Can IEEE 802.11p and Wi-Fi Coexist in the 5.9GHz ITS band ?

Irfan Khan and Jérôme Härri,
EURECOM
06904 Sophia Antipolis, France
E-mails: {khanm, haerri}@eurecom.fr

***Abstract*—To support the increasing need for WiFi gigabit links, the IEEE 802.11ac technology introduced 80MHz and 160MHz channels, which led to an extended WiFi channelization at 5GHz, spanning over the ISM band up to 5.9GHz. However, 5.9GHz also accommodates the 70MHz spectrum reserved for vehicular traffic safety-related applications using IEEE 802.11p technology, forcing both technologies to coexist. In this paper, we highlight the inherent differences between these two technologies and formulate the coexistence challenge on a basic urban scenario. We present and evaluate two coexistence protocols proposed by the WiFi community. Lastly, we illustrate WiFi potential 'harmful' interferences to safety-related ITS applications and propose improvements for a better coexistence.**

I. Introduction

Future connected and cooperative vehicles will be based on the capability of vehicles to exchange awareness information based on the IEEE 802.11p technology (a.k.a Dedicated Short Range Communications - DSRC - in the US and ITS-G5 in the EU). For this purpose, seven 10MHz channels have been allocated in the 5.9GHz band exclusively for safety-related ITS communications. Although reserved since 1999 in the US and 2008 in Europe, *Day One* connected and cooperative vehicle applications merely use one of these seven channels, the six others being planned for *Day Two*.

Moving away from the high interference of the 2.4GHz, the WiFi community reached the 5GHz spectrum with the roll-out of the IEEE 802.11a/n technology. Recently the IEEE 802.11ac has been proposed to reach gigabit wireless links, yet considering a larger bandwidth of 80MHz and even 160MHz. Consequently, additional WiFi spectrum becomes necessary, and the ISM band, on which the IEEE 802.11p is located, naturally becomes a potential target. Yet, considering that WiFi is not used for safety-related wireless communications, its access to the ITS spectrum must be restricted.

Recently, considering the limited available spectrum at 5GHz, and the opportunity for WiFi to use the ITS spectrum when IEEE 802.11p does not use/need it, both the US Department of Commerce (US DOC) and the US Department of Transportation (US DOT) initiated a discussion on the potential coexistence of future WiFi and 802.11p technologies. A similar effort is currently under discussion by the European Communication Commission (ECC) and at the ETSI BRAN [1]. Regulators decided to allow WiFi to use the ITS bands, under the strict condition that 802.11p remains the primary user and WiFi should not cause harmful interference on 802.11p. The need for coexistence will primary be in urban environment, mostly due to the high density of indoor WiFi and even outdoor WiFi hotspots which may impact ITS safety at urban intersections and urban highways.

The coexistence mechanisms under consideration follow an *underlay* Cognitive Radio (CR) strategy as described in [2]. Cognitive Radio (CR) networks have been investigated in detail over the last decade. Besides the seminal work from Goldsmith et al. [2], Akyildiz et al. [3], [4] described main challenges behind Cognitive Radio (CR) from a hardware and protocol perspective. Detailed descriptions of the challenges and potential strategies may also be found in recent surveys [5], [6]. Several papers introduced enhanced or new WiFi MAC protocols supporting CR networks [7], [8]. And more recently, CR approaches applied to vehicular networks have also been proposed and discussed in detail in [9]–[13]. Yet, to the best of our knowledge, none of the previous work investigated the impact of ITS spectrum sharing from *standardized* cognitive WiFi algorithms on *safety-critical* ITS communications.

In this paper, we investigate two cognitive WiFi protocols for coexistence with IEEE 802.11p, very recently proposed by the WiFi community for standardization at ETSI [1]. We analyze these protocols from a vehicular communication point of view, focusing on their performance to prevent interference with cooperative awareness messages (CAM)[1]. More specifically, our contributions are: (i) formulation of the coexistence challenge between WiFi and IEEE 802.11p; (ii) description of the two spectrum sharing protocols proposed for standardization and presenting some of their issues; (iii) simulation-based evaluation of their interference prevention performance; (iv) suggesting improvements for better coexistence.

The rest of the paper is organized as follows: In Section II, we formulate the coexistence problem, while in Section III, we describe two coexistence protocols. Section IV provides evaluation results, while Section V concludes this work.

II. Problem Formulation

A. Spectrum Sharing

The necessity for coexistence in the 5GHz band is directly related to the scarce capacity left in this band. As illustrated in Fig. 1, on the lower part the 5GHz band is composed of multiple 20MHz WiFi channels, while on the upper part there are seven 10MHz IEEE 802.11p channels. With IEEE 802.11ac required support for 80MHz and 160MHz channels, a channelization extension has been proposed to have multiple 80MHz and 160MHz channels ranging from 5.4GHz up to

[1]Cooperative Awareness Messages (CAM) and their US counterparts Basic Safety Messages (BSM) are safety-critical messages.

