Journal of
Sensor and Actuator Networks

MDPI

Article

Wi-Fi Direct Performance Evaluation for V2P Communications

Thales Teixeira de Almeida [1,2], José Geraldo Ribeiro Júnior [2], Miguel Elias M. Campista [1] and Luís Henrique M. K. Costa [1,*]

[1] Federal University of Rio de Janeiro—UFRJ—PEE/COPPE-DEL/Poli-GTA, Av. Athos da Silveira Ramos 149, Rio de Janeiro 21941-972, Brazil; almeida@gta.ufrj.br (T.T.d.A.); miguel@gta.ufrj.br (M.E.M.C.)

[2] Federal Center for Technological Education of Minas Gerais—CEFET-MG—DCMLP, R. José Péres 558, Leopoldina 36700-001, Brazil; junior@cefetmg.br

* Correspondence: luish@gta.ufrj.br; Tel.: +55-21-3938-8635

Received: 3 April 2020; Accepted: 1 June 2020; Published: 6 June 2020

Abstract: The high cost of IEEE 802.11p-compliant devices and the lack of a widely adopted standard motivate the search for alternative methods for vehicular communication. As a consequence, and due to the ubiquity of smartphones, we see an increasing number of proposals based on Wi-Fi Direct, especially related to the integration of pedestrians in VANETs. Nevertheless, given the complexity of real experimentation, it is difficult to assess the ability of Wi-Fi Direct to offer connectivity in the vehicular environment on a large scale, leading to the evaluation through simulation. In order to verify the ability of a simulation model of reproducing the Wi-Fi Direct behavior, we analyze the performance of a safety application based on the communication range, packet delivery rate, and packet inter-reception time. In V2P scenarios, with and without line of sight, with varying vehicle speed, measurements using smartphones are performed and their results compared with those of OMNeT++ simulator. The results indicate, apart from the simulator's accuracy, that the connection establishment time hinders the use of Wi-Fi Direct as a replacement to 802.11p. As an outcome of this observation, we evaluate a new transmission method for Wi-Fi Direct based on beacon stuffing, which mitigates the long connection establishment issue.

Keywords: VANETs; vehicular networks; connected vehicles; Wi-Fi Direct; Wi-Fi P2P; IEEE 802.11p; INET; OMNeT++

1. Introduction

According to the World Health Organization (WHO), traffic accidents are now the eighth cause of deaths in the world, and the main cause among young people aged from 5 to 29 years [1]. In 2018 only, about 1.35 million people died due to injuries caused by traffic accidents. More than 50% of all deaths caused by traffic accidents are among so-called VRUs (Vulnerable Road Users), the group formed by pedestrians, cyclists, and motorcyclists. This problem is even more serious in low and middle-income countries. Despite concentrating 60% of the car fleet, these countries account for more than 90% of fatal traffic accidents. The road infrastructure in these countries is directly associated with these fatalities, as many roads do not have exclusive lanes for cyclists or even suitable pedestrian crossings, in addition to allowing very high speed limits. In fact, 88% of pedestrians travel on unsafe roads and the risk of death of a pedestrian after being hit increases by about 4.5 times if the vehicle speed goes from 50 to 65 km/h. Besides that, it is important to consider the unbridled use of smartphones during the pedestrian trajectory along the road, the distraction of which motivates the development of an exclusive alert system for such users [2].

As one of the consequences, research involving VANETs (Vehicular Ad-hoc NETworks) has become increasingly important. Using OBUs (On-Board Units) installed inside the vehicles, it is possible to increase the traffic safety through the exchange of CAM (Cooperative Awareness Messages) [3] and DEN (Decentralized Environmental Notifications) messages [4], transmitted to propagate the environment state and emergency situations. This message exchange is supported by IEEE 802.11p [5], a standard specifically designed to support communication in the vehicular environment, but which is struggling to be widely deployed [6]. This difficulty is mainly due to the lack of a widely adopted communication standard (there are differences between the European, Japanese, and American standards) and the high cost of compliant devices. As 802.11p requires vehicles to be equipped with dedicated hardware, a large initial investment is required [7], hindering penetration in low and middle-income countries. Moreover, to enable the detection of pedestrians on the road and avoid accidents, a periodic safety message exchange via V2P (Vehicle-to-Pedestrian) communication is required. Nevertheless, up to now, no smartphone or other device used in the VRU context supports 802.11p natively [8], motivating the search for alternative communication methods in VANETs.

Estimations state that 44.9% of the global population will have a smartphone in 2020 [9]. Due to the high penetration, versatility, and ubiquitous nature of smartphones, the network technologies embedded in these devices are considered communication alternatives to 802.11p. In addition to accelerating the adoption of VANETs, such devices enable the integration of different VRUs into the vehicular context. For example, in the study carried out in [8], 82% of the surveyed V2P communication systems use the smartphone as a VRU device. Through sensors such as accelerometer, gyroscope, and GPS, it is possible to collect geographic coordinates, speed, and travel direction of vehicles and VRUs, making it possible, for example, to predict the collision between a vehicle and a pedestrian carrying a smartphone. With respect to data sharing, communication technologies such as NFC (Near Field Communication), BLE (Bluetooth Low Energy), 4G/5G cellular networks and Wi-Fi Direct are the main candidates. Introduced in 2010 by the Wi-Fi Alliance (https://www.wi-fi.org/wi-fi-direct) and available for Android since version 4.0 (Ice Cream Sandwich), Wi-Fi Direct is the one showing the best benefit so far.

