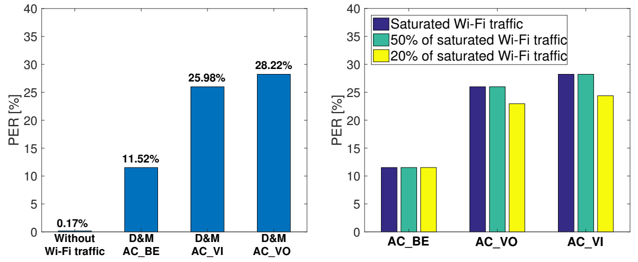
B. Near-worst case study

D&V and D&M suffer from the unilateral hidden terminal problem in different levels. D&V leaves the spectrum upon detecting DSRC transmissions for several seconds. Therefore, after a successful detection, the Wi-Fi device will not affect the DSRC transmissions. On the other hand, D&M tries to squeeze Wi-Fi transmissions between DSRC transmissions after detection. In this section we focus on the analysis of the post-detection performance of D&M. Considering the same example in Fig. 6, transmissions from DSRC device 2 may collide with transmissions from the Wi-Fi device due to the unilateral hidden terminal problem, and it is expected that *a) a longer Wi-Fi transmission duration would lead to a higher packet collision probability; b) shorter Wi-Fi interframe idle periods would also result in a higher packet collision probability*. According to the EDCA parameters of D&M for the post-detection phase in Table II, the minimum Wi-Fi interframe idle periods are 18.72 ms, 9.32 ms, and 4.65 ms for AC_BE, AC_VI and AC_VO, respectively. The Wi-Fi transmission duration is limited by the defined ”Max TxOp”, which are 2.2 ms, 3.0 ms, and 1.5 ms for AC_BE, AC_VI and AC_VO, respectively. With these configurations, the collision probability between Wi-Fi transmissions and DSRC transmissions can be estimated as equal to the ratio of the Wi-Fi transmission duration to the total Wi-Fi transmission cycle (the transmission duration plus the interframe idle duration). Based on the Max TxOp and minimum interframe idle periods above, the collision probability estimates are 10.5% for AC_BE (i.e., $2.2/(18.72+2.2)$), 24.3% for AC_VI (i.e., $3/(9.32+3)$) and 24.4% for AC_VO (i.e., $1.5/(4.65+1.5)$). The calculation is based on two assumptions: 1) Wi-Fi traffic is saturated. Therefore, besides AIFS and backoff time, there is no other significant idle time between two Wi-Fi transmissions; 2) The transmission timing of Wi-Fi packets and DSRC packets is independent, i.e., when a Wi-Fi transmission occurs is independent of when a DSRC transmission starts. The calculated results identify the near-worst case occurs when using AC_VO.

We validate the aforementioned theoretical analysis via the ns-3 simulations. The studied scenario is: two DSRC devices in Fig. 2 remain stationary and each one is 40 m away from the stop line. Two Wi-Fi devices are located indoors, 40 m away from the stop line (one near each DSRC device), see Wi-Fi device 2 and 3 labeled by ”active in scenario 2” in Fig. 2. With this configuration, two unilateral hidden terminal pairs are created, i.e., Wi-Fi device 2 is hidden from DSRC device 2 and Wi-Fi device 3 is hidden from DSRC device 1. This simulation setting also ensures Wi-Fi devices 2 and 3 are incapable of communicating with each other due to strong signal attenuation through walls; instead each Wi-Fi device transmits to unshown clients nearby.

Fig. 7a shows the PER of DSRC device 1 receptions for different Wi-Fi ACs causing interference. It is observed that without any Wi-Fi traffic, the packet loss for the link from DSRC device 2 to DSRC device 1 is about 0.2% only. However, 11.35% extra packet loss is introduced by the Wi-Fi transmissions when AC_BE is used. The extra PER increases to 25.98% and 28.22% for AC_VI and AC_VO, respectively. The simulation results approximately agree with the theoretical analysis. The slight difference results from the fact that the transmission events of DSRC and Wi-Fi are not fully independent in the simulations.

One may argue that the generated traffic for AC_VO and AC_VI is normally not high enough to saturate the channel. Therefore, this near-worst case primarily caused by saturated Wi-Fi traffic rarely occurs. However, notice that the maximum channel utilization for these traffic classes during mitigation is only 24% due to the relaxed EDCA parameters, so ”saturation” occurs at this relatively low channel load. As shown in Fig. 7b, if Wi-Fi traffic is limited to no more than 20% of the channel load we would see under saturation with normal EDCA parameters, the resulting PER is similar as for the saturated traffic case. This is because in the saturated case the actual Wi-Fi channel utilization is not much more than 20%.