978-1-5386-2723-5/17/$31.00 © 2017 IEEE

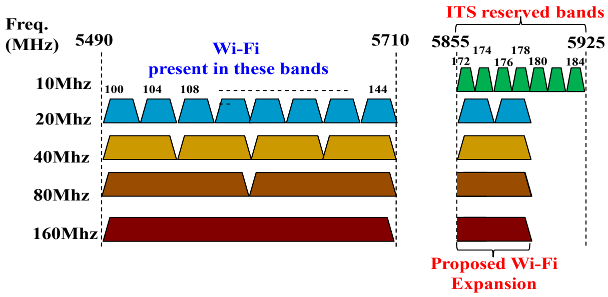

Fig. 1. WiFi & ITS Spectrum Sharing in 5.7 - 5.9GHz band

5.9GHz. Accordingly, the 70MHz ITS band will no longer be reserved for seven 10MHz channels, but will also include two 20MHz, or one 40MHz, or a part of 80MHz and 160MHz channels. WiFi not being capable of operating on 10MHz, IEEE 802.11p will need to share its spectrum with WiFi operating on larger bands.

B. Co-Existence Challenges

Both in Europe and USA, regulators agreed that due to the safety-critical nature of IEEE 802.11p traffic, it should remain the primary user of the coexisting band, and WiFi should follow a generic *detect-and-avoid* CR strategy to prevent harmful interference. Although originating from the same root, the coexistence between IEEE 802.11p and WiFi is not straightforward. Without loss of generality, we describe several challenges that need to be addressed for fair coexistence.

1) Physical Layer Challenges:

Reduction of Awareness: WiFi operates on 20MHz or wider channels while ITS-G5 channels are 10MHz. During Clear Channel Assessment (CCA), ITS-G5 or WiFi cannot decode each other's preamble at -85dBm in order to declare channel busy. Thus, ITS-G5 can assess the channel busy for a WiFi signal and vice versa only 20dB above this minimum sensitivity at -65dBm. Consequently, the ITS station needs to move much closer to WiFi in order to detect and be detected by WiFi, which corresponds to a loss of awareness.

Asymmetric Detection: As ITS-G5 cannot be modified to operate on 20MHz channels, WiFi coexisting with ITS-G5 has been proposed in the standard to have a 10MHz detector, which will enable WiFi to decode ITS-G5 preamble and detect channel busy at -85dBm. Nevertheless, WiFi will still remain **unilaterally hidden** to ITS-G5, unless the latter comes close enough to detect WiFi signal at -65dBm.

Figure 2 visually illustrates this asymmetric detection and unilateral hidden problem. It corresponds to an intersection, with a corner equipped with a WiFi Access Point (AP). As V1 approaches the WiFi AP, it moves through three zones, with different degree of visibility:

- **Zone 1:** both V1 and WiFi AP are too far and outside the detection range and may interfere with each other. Any other ITS station at the intersection with its minimum sensitivity of -92dBm for ITS-G5 signal, would be able to detect V1 in Zone 1. However WiFi with the -85dBm sensitivity of its 10MHz detector, cannot detect ITS stations in this zone.

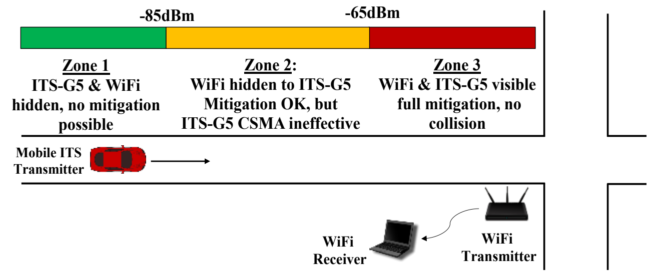

Fig. 2. Three Zones of visibility between ITS-G5 and WiFi

- **Zone 2:** the awareness range of WiFi starts from here so WiFi may detect ITS-G5 signal at -85dBm and engage a mitigation strategy (explained later). However V1 (with -65dBm CCA sensitiviy), yet cannot detect WiFi and will transmit ignoring WiFi transmissions. WiFi is unilaterally hidden to ITS-G5 and this zone is critical for coexistence.
- **Zone 3:** V1 is close enough to detect WiFi signal at -65dBm and assess the channel busy. Both WiFi AP and V1 are visible to each other, resulting minimum interference in this zone.

2) MAC Layer Challenges:

The CAM/BSM are the two major safety-related messages used by IEEE 802.11p. In both ETSI ES 202 663 [14] and SAE J2945/1 [15] standards, CAM/BSM are broadcast with the access category *Best Effort (AC_BE)*. This gives it a handicap when competing for the channel against high demanding unicast WiFi traffic, which can be on more stringent access categories, such as *Voice (AC_VO)* or *Video (AC_VI)*. Accordingly, CAM/BSM might either be delayed or lost due to WiFi packets.