While Wi-Fi Direct has a theoretical communication range of 200 m [10], BLE can send data only at distances ranging from 60 to 100 m [11]. NFC is not even considered, as its communication range is $<$10 cm [12]. Since the reception of CAM messages is generally not required over large distances [13], the communication range of 200 m of Wi-Fi Direct meets the requirement of some VANET safety applications [14], especially in the VRUs context. Besides that, on Wi-Fi Direct, it is possible to send data at 250 Mbps PHY rate, as opposed to BLE that supports only 1 Mbps [15]. Compared to cellular networks, since the devices communicate directly, the end-to-end delay on Wi-Fi Direct is smaller than with 4G [16], which does not meet the requirements of safety applications [17]. Despite the potential for C-V2X (Cellular V2X) as part of 5G, currently there are no estimates for the use of this technology in a V2P system [8]. On the other hand, Wi-Fi Direct is present in most smartphones. This fact allows the immediate adoption of VANETs, something that is not expected for 802.11p or 5G. In addition, with respect to the minimum size of a CAM message (50 bytes), and that a safety application has a typical transmission frequency of 10 Hz, a load of 1.72 MB per hour would be generated. In the case of cellular networks, the cost to the user and the overhead of the cellular network need to be considered.

Despite its benefits, Wi-Fi Direct has a major limitation: the long Connection Establishment Time (CET, for short), which makes the use of this technology in the vehicular environment challenging. Different works have been proposed to reduce the CET of Wi-Fi Direct [18–20], which can reach 15 s [21]. Since the contact time among vehicles can be very short, a CET of 15 s can prohibit the use of Wi-Fi Direct in the vehicular environment. Therefore, solutions that eliminate or minimize the CET of Wi-Fi Direct are required to allow the use of this technology in VANETs. Moreover, as Wi-Fi Direct was designed for stationary environments [16], it is mandatory to analyze the CET performance in mobility scenarios. One must investigate whether the speed of vehicles is capable of impacting the

communication—and, consequently, the CET—due to the Doppler shift. Moreover, it is necessary to evaluate the capacity of Wi-Fi Direct to provide communication in a realistic scenario. Nevertheless, due to the high cost and complexity of carrying out real experiments in VANETs, it is difficult to predict whether Wi-Fi Direct will be able to offer connectivity for large-scale operation, meaning that its viability must be assessed through simulation. In this case, model simplifications and unforeseen conditions can produce differences between the results obtained with synthetic simulations and those from real experiments.

In order to analyze the viability of using Wi-Fi Direct in the vehicular environment, this paper investigates the impact of CET in mobility scenarios. Based on the periodic exchange of safety messages, Wi-Fi Direct performance is evaluated through real measurements using commercial smartphones and simulations using the simulation model of Wi-Fi Direct [22] available on framework INET (https://inet.omnetpp.org/), from the popular OMNeT++ simulator (https://omnetpp.org/). In V2P communication scenarios, with LoS (Line-of-Sight) and NLoS (Non-Line-of-Sight) conditions, the communication range, PDR (Packet Delivery Rate) and PIR (Packet Inter-Reception time) are evaluated. The impact of different speeds employed by the vehicle is also investigated. The results confirm that the long CET is an obstacle to Wi-Fi Direct as an alternative to 802.11p, especially in NLoS conditions.

To work around this problem, based on the beacon stuffing method originally proposed in [23], we evaluate a new transmission method for Wi-Fi Direct that does not require granting root privileges to operate. For example, the ad hoc mode enables the immediate transmission of packets in broadcast. Nevertheless, as opposed to Wi-Fi Direct, the ad hoc mode is not natively supported by Android smartphones. For security reasons, these devices must first be granted root privileges. The obtained results of the new transmission method for Wi-Fi Direct indicate a good potential to support communication among vehicles and VRUs in NLoS conditions. As this transmission method is evaluated by simulations, another goal of this paper is to investigate the ability of the model of Wi-Fi Direct available on INET to mimic our experimental scenario. Comparing the results of real measurements with those obtained by such a simulation model, it is possible to provide trustworthiness to the results obtained by simulations, thus enabling the evaluation of Wi-Fi Direct for large-scale operation in VANETs. To the best of our knowledge, this is the first paper that compares the performance of Wi-Fi Direct in the real vehicular environment with that obtained by the simulation model available on INET [22].

This paper is organized as follows: Section 2 presents the operation of connection establishment in Wi-Fi Direct in detail, while Section 3 presents related work. Section 4 describes the CET evaluation scenarios, in addition to the details of real experiments and simulations. Section 5 compares and discusses the results of the evaluation of CET in mobility scenarios, and Section 6 demonstrates the transmission method proposed. Finally, Section 7 concludes the paper and indicates future work directions.

2. Wi-Fi Direct Background

In the current section, the process of establishing the connection in Wi-Fi Direct is presented in detail. The idea is to identify the main challenges concerning Wi-Fi Direct adoption in mobile scenarios. Figure 1 illustrates the Wi-Fi Direct device discovery.