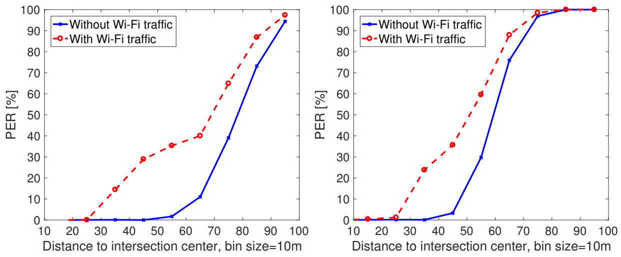
(a) (b)

Fig. 7: The post-detection PER of DSRC device 1 in Fig. 2 (a) different EDCA categories; (b) different traffic volume

C. Performance evaluation in a mobile scenario

We have identified that the near-worst case of packet loss introduced by Wi-Fi transmissions to DSRC transmissions occurs when the Wi-Fi devices use the AC_VO category. In this subsection, we focus on studying the performance of this near-worst case in a mobile scenario. The simulated scenario is similar to the previous DSRC stationary scenario, except two DSRC devices in Fig. 2 are now moving towards the intersection center from 200 m away at speed 10 m/s.

Fig. 8a and Fig. 8b depict the PER of DSRC transmissions at different distances to the intersection center with different DSRC signal propagation conditions. It is observed from both figures that at a short distance (e.g., < 25 m) there is essentially no DSRC packet loss even with Wi-Fi traffic, while at large distances (e.g., > 85 m), the performance difference between with and without Wi-Fi traffic is not large. It is because at short distances, the signal strength between the two DSRC device is strong enough to overcome the interference from the Wi-Fi device. However, even though at such short distances the DSRC devices can communicate with each other with a low packet loss rate, we argue that 25 m to the intersection center may be too short for drivers to take necessary actions to prevent car collisions. At large distances, the packet loss is dominated by the propagation loss, such that the extra packet loss introduced by the Wi-Fi traffic is not as visible in the PER plot, though Wi-Fi is still interfering with many of the remaining packets that have enough power to be received (e.g. at a distance where only 25% of DSRC packets can be received on the ”without Wi-Fi traffic” curve, about half of those successful DSRC packets are killed by Wi-Fi interference on the ”with Wi-Fi traffic” curve). Most importantly, at the critical distance range $25 - 75$ m, D&M introduces up to 30 percentage points of extra packet loss to the DSRC transmissions. We believe this high extra packet loss can significantly degrade the DSRC application performance. From Fig. 8b, we also observe that in a harsher propagation environment, the DSRC devices are required to be closer in order to overcome the interference from the Wi-Fi devices. And the propagation loss increases more dramatically, such that at a shorter distance (i.e., starting from 65 m) the signal propagation becomes the dominating factor for the packet loss.



(a) (b)

Fig. 8: The PER of DSRC transmissions v.s. the distance of DSRC devices to intersection center with different DSRC propagation environments: (a) less harsh environment [17]; (b) harsher environment

VI. Discussion

The previous sections investigate the impact of Wi-Fi transmissions on DSRC network performance. However, how network performance can address application requirements and then contribute to application performance remain challenging. To tackle the challenge, we utilize awareness, proposed in [20], to link the DSRC network performance and the safety application performance. We believe the awareness is an intermediate metric which is influenced by the network layer and understood by the application layer.

In [20], the neighborhood awareness of a DSRC network is defined as at least n safety messages are successfully received during a tolerance time window T, and the awareness

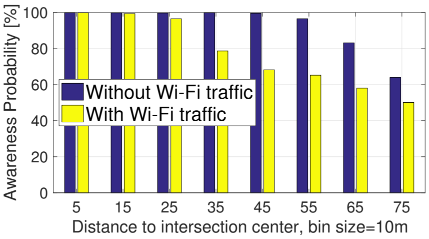


Fig. 9: Awareness probability of D&M with AC_VO at different distances

probability is used to evaluate the chances of a vehicle being aware. A higher awareness probability indicates a vehicle has more chances of being aware of its neighboring vehicles and thus the safety applications which are built upon neighborhood awareness can operate with higher reliability.

To investigate the impact of Wi-Fi traffic on the awareness probability and further on the effectiveness of safety applications, we perform an example study in the simulation scenario 2 described in Fig. 2 with two DSRC devices moving at 10 m/s and Wi-Fi devices operating in the AC_VO category. The primary focus is the post-detection performance of D&M. Different safety applications may require different levels of awareness, i.e., different n and T. In our study, we assume $n = 1$ and $T = 0.5s$, which matches the requirements of the collision avoidance application described in [20].

Fig. 9 compares the awareness probability of simulations with and without Wi-Fi traffic at different distances to the intersection center. It can be observed that the awareness probability is decreased as the Wi-Fi traffic is introduced into the network, especially at 45 m and 55 m, the awareness probability is reduced by more than 30 percent points. If a safety application requires more than 90% awareness probability, the safety application will not be able to operate effectively with the presence of Wi-Fi traffic at these distance bins.