To summarize, the problem deals with channel access contention between two types of transmissions. On one side there is WiFi, which is unicast with acknowledgment, can have higher EDCA priority, larger packet size, higher packet frequency compared to ITS-G5. Moreover, ITS-G5 significantly suffers from the loss of awareness when detecting WiFi signal. In spite of all these handicaps, ITS-G5 communication is for critical safety-of-life applications and has to remain the primary channel user, against infotainment WiFi communication.

III. WiFi Coexistence Proposals

Detect and Mitigate (DAM) and Detect and Vacate (DAV) are two coexistence protocols proposed in Europe by WiFi Industry for standardization at ETSI ITS and ETSI BRAN[2] [1].[3] For both these protocols, WiFi must have a 10MHz ITS-G5 detector per ITS channel, without any modification to ITS-G5 i.e. ITS-G5 cannot decode WiFi preamble and does not take any active part in these protocols.

A. Detect and Mitigate (DAM)

The basic principle of DAM is that once ITS-G5 is detected, WiFi uses higher EDCA parameters, and waits longer than ITS-G5 traffic of the same EDCA class before transmitting. Figure 3 demonstrates the behavior of this protocol as a state machine, as we interpreted it from the standard. It starts with a CCA by WiFi. If a WiFi device does not detect ITS-G5 signal, it can fully use the ITS-G5 channels using regular

[2]Detect and Vacate is also considered for coexistence in the US

[3]We describe and evaluate the latest version (v24) of the standard at the time of writing

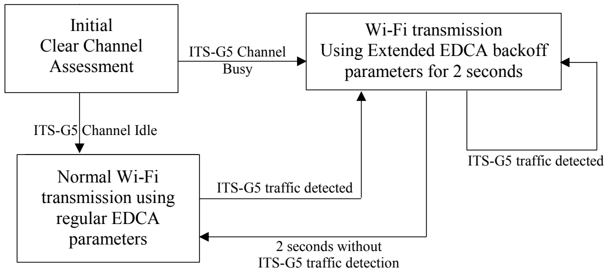

Fig. 3. Detect & Mitigate State Machine

IEEE 802.11a/n backoff parameters. If WiFi detects ITS-G5 traffic, it activates an extended EDCA mode by increasing the parameters of its own EDCA queues with higher backoff values (obligatory AIFS + random backoff), compared to ITS-G5, for at least 2s, and continues further if ITS-G5 is detected again during those 2 seconds.

There are two versions of DAM i.e. **Reduced** and **Absolute DAM**, and Table I shows both backoff values.

- **Reduced DAM**, ensures that WiFi performs an obligatory CCA via AIFS and random CW, for a period at least longer than the **AIFS+CWmin** of ITS-G5 traffic of the same EDCA class. For example, for class AC_VI ITS-G5 AIFS+CWmin is 3+7=10 slots, while in Reduced DAM mode, WiFi AIFS itself is 21 slots. The goal is to enforce a waiting time on WiFi longer than ITS-G5 CWmin, during channel contention and prioritize ITS-G5 packets.
- **Absolute DAM** prioritizes ITS-G5 even more. For each traffic class, it gives WiFi an AIFS longer than the **AIFS+CWmax** of ITS-G5 traffic of that class. For example class AC_VI of WiFi Absolute DAM mode has an AIFS of 3x2+CWMax = 1029 slots. This is to ensure that a WiFi node absolutely waits longer than ITS-G5, regardless of the ITS-G5 random backoff value between 0 & CWmax, which could be useful to prioritize unicast ITS-G5 packets with backoff > CWmin during retransmission.

Coexistence Limitations: Firstly DAM protocol suffers from the asymmetric detection limitation, as explained Section 2. Moreover, the aim of the extended backoff for WiFi in DAM mode is to ensure that WiFi traffic waits in the queue, longer than ITS-G5 traffic of the same EDCA class. However it does not provide such guarantee across different traffic classes. Therefore, when a ITS-G5 CAM of class AC_BE competes against DAM-enabled higher priority WiFi traffic of class AC_VI, WiFi traffic will be transmitted before ITS safety traffic. Similarly, if they both have the same AIFS + random contention window, a collision may still occur. Lastly, DAM only considers the presence of ITS-G5 traffic upon detection via CCA, and unlike DAV (explained next) doesn't consider a WiFi packet loss as a sign of ITS-G5 presence. Therefore

TABLE I
DETECT & MITIGATE EDCA PARAMETERS

AC	CW min	CW max	AIFSN (Reduced)	AIFSN (Abs)	TXOP Limit (Reduced)	TXOP Limit (Abs)
BK	31	2047	49	2065	2528 ms	2258 ms
BE	31	2047	43	2059	2528 ms	2258 ms
VI	15	31	21	1029	3000 ms	3008 ms
VO	7	15	11	515	2080 ms	1504 ms