The connection establishment is composed of two main procedures: device discovery and group formation. In the device discovery, the goal is to detect other nodes within the communication range. This is done in two phases: Scan and Find. During the Scan phase, the device senses all available channels (1 to 13) for other nodes, groups, or traditional Wi-Fi networks. In the Find phase, the node transmits (Search) Probe Requests on the social channels (1, 6 and 11), and listens (Listen) to one of these channels waiting for Probe Requests. The nodes alternate between the social channels defined in the Search and Listen steps, persisting a certain time (100, 200 or 300 ms) on each channel, until they discover another node. The connection is established only when two nodes synchronize on the same

channel. For example, in Figure 1, node A discovers node B only when node A transmits Probe Requests on channel 6, which had been selected by node B in the Listen step. This is the main cause of the long delay in the connection establishment time.

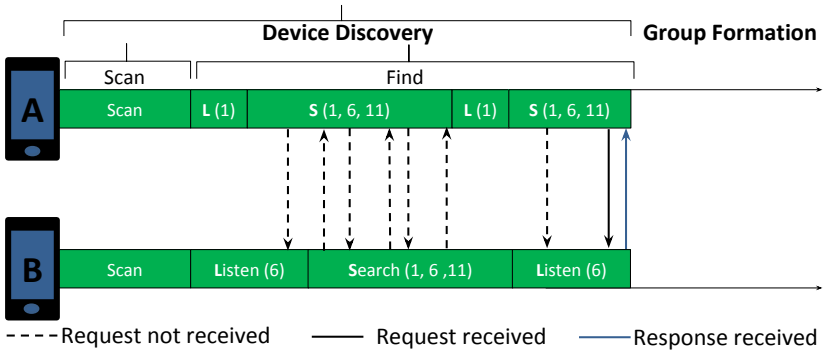


Figure 1. Wi-Fi Direct device discovery—adapted from [12].

After discovering devices, the nodes are able to form a communication group, equivalent to a BSS (Basic Service Set) of IEEE 802.11, which can be of three types: Standard, Autonomous and Persistent. In Standard Groups, the nodes negotiate which of them will play the role of GO (Group Owner), similar to the Wi-Fi access point. This is done by sending a random number, called Intent Value, which measures the willingness of the node to become the GO. The node whose Intent Value has the highest value will be defined as GO. In the case of two nodes having set the same value, a tiebreaker bit is included in the frame exchanged in the GO negotiation. In Autonomous Groups, a node announces itself as GO by sending beacons. Finally, Persistent Groups reactivate a group that has existed before, with each node playing the same role it played in the previous group. The last step concerns the establishment of a secure connection among the nodes through WPS (Wi-Fi Protected Setup). This is required to enable data exchange.

The transmission method based on beacon stuffing [23] minimizes the effect of the long CET of Wi-Fi Direct, since it enables the opportunistic sending of the safety message content (latitude, longitude, speed and travel direction) in the beacons announced by the GO after the creation of the Autonomous group. Section 6 presents more details about the transmission method proposed.

3. Related Work

As mentioned in Section 1, many studies involving Wi-Fi Direct are proposed to reduce the CET. To a lesser extent, others aim to analyze the behavior of this technology in VANETs. In the current section, these studies are classified, and the relation with our work, discussed.

3.1. Wi-Fi Direct Performance Evaluation

In order to analyze the delay in the formation of Wi-Fi Direct groups, Camps-Mur, et al. [21] present the first performance analysis of Wi-Fi Direct through real experiments and simulations, performed on the NS-3 software [24]. The results show that the delay in device discovery is similar for Standard and Persistent groups, whereas the Autonomous group obtains the shortest delay. To form the group, the Persistent group is the one that obtains the best performance in term of delay. Since the simulations do not consider interference, they do not reproduce the real experiments. It is worth mentioning that NS-3 does not have Wi-Fi Direct modules, being compatible only with ad hoc mode. The authors do not mention any adaptation of this module. Balasundram et al. [7] compare the performance of Wi-Fi Direct and 802.11p through simulations performed on NS-3. Since NS-3 does not have Wi-Fi Direct modules, IEEE 802.11a is used. In the simulations, the group formation is not considered. The PDR indicates that, in Wi-Fi Direct, the loss increases with the distance between the nodes. As for the throughput, it decreases with the distance between nodes. The nodes are able to communicate up to

300 m away, which conflicts with the maximum range of Wi-Fi Direct (200 m) and may be associated with the use of 802.11a. In multi-hop transmission, the average end-to-end delay on Wi-Fi Direct is higher than on 802.11p, while the PDR is lower. Lastly, the speed of vehicle does not impact the PDR. This result may be associated with the fact that the propagation model defined in the NS-3 does not consider mobility.

We note that some studies involving Wi-Fi Direct in VANETs are based on simulations, which may not accurately reproduce the real world. To fill this gap, the present paper analyzes the ability of the Wi-Fi Direct simulation model implemented by INET to mimic the real world, enabling the evaluation of this technology on a larger scale.