VII. Conclusion

In this paper, we evaluate the performance of two mechanisms for sharing the ITS band between DSRC devices and Wi-Fi devices. The two mechanisms were proposed by the Wi-Fi industry and actively discussed in the European standardization group for possible deployment. We identify that the Wi-Fi devices suffer from a delayed detection problem in both mechanisms. However, by adding an extra idle period to the Wi-Fi interframe idle period, the detection performance can be significantly improved. After detection, we observe that D&M can introduce more than 30% extra DSRC packet loss in certain cases, compared to none for D&V, which appears undesirable. We also observe that the degraded network performance can further reduce the effectiveness of safety applications that are built upon V2V communications.

One key observation is that even though DSRC and Wi-Fi use similar medium access control mechanisms, this mechanism is less effective when these technologies operate over different bandwidths (10MHz in DSRC and 20+MHz for Wi-Fi). Devices are not able to perform mutual preamble detection for carrier sensing, which leads to less effective channel access decisions. This explains the lower performance of the D&M mechanism, whose mitigation strategy appears to assume mutual detection.

References

[1] 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*, Dec 2013, pp. 9–16.

[2] Y. Park and H. Kim, "On the coexistence of ieee 802.11ac and wave in the 5.9 ghz band," *IEEE Communications Magazine*, vol. 52, no. 6, pp. 162–168, June 2014.

[3] The U.S. Federal Communications Commission, "Fcc 03-324 report and order," Tech. Rep., FCC, Dec. 2003.

[4] I. F. Akyildiz, W. y. Lee, M. C. Vuran, and S. Mohanty, "A survey on spectrum management in cognitive radio networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 40–48, April 2008.

[5] Eugene Chai, Karthik Sundaresan, Mohammad A. Khojastepour, and Sampath Rangarajan, "Lte in unlicensed spectrum: Are we there yet?," in *Proceedings of the 22Nd Annual International Conference on Mobile Computing and Networking*, New York, NY, USA, 2016, MobiCom '16, pp. 135–148, ACM.

[6] Paramvir (Victor) Bahl, Rohan Murty, Thomas Moscibroda, and Ranveer Chandra, "Senseless: A database-driven white spaces network," *IEEE Transactions on Mobile Computing*, vol. 11, pp. 189–203, 2011.

[7] Broadband Radio Access Networks (BRAN), "5 GHz high performance RLAN; Mitigation techniques to enable sharing between RLANs and Road Tolling and Intelligent Transport Systems in the 5 725 MHz to 5 925 MHz band ETSI TR 103 319 V1.1.1," Tech. Rep., 2017.

[8] Jian Wang, Tao Wu, Yanheng Liu, Weiwen Deng, and Heekuck Oh, "Modeling and performance analysis of dynamic spectrum sharing between dsrc and wi-fi systems," *Wireless Communications and Mobile Computing*, vol. 16, no. 16, pp. 2743–2758.

[9] Gaurang Naik, Jinshan Liu, and Jung-Min (Jerry) Park, "Coexistence of dedicated short range communications (dsrc) and wi-fi: Implications to wi-fi performance," in *Proceeding of 2017 IEEE International Conference on Computer Communications (INFOCOM)*, May 2017.

[10] "IEEE Standard for Information technology– Telecommunications and information exchange between systemsLocal and metropolitan area networks– Specific requirements–Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications–Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz.," *IEEE Std 802.11ac-2013*, Dec 2013.

[11] "Coexistence of 5 GHz RLAN with ITS," Tech. Rep., 2013.

[12] Y. Park and H. Kim, "On the coexistence of ieee 802.11ac and wave in the 5.9 ghz band," *IEEE Communications Magazine*, vol. 52, no. 6, pp. 162–168, June 2014.

[13] "IEEE Standard for Information technology– 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*, July 2010.

[14] 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.

[15] T. Mangel and H. Hartenstein, "5.9ghz ieee 802.11p inter-vehicle communication: Non-line-of-sight reception under competition," in *2011 IEEE Vehicular Networking Conference (VNC)*, Nov 2011, pp. 155–162.

[16] "Network simulator 3," https://www.nsnam.org/.

[17] Thomas Mangel, Oliver Klemp, and Hannes Hartenstein, "5.9 ghz inter-vehicle communication at intersections: a validated non-line-of-sight path-loss and fading model," *EURASIP Journal on Wireless Communications and Networking*, vol. 2011, no. 1, pp. 182, 2011.

[18] "IEEE P802.11 Wireless LANs TGn Channel Models," Tech. Rep., 2014.

[19] "IEEE P802.11 Wireless LANs: Proposal for 5850-5925 MHz unlicensed devices," *IEEE 802.11 submission*, 2013.

[20] N. An, T. Gaugel, and H. Hartenstein, "Vanet: Is 95% probability of packet reception safe?," in *2011 11th International Conference on ITS Telecommunications*, Aug 2011, pp. 113–119.