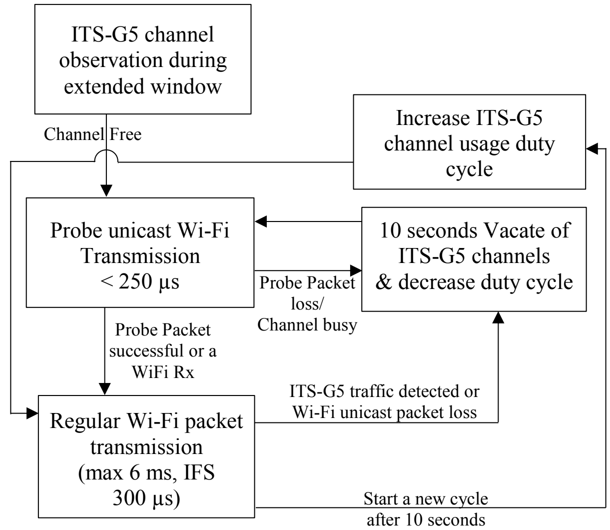

Fig. 4. Detect & Vacate State Machine

ITS-G5 packets may collide with WiFi packets, due to the unilateral hidden issue, and in such case a WiFi node in DAM mode will not identify the presence of ITS stations.

B. *Detect and Vacate (DAV)*

DAV protocol takes a more cautious approach when using the ITS channels by using longer initial observation period and probe packets. Figure 4 presents a simplified version of this protocol as a state machine, according to our interpretation of the standard. In order to transmit WiFi traffic, DAV requires to pass through the following states:

1) **Initial Extended Channel Observation –** the WiFi device senses ITS channels during an extended period, which could be as high as 30 minutes.
2) **Short Packet Probe –** If the ITS-G5 channel is idle during initial observation, it is probed for hidden ITS stations by a unicast short packet of $< 250\mu$sec.
3) **WiFi Packet transmission –** If the probe packet is acknowledged, WiFi uses ITS channels, limiting transmissions to < 6ms followed by a 300μsec AIFS.

Figure 5 shows an example of the different phases of DAV protocol. At any state, if an ITS-G5 transmission is detected or a WiFi unicast packet is unacknowledged, the WiFi device vacates the ITS channels for 10s. Moreover, each 10 seconds channel usage is considered as a cycle and a new cycle is started by updating the WiFi duty cycle limit of ITS channel usage i.e. the limit is increased if no ITS-G5 is detected in the last cycle. However we don't consider this duty cycle aspect in this paper. Our main focus is that once a WiFi device is in a state of ITS channel usage in regular mode, how effectively can the coexistence protocol detect a new ITS station and

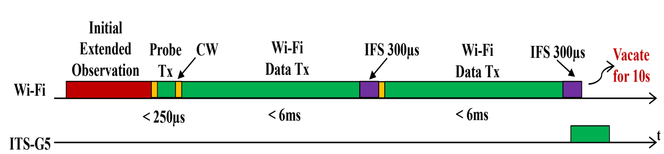

Fig. 5. Detect & Vacate phases of CCA and transmission

implement the coexistence mode to prevent interference with ITS-G5 communication.

Coexistence Limitations: Similar to DAM, DAV will also suffer from the limitation of asymmetric detection of ITS-G5 detecting WiFi at -65dBm. Secondly, although DAV considers a WiFi acknowledgment loss as an indication of ITS-G5 presence, but detecting a collision between WiFi and ITS-G5 can be difficult. ITS-G5 CAMs are broadcast without acknowledgment, so ITS stations cannot detect a collision. Although WiFi packets are mostly unicast, but the SINR at the WiFi receptor can be much higher than that at the ITS-G5 receptor, due to the shorter distance between WiFi nodes, static nodes and lower signal distortion compared to ITS-G5. So a collision between a CAM and WiFi packets could occur after which the WiFi packet could still be decoded, while the CAM being damaged beyond correction, causing DAV protocol to remain unaware of the collision.

IV. Performance Evaluation

We evaluate the DAM and DAV mechanisms on a simple urban intersection scenario with two WiFi and two ITS stations. We consider an urban scenario as WiFi is more densely deployed in cities, such as residential and commercial indoor WiFi and public outdoor WiFi hotspots. The first scenario is artificial and corresponds to the setup in Fig. 2 with a static ITS-G5 receiver placed at the intersection. The WiFi nodes are in Line of sight (LOS) to the ITS stations and there is log-distance attenuation without fading. This artificial scenario is used to analyze microscopically the asymmetric detection and unilateral hidden issue between ITS-G5 and WiFi as described in Section 2. The following scenario has two mobile ITS stations approaching an intersection and in LOS with WiFi, to simulate the coexistence with an outdoor WiFi hotspot. The last scenario simulates the same intersection, but with the WiFi nodes inside a building and in Non line of sight (NLOS) with the ITS stations, corresponding to indoor commercial or residential WiFi.