3.2. Wi-Fi Direct Delay Reduction

Jeong et al. [12] propose the use of Wi-Fi Direct and 4G cellular networks to minimize the device discovery delay. In the proposal, through the 4G network, each node is responsible for sending its current geographic coordinates and speed to a server. The server then sends a request for the nodes to start group formation on Wi-Fi Direct, whenever the distance between them is less than 200 m. The experiments are carried out using vehicles that travel at 20 and 30 km/h. The results indicate that the proposal is able to reduce the device discovery delay from 1.5 s to 100 ms. In the GO disconnection scenario, the reduction is from 3 s to 200 ms. Nevertheless, the authors do not consider the impact of NLoS conditions (obstacles). Manamperi et al. [25] propose a new transmission method among the GO and other members of the group to minimize the transmission delay and enable the use of Wi-Fi Direct in VANETs. Replacing the P2P (Peer-To-Peer) model, the proposal determines that, after receiving the frames transmitted by the members of the group, the GO must aggregate these frames in a single frame and then send to all the members via broadcast. As in the present paper, the authors evaluate the transmission method using the Wi-Fi Direct simulation model available on INET [22]. The speed of vehicles is defined as 80 and 120 km/h. The proposed method reduces the total average delay compared to P2P mode, despite the increase of members in the group leading to a reduction in the delivery rate. It is worth noting that some parameters of the simulation are not realistic, such as the value defined for the loss exponent of the propagation model. Shahin et al. [26] propose to incorporate an alert message in the frame of the optional Wi-Fi Direct service discovery mechanism. In the proposal, it is not necessary to be a member of a group to transmit data. Based on the publish/subscribe model, nodes interested in receiving alerts send a request to other nodes that have stored alerts, which transmit the alerts after receiving the request. The authors have implemented the proposed method in real devices. Although the validation of the method has been performed, the use in the real world has not been discussed by the authors. Moreover, the publish/subscribe model is not suitable for safety applications, because the lack of periodic safety messages reduces the situational awareness.

In comparison with the before aforementioned work, the present paper evaluates a transmission method based on beacon stuffing [23], which reduces the delay of device discovery. This transmission method enables the periodic safety message exchange. Consequently, situational awareness is increased. Besides that, the problem imposed by the long CET of Wi-Fi Direct is minimized, with no need to integrate cellular networks or use the optional service discovery method.

3.3. Wi-Fi Direct Security Systems

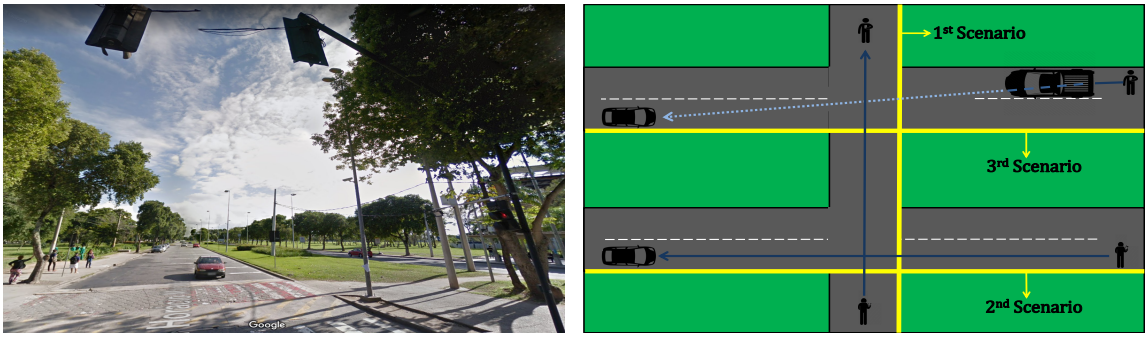
Dhondged et al. [27] propose WiFiHonk, a security system that alerts collisions among vehicles and pedestrians. Despite using Wi-Fi, WiFiHonk does not require association and authentication. Using beacon stuffing, alerts based on geographic coordinates, speed, and travel direction are inserted in the 32-byte field of the SSID (Service Set IDentifier) or of the BSSID (Basic Service Set IDentifier) of beacons. The method periodically transmits the modified beacons every 100 ms, allowing them to be passively inspected by the hotspot (on Wi-Fi) or the device discovery (on Wi-Fi Direct). In mobility conditions, the authors compared WiFiHonk with Wi-Fi Direct. Whereas WiFiHonk is able to successfully delivery at least one message to the receiver, even in conditions of high mobility (up to 112 km/h), Wi-Fi Direct

fails to deliver messages at speeds above 24 km/h due to the long CET. It should be noted, however, that modifying beacons of Wi-Fi access points requires root privilege, which makes the solution difficult to deploy in the real world. Won et al. [28] propose a system for propagating safety messages and monitoring the risk of collisions among vehicles and pedestrians via Wi-Fi Direct. After detecting a screen view during the pedestrian's route near the crosswalk, the system creates an Autonomous group among the pedestrian (GO) and the vehicles. The nodes then exchange messages containing the time to reach the crosswalk. Upon receiving the message, the system in the pedestrian side calculates the collision probability. If there is a risk of collision, an alert is sent. In the assessment, the authors do not consider the CET. Under LoS conditions, the authors measure the communication range based on the PDR and the end-to-end delay based on the RTT (Round-Trip-Time). The results indicate that PDR is >80% over distances <70 m, and the RTT is between 100 and 200 ms. The lower the speed of the vehicle, the greater the chance of avoiding an accident. Lastly, despite small losses, in general the vehicle speed has little impact on the PDR.

Similar to the above-mentioned studies, our goal is to analyze the feasibility of Wi-Fi Direct in providing connectivity in the context of safety applications and VRUs. For this purpose, high speeds, NLoS conditions as well as the impact of CET are considered. Besides that, based on the evaluation of the NLoS scenario, a transmission method based on beacon stuffing [23] is also evaluated. Nevertheless, no root privileges are required.