We use the iTETRIS simulator [16], which has a full ITS-G5 and WiFi protocol stack, which we modified to implement DAV and DAM. Table II shows the simulation parameters. We use the CAM Packet Reception Ratio (PRR) as the performance metric of the coexistence protocols, i.e. effective coexistence should not interfere with CAMs and result in high PRR. Metrics such as Inter Reception Time is also interesting

TABLE II
Simulation Parameters

Parameter	Value
Transmit Power	ITS-G5: 23 dBm, WiFi: 23dBm & 13dBm
Transmit Rate	ITS-G5: 10 [Hz] WiFi: ∼300 [Hz] @ 2250 [B] 5.4 [Mps]
Packet Transmit time	ITS-G5: 0.4 [ms] WiFi: 1.5, 2 & 3 [ms]
Preamble Detection Threshold	ITS-G5: -92 [dBm] WiFi: -85 [dBm], WiFi: -65 [dBm]
Mobility	Static & 10 [m/s]
EDCA queue	ITS-G5: AC_BE WiFi: AC_VO / AC_VI / AC_BE
Fading	Scenario 1: No fading Scenario 2&3: WINNER B1 Urban Microcell (Correlated Gaussian & Ricean)
Performance Indicators	Packet Reception Ratio (PRR) (95% Confidence Intervals – 1000 runs)

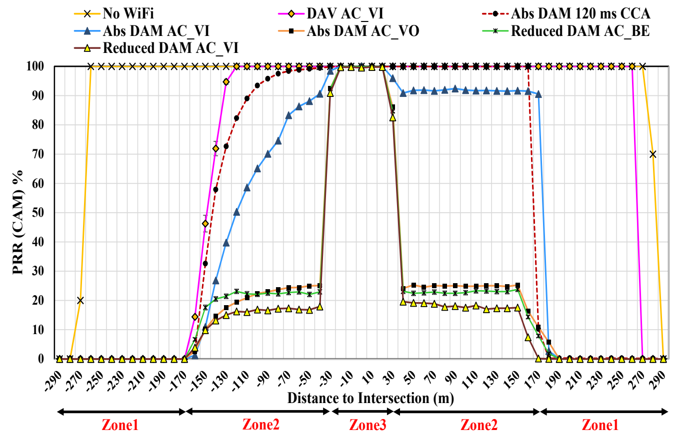

Fig. 6. CAM PRR for 3 Zones of Awareness

to analyze the effect of interference on ITS applications, but due to space limitation we leave it for future studies.

A. *Artificial Scenario: 3 Zones of Awareness*

Figure 6 illustrates the impact of WiFi on PRR of ITS-G5 CAM, for various WiFi mitigation mechanisms and traffic classes, as the ITS-G5 transmitter V1 in Fig. 2 approaches the WiFi AP through three zones. The negative and positive x-axis values are the positions of V1 before and after the intersection respectively. The curve without WiFi has the maximum PRR as there is no interfere to the ITS-G5 communication, with minimum sensitivity of -92dBm. For all other curves, when V1 is in Zone 1 (<-170m), it is hidden from the WiFi AP, which starts detecting ITS-G5 at -85dBm, as explained in Section 2. Similarly the WiFi AP is hidden to V1 in Zone 1, due to ITS-G5 detecting WiFi at -65dBm, so PRR is almost 0.

In Zone 2, V1 becomes visible to WiFi but not vice-versa. However, the switching to DAM or DAV mode by WiFi starts only when a CAM probabilistically coincides with a WiFi non-transmission period. This probabilistic coincidence results a gradual (not sharp) rise of CAM PRR, even if the attenuation is only log-distance without fading.

Unlike DAV, with DAM protocol WiFi doesn't sleep for 10s upon detecting ITS-G5, but transmits lesser than usual, using higher AIFS and backoff window. Reduced DAM performs the worst in Fig. 6, giving only ∼20% CAM success rate (PRR) in Zone 2. This low PRR doesn't improve much if WiFi transmits lower priority traffic of class AC_BE, so an increase in EDCA parameters for AC_BE is not significant to improve the performance of Reduced DAM. This is also the case with Absolute DAM class AC_VO, as even an AIFS of ∼4.6ms (515x9μs, ref Table 1) is not enough. Absolute DAM with class AC_VI, with ∼9ms AIFS (1029x9μs) performs better, but can't fully prevent CAM loss. The reason for this lack of effectiveness of DAM, even with higher AIFS, is that as the WiFi AP is unilaterally hidden to V1 in Zone 2, the long AIFS or backoff cannot guarantee that V1 will not transmit during a WiFi transmission. Nevertheless, a longer WiFi AIFS increases the probability that an ITS-G5 transmission will coincide with a WiFi non-transmission period and will not collide with WiFi.

In Zone 2, as WiFi has a better detection capability, the only way to fully prevent interference is that upon detecting the first CAM, WiFi should abstain and perform CCA **long enough** to detect the next ITS CAM. In Fig. 6 the curve

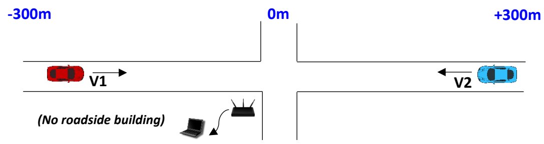

Fig. 7. Scenario Outdoor WiFi, ITS-G5 in LOS with WiFi

DAM absolute EDCA (120ms fixed CCA) is a hypothetical implementation to demonstrate this aspect. In case of 100ms periodic CAMs, 120ms WiFi CCA significantly improves the DAM performance. Unlike the 10s duration of DAV, DAM only lasts for 2s (if WiFi doesn't detect further ITS-G5), so WiFi returns to normal EDCA mode within 2 seconds of V1 quiting the WiFi detection range near +170m, whereas DAV continues channel vacate for 10 more seconds.

Finally as V1 enters Zone 3, WiFi is no longer hidden, so no interference may be observed. However, Zone 3 starts at 30m to the intersection, and is far too short for safety-related ITS applications. On the contrary, Zone 1 is too far away to affect such safety-related applications. Accordingly, Zone 2 remains the critical area, where DAM and DAV intend to ensure coexistence and prevent collision with ITS-G5 packets, which we analyze further in the next scenarios.

B. Scenario: Outdoor WiFi

This scenario has two ITS mobile nodes, both transmit and receive CAMs at 10Hz. The channel contains fading (WINNER B1; Gaussian Shadowing & Ricean fast fading). Figure 7 shows the setup, i.e. an intersection without buildings to simulate outdoor WiFi.

Figure 8 shows the CAM PRR (average of V1 & V2) for various mitigation techniques for outdoor WiFi. At any point, both vehicles are equidistant to the intersection. WiFi traffic of class AC_VI is only analyzed and presented on the graph for the sake of readability.

Unlike the last scenario, the receiver is now mobile and the maximum CAM PRR is governed by the distance between transmitters and receivers. The attenuation of WINNER LOS propagation is lower than th log-distance one, so the start of Zone 2 i.e. the WiFi awareness range stretches as far as -250m.

The PRR rises gradually for the different mitigation techniques, with Reduced and Absolute DAM resulting 10%$\sim$20% CAM loss in Zone 2, compared to the curve of CAM PRR with no WiFi, and reach even closer to the curve of no WiFi in Zone 3 starting at -50m, indicating an increase in PRR. The curves of Absolute DAM 120ms CCA and DAV follow the curve of CAM PRR with no WiFi, indicating their high effectiveness in preventing interference. Therefore, we can conclude that both the coexistence protocols perform relatively well in outdoor WiFi scenario.

C. Scenario: Indoor WiFi

In this scenario, the WiFi stations are inside a building, for NLOS propagation between WiFi and the ITS stations, as shown in Fig. 9. With indoor WiFi, in addition to the three zones, two other factors affect the CAM PRR, i.e. is the ITS receiver within the transmission range of the ITS transmitter and is the ITS receiver within the interference range of WiFi. This aspect can be explained via points **1 to 5** on the curve Reduced DAM in Fig. 10.