4. Wi-Fi Direct Experimental Scenarios

In this work, we conducted real and simulation experiments to, first, evaluate the impact of the CET in V2P scenarios and, second, to evaluate the improvements achieved with the use of beacon stuffing [23]. In the real experiments, the performance analysis of Wi-Fi Direct is evaluated taking into account a pedestrian carrying a smartphone (as a member of the communication group) as well as a vehicle containing a smartphone (GO). The same elements are modeled in the framework INET of OMNeT++. The assessment scenarios are based on a signalized road (Figure 2a), where pedestrians can cross while vehicles wait for the traffic light to go green. In the real world, in many countries, pedestrians crossing with the traffic light green to vehicles is a common situation, which puts pedestrians and drivers at risk. Over 80% of fatalities involving pedestrians occur during a crossing attempt [29]. This situation is impaired by obstacles, such as a bus collecting passengers, since most VRU detection systems (such as sensors and cameras) require LoS conditions to work properly [30]. In the case of VANETs, obstacles lead to the obstruction of the radio signal propagation. Besides that, there is also the blocking of the pedestrian's visual field, who may not perceive the arrival of vehicles when trying to make the crossing with the traffic light open. In this context, three scenarios are defined, as Figure 2b illustrates.



(**a**) Signalized road at Federal University of Rio de Janeiro. (**b**) Situations evaluated in the experimental scenario.

Figure 2. Example of a real scenario and assessed situations.

1st Scenario—Real Communication Range (LoS): in addition to analyzing the range obtained by Wi-Fi Direct in the real world, the main goal of this scenario is to be used as a reference for the

calibration step of INET propagation model, that is, to approximate the simulated environment to the real one using the results of real communication range as a reference. In this scenario, after the connection is established, two static pedestrians, carrying smartphones, communicate with each other via safety messages, hereafter defined as BSMs (Basic Safety Messages), a type of CAM message defined in the SAE J2735 standard. The assessment is based on the transmission of a series of 500 BSMs at each 10 m road segment. After transmitting 500 BSMs, the transmitter is positioned 10 m away from the receiver, and the procedure is repeated until the devices are 150 m away.

2nd Scenario—Mobility Impact (LoS): assesses whether vehicle mobility impacts Wi-Fi Direct performance. With the pedestrian standing still and her smartphone transmitting BSMs continuously, the vehicle approaches at different speeds, varying between 20, 60, and 100 km/h. Starting its route 500 m away, the vehicle enters the pedestrian's communication range with the desired cruise speed. The goal of this scenario is to investigate if the Doppler shift impacts the communication and, consequently, the CET. As opposed to the 1st Scenario, the number of BSMs transmitted is not fixed. All transmissions performed during the route of the vehicle are accounted for, with PDR and PIR being calculated every 20 m.

3rd Scenario—Mobility Impact (NLoS): in order to analyze the impact of NLoS conditions on CET, caused by the obstruction of the radio signal propagation in the current scenario, a large vehicle (with no communication ability) is inserted between the pedestrian and the vehicle that plays the role of GO. In a realistic environment, it is not possible to ensure the line of sight during nodes communication. In the real world, the signal propagation can be affected by trees, buildings or vehicles. In this case, it is necessary to assess whether the BSMs will be able to alert the vehicle about the inappropriate crossing of a pedestrian, whose visual field is obstructed by the obstacle. The transmission method based on beacon stuffing [23] is evaluated for Wi-Fi Direct, especially, for operation in these conditions.

The performance analysis of Wi-Fi Direct in VANETs is based on PDR and PIR. The PDR indicates the percentage of BSMs successfully received, whereas the PIR measures the time interval between two successful receptions, which translates to the level of situational awareness of the node. Through the received BSMs, the vehicle is able to know the geographic coordinates, speed and travel direction of VRUs. The PIR analysis is essential to indicate long periods with no communication. The greater the situational awareness, the shorter the reaction time required under a dangerous condition. Table 1 summarizes the main characteristics of the assessment scenarios.

Table 1. Summary of assessment scenarios.

Scenario	Goal	Condition	Ped. Speed	Veh. Speed	PHY Rate
1st	Analyze the real range	LoS	0 km/h	—	250 Mbps
2nd	Analyze the mobility impact	LoS	0 km/h	20–60–100 km/h	250 Mbps
3rd	Analyze the mobility impact	NLoS	0 km/h	20–60–100 km/h	250 Mbps

4.1. Real Experiments Setup

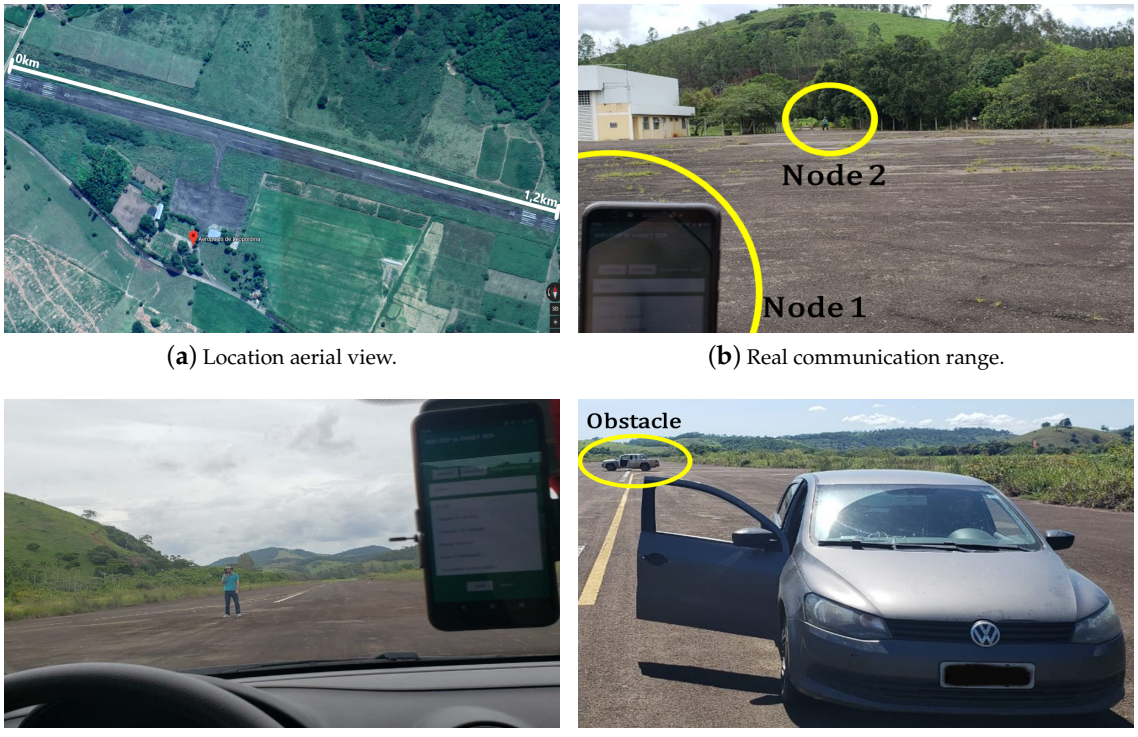
In our real experiments, we use two commercial smartphones: (1) Xiaomi MI A2, Octa-Core processor of 2.0 GHz and 4.0 GB of RAM, inside the vehicle and acting as GO; and (2) Asus Zenfone Live L1, Octa-Core processor of 1.4 GHz and 2.0 GB of RAM, in use by the pedestrian and acting as a member of the communication group. The height of the smartphone inside the vehicle in relation to the ground was approximately 1.3 m, whereas with the pedestrian it was around 1.6 m. Android versions used are 9.0 One Pie (API 28) for Xiaomi, and 8.0 Oreo (API 26) for Asus.

Once the goal is to analyze the Wi-Fi Direct performance with respect to networking aspects, there is no need to select the node in the smartphone screen to establish the connection. Consequently, the delay based on the user's interaction with the screen is not considered in all experimental scenarios. This is performed by calling the Wi-Fi Direct connection method within the method named `PeerListListener` (https://developer.android.com/reference/aandroid/net/wifi/p2p/WifiP2pManager.PeerListListener), passing the node ID that plays the role of GO as a parameter.

The `PeerListListener` method is responsible for showing on the screen the list of devices discovered on the network and that are available for establishing the connection. The same is done in relation to the transmission of BSMs. By creating a UDP socket, as soon as the group is formed, the member of the group transmits BSMs to the GO. This way, the user does not need to interact with the application to start the transmission of BSMs.

As mentioned in Section 1, the exchange of BSMs aims to disseminate the environment state. Each BSM is composed by latitude and longitude of the node—obtained through GPS with an update frequency of 1 Hz—its current speed, travel direction, and timestamp of the information. Security systems require lane-level positioning accuracy (2.5 and 3.5 m) [31], whereas in the real world, the accuracy obtained by GPS can reach 10 m [29]. Some studies have shown that it is possible to improve the accuracy of GPS embedded in smartphones, obtaining an accuracy of up to 30 cm [32]. The data processing for increasing the GPS accuracy, however, is not the focus of the present paper.

Other parameters of the real experiment that must be noted are as follows. With 80 bytes, the BSMs are transmitted periodically every 100 ms. It should be noted that the windows of the vehicle remained closed during the communication with the pedestrian. The real experiments were carried out in a deactivated airport located at Leopoldina—MG, Brazil. Because it is located in a rural area, this place does not receive interference from cellular or Wi-Fi networks, making it ideal for carrying out the real experiments. Besides that, as it is located in a predominantly open area without buildings, the evaluation under LoS conditions is possible. Figure 3a shows the aerial view of the airport, while Figure 3b–d show the devices used and the evaluation in progress, respectively.



(**a**) Location aerial view.

(**b**) Real communication range.

(**c**) Mobility impact (LoS).

(**d**) Mobility impact (NLoS).

Figure 3. Location of the experiments and evaluation in progress.

4.2. INET/OMNeT++ Simulation Setup

The simulations are based on the Wi-Fi Direct module available on INET [22], where both vehicle and pedestrian are modeled as nodes with a Wi-Fi Direct interface. Based on OMNeT++—a popular event-driven network simulator—INET is responsible for providing protocols, agents and application models to be used in the simulation. Protocols such as UDP (transport layer), IPv4 (network layer),

802.11 (link layer), as well as an application model for generating UDP traffic, are defined in the network nodes. INET also allows modeling physical layer phenomena, such as radio interference and noise—which supports the decision whether the frame will be decoded based on noise level and bit error probability—as well as environmental factors, such as shadow zones caused by obstacles and the radio signal attenuation based on the propagation model.

As in real experiments, in simulations, BSMs are 80 bytes long and are sent every 100 ms. In both nodes, an application that generates UDP traffic is defined. Based on the Asus Zenfone [33]—the device that acts as the transmitter in real experiments—the transmission power is defined as 13.90 dBm. Based on the configuration proposed in [34] for VANET simulations, the background noise is defined as −98 dBm. The data rate is defined as 54 Mbps (IEEE 802.11g), with constant propagation delay. The frame retransmission is disabled. The `LogNormalShadowing` propagation model is chosen to simulate the radio signal attenuation. In the present paper, the `LogNormalShadowing` is the model that best reproduced the real experiments. At first, simulations were performed using `TwoRayInterference` propagation model. Nevertheless, even adapting the parameters associated with the dielectric constant to different values, the PDR was always 100% in the calibration step. The calibration step is necessary to approximate the simulated environment to the real one using the results of the real communication range as a reference. In the `LogNormalShadowing`, the parameter alpha is set to 2.21. In the literature, this value varies between two and six, where two represents the propagation in free space [35]. The parameter alpha is defined in the calibration step of simulations, as described in Section 4.

For the NLoS scenario, an obstacle is inserted simulating a bus stopped between the vehicle and the pedestrian, five meters away from the latter. The obstacle is 10 m long, 2.5 m wide and 2.5 m high. It consists of two materials: (1) aluminum, with a thickness of 1.5 cm and height of 1.8 m for each side, 2.5 m for the rear and 1.5 m for the front; and (2) glass, which completes the total height of the obstacle and has a thickness of 1.0 cm. These data are necessary to calculate the dielectric constant of the obstacle, which will allow or not the passing of the incident radio signal. The original implementation of the material in the used version of INET has been modified, since it has no relative permissiveness and permeability values for aluminum. These parameters are defined 8.1 and 1.00002, respectively, according to [36,37]. All other parameters are set to the default values defined in the simulation model.

To reproduce the vehicle mobility and enable the simulation of the georeferencing provided by GPS, the SUMO (https://sumo.dlr.de/docs/index.html) traffic simulator is used. The attributes of the simulated road configured in SUMO are based on the physical characteristics of the location of real experiments, as well as the spatial properties of the vehicle and pedestrian, such as height, width and length. The framework Veins (https://veins.car2x.org/) is also used. Through the Veins_INET subproject, it is possible to use Veins as a mobility model for INET. The following software versions are used: INET 3.4, OMNeT++ 5.0, SUMO 0.32, and Veins 4.5. Table 2 summarizes the parameters defined in our simulations.

Table 2. Simulation parameters.

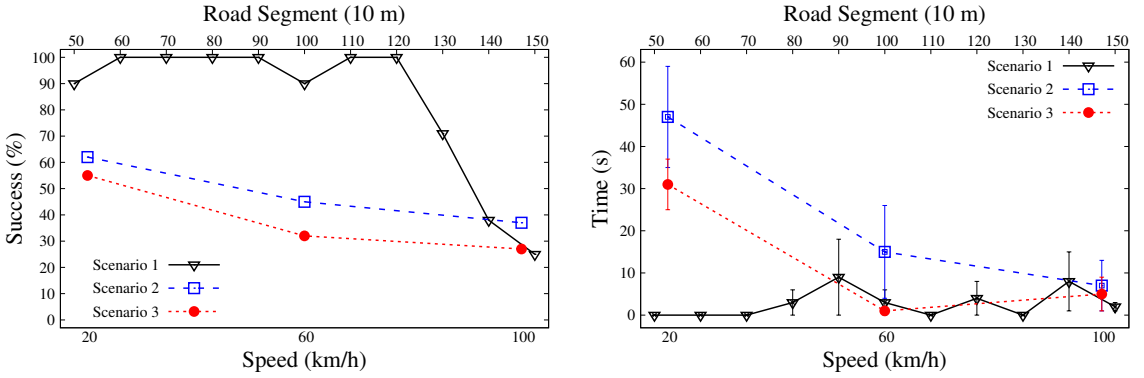
Parameter	Value
`udpApp`	`UDPBasicApp` (Tx) and `UDPSink` (Rx)
`mgmtType`	`Ieee80211MgmtSTAWifiDirect`
`bitrate`	`54 Mbps`
`power (transmitter)`	`24.60 mW` (13.90 dBm)
`retryLimit`	`0`
`obstacleLossType`	`DielectricObstacleLoss`
`pathLossType`	`LogNormalShadowing`
`alpha (pathLoss)`	`2.21`
`backgroundNoise`	`IsotropicScalarBackgroundNoise`
`power (backgroundNoise)`	`−98 dBm`
`propagation`	`ConstantSpeedPropagation`
`mobilityType`	`VeinsInetMobility`
`height (mobility)`	`1.6 m` (pedestrian) and `1.3 m` (vehicle)

5. CET Evaluation

This section presents the results of the CET performance evaluation through real experiments. In addition, this section also investigates the ability of the Wi-Fi Direct simulation model available on INET to reproduce the behavior obtained by smartphones in the real vehicular environment. For each scenario defined in Section 4, 10 rounds of experiments are performed. Since the results are divided by road segments (10 or 20 m long), only road segments in which PDR and PIR have non-zero values for at least 5 of 10 rounds are eligible for representation in plots. The median of the results is presented with vertical error bars, which correspond to the median absolute deviation. The choice for the median is due to its robustness in dealing with outliers.

It is worth highlighting the impact of the long CET of Wi-Fi Direct. In many rounds, it is not possible to establish a connection between the nodes. Thus, the results in this section are based on the rounds where the connection is established. We run the simulation until 10 successful rounds are achieved for each experiment. Figure 4a shows, for each scenario, the success rate taking into account the ratio between the 10 successful rounds and total number of simulation runs for each experiment. For example, in the simulations of the 1st Scenario, at 150 m, 40 executions are necessary to establish the connection in 10 of them, generating a success rate of 25%. As can be seen, in more distant road segments (1st Scenario), higher speeds (2nd Scenario and 3rd Scenario) and NLoS conditions (3rd Scenario) it is more difficult to establish a connection. These results demonstrate the challenge of using Wi-Fi Direct in mobility scenarios.

Figure 4b shows the CET duration in each scenario of the simulations, calculated as the time interval between the first Probe Request received by the group member (pedestrian) and the association with the GO (vehicle). We note that the CET is less affected by the distance (1st Scenario) than by the mobility (2nd and 3rd Scenario). Also, it is possible to note that the CET is higher at lower speeds. This happens because at lower speeds, the vehicle takes more time to reach the pedestrian since the first probe received. The larger time helps the connection establishment as the vehicle has more time to perform the whole process (Probe Response, GO negotiation, etc.) even considering possible message losses. At higher speeds, to succeed, the whole process must be finished possibly without losses, leading to a lower CET. In real experiments, the collection of the connection data is not performed.



(**a**) Success rate of establishment connection.

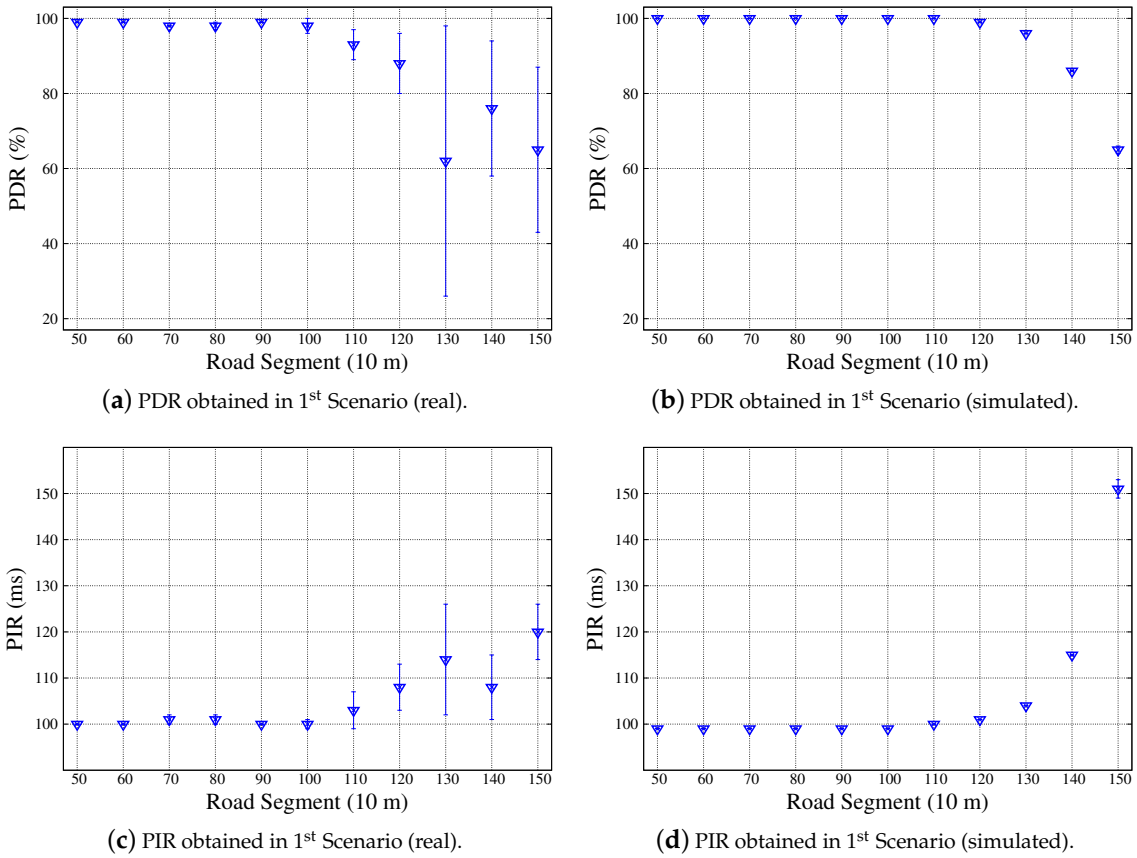
(**b**) CET Duration in Wi-Fi Direct.

Figure 4. Wi-Fi Direct Connection Establishment Time (CET) assessment.

5.1. Real Communication Range

As mentioned in Section 4, the results of this first set of experiments are used as a reference to the calibration step of the INET propagation model, bringing the simulated environment closer to the real world. The calibration process consists of obtaining, in the road segment that corresponds to the distance of 150 m among the nodes in simulations, a PDR similar to that one obtained in the same road segment in real experiments. After this procedure, we investigate