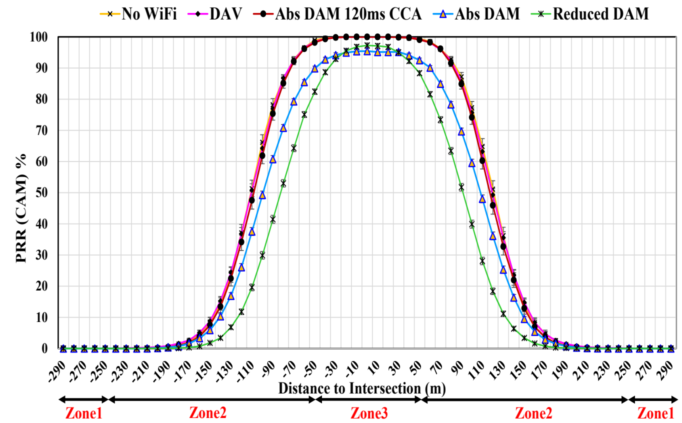

Fig. 8. CAM PRR for Outdoor WiFi

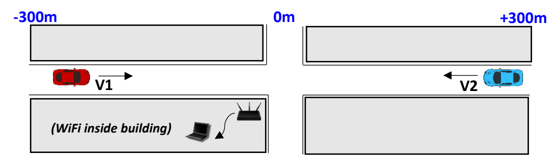

Fig. 9. Scenario Indoor WiFi, ITS-G5 in NLOS with WiFi

Point 1: The ITS receiver (either V1 or V2) is outside the transmission range of the transmitter (either V1 or V2), so low PRR due to strong attenuation (irrespective of WiFi). **Point 2:** The CAM PRR rises as the mobile ITS receiver comes inside the transmission range of the mobile ITS transmitter. Zone 2 starts at -70m and WiFi begins to detect ITS-G5, but Reduced DAM cannot fully prevent interference in Zone 2, as discussed earlier. **Point 3:** Unlike outdoor WiFi, the PRR doesn't always increase in Zone 2, but there is a dip in PRR as the ITS receiver moves more and more inside the interference range of the WiFi AP, i.e. the SINR of received CAMs decreases due to stronger interference from WiFi. This is the point of highest interference at around -30m. **Point 4 & 5:** The ITS stations move closer to the WiFi nodes and detect WiFi signal above -65dBm in Zone 3 at around -20m, causing a sharp rise in PRR.

Compared to outdoor WiFi, Zones 2 and 3 start later for Indoor WiFi as the awareness range of WiFi is attenuated by the walls. ITS stations have to come nearer and overlap with

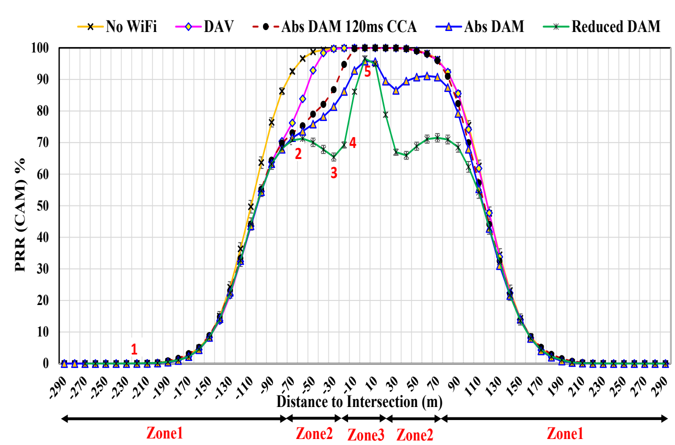

Fig. 10. CAM PRR for Indoor WiFi

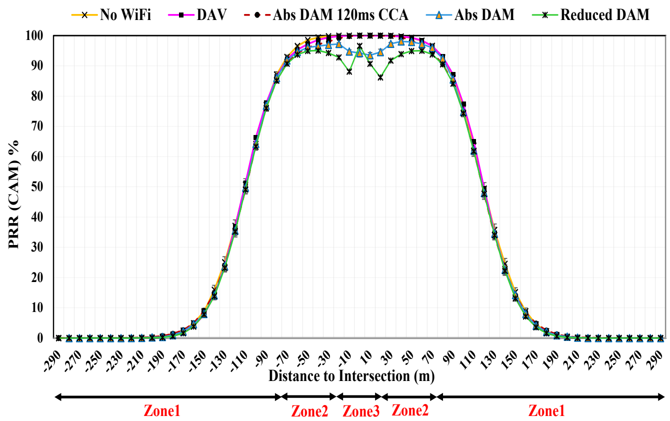

Fig. 11. CAM PRR for Indoor WiFi Reduced Power

a WiFi non-transmission period, in order for WiFi to detect ITS-G5 signal above -85dBm and apply DAM or DAV. Zone 2 starts at -70m, and different mitigation techniques vary in their level of performance, following the same trend as before. DAV gives the highest CAM PRR, followed by Absolute DAM 120ms CCA, then Absolute DAM and finally Reduced DAM produces the highest interference so lowest PRR.

This decrease in awareness range of indoor WiFi for detecting ITS stations and vice versa in NLOS condition is a significant challenge, regardless of the mitigation protocol. Reduced & Absolute DAM both create significant interferences in Zone 2, and even DAV causes interference, while 100% PRR is achieved not until Zone 3.

One aspect to notice is that beyond the generated interference, one may notice their spatial scales. All WiFi induced interferences occur in Zone 2, at distances below 70m for indoor WiFi, which corresponds to 3-5s drive time for 70km/h and 50km/h respectively. In both cases, that would lead to a too short detection time by any mobile vehicle to avoid a potential impact, which is not acceptable and needs to be improved.

Proposal - Reduce WiFi Transmit Power: One possible solution to counter loss of awareness from indoor WiFi is to decrease the WiFi Tx power. The CAM PRR for lower WiFi power i.e. 13dBm instead of 23dBm, is shown on Fig. 11. WiFi induced interferences follow similar trends for Absolute and Reduced DAM, but at a significantly higher CAM PRR compared to Fig. 10.

Similarly at reduced power, DAV does not generate almost any interference with ITS-G5. This is a clear indication that a reduction in WiFi power for indoor WiFi might be necessary to mitigate interferences with ITS-G5. The impact of such Tx power reduction on the WiFi performance remains to be evaluated, but is out of the scope of this paper, as we focus on ITS-G5 and it is not the role of ITS-G5 to maximize the performance of WiFi when using ITS-G5 channels.

V. Discussion and Conclusion

In this paper, we highlight the challenges of coexistence between IEEE 802.11p and WiFi on the 5.9GHz ITS band. We identify 3 zones of awareness relevant for coexistence, and find that at short distances between ITS transmitter and receiver, there isn't much problem of coexistence. At long distances, there is high ITS packet loss due to interference from WiFi, but long distances are not critical for safety related ITS applications. At medium distances, outdoor WiFi can coexist better than indoor WiFi, the latter creating non-negligible ITS CAM loss which can be problematic for ITS safety applications. We demonstrate that reducing indoor WiFi transmit power significantly improves the performance of the proposed coexistence protocols.

We observe that the coexistence protocol Detect and Mitigate faces performance issues, and we show that one way to improve its performance is that upon a single ITS-G5 packet detection, the WiFi channel non-usage time and CCA should be at least similar to the periodicity of ITS-G5 packets, in order to detect the presence of further ITS-G5 packets.

The CCA duration and abstention period can be optimized and adapted by WiFi through a cognitive process and we will look into this in our future work. We will also look into the effect of WiFi interference on ITS applications, such as the impact on breaking distance and other safety applications.

Acknowledgment

This work has been funded by the EU H2020 HIGHTS project (grant no. 636537). EURECOM acknowledges the support of its industrial members, namely, BMW Group, IABG, Monaco Telecom, Orange, SAP, ST Microelectronics, and Symantec.

References

[1] ETSI, "ETSI TS 103 319 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."

[2] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrum gridlock with cognitive radios: An information theoretic perspective," *Proceedings of the IEEE*, 2009.

[3] I. F. Akyildiz, W. y. Lee, M. C. Vuran, and S. Mohanty, "A survey on spectrum management in cognitive radio networks," *IEEE Communications Magazine*, 2008.

[4] I. F. Akyildiz, W. . Y. Lee, and K. R. Chowdhury, "Crahns: Cognitive radio ad hoc networks," *Ad Hoc Networks*, 2009.

[5] B. Wang and K. J. R. Liu, "Advances in cognitive radio networks: A survey," *IEEE Journal of Selected Topics in Signal Processing*, 2011.

[6] E. Z. Tragos, S. Zeadally, A. G. Fragkiadakis, and V. A. Siris, "Spectrum assignment in cognitive radio networks: A comprehensive survey," *IEEE Communications Surveys Tutorials*, 2013.

[7] S. C. Jha, U. Phuyal, M. M. Rashid, and V. K. Bhargava, "Design of omc-mac: an opportunistic multi-channel mac with qos provisioning for distributed cognitive radio networks," *IEEE Trans. Wireless Commun*, 2011.

[8] J. Jia, Q. Zhang, and X. S. Shen, "Hc-mac: A hardware-constrained cognitive mac for efficient spectrum management," *IEEE Journal on Selected Areas in Communications*, 2008.

[9] K. D. Singh, P. Rawat, and J.-M. Bonnin, "Cognitive radio for vehicular ad hoc networks (cr-vanets): approaches and challenges," *EURASIP Journal on Wireless Communications and Networking*, 2014.

[10] S. Chen, A. M. Wyglinski, M. Advisor, W. Ece, K. Pahlavan, P. C. Pedersen, and S. K. Jayaweera, "Vehicular dynamic spectrum access: Using cognitive radio for automobile networks," 2013.

[11] N. Cheng and X. Shen, *Opportunistic Spectrum Utilization in Vehicular Communication Networks*, 2015.

[12] M. D. Felice, K. R. Chowdhury, and L. Bononi, "Analyzing the potential of cooperative cognitive radio technology on inter-vehicle communication," in *Wireless Days*, 2010.

[13] M. Di Felice, R. Doost-Mohammady, K. R. Chowdhury, and L. Bononi, "Smart radios for smart vehicles: cognitive vehicular networks," *IEEE Veh. Tech. Mag*, 2012.

[14] ETSI, "ETSI ES 202 663 intelligent transport systems (its); european profile standard for the physical and medium access control layer of intelligent transport systems operating in the 5 ghz frequency band."

[15] SAE, "SAE J 2945/1 on-board system requirements for v2v safety communications."

[16] M. Rondinone et al., "itetris: A modular simulation platform for the large scale evaluation of cooperative {ITS} applications," *Simulation Modelling Practice and Theory*, 2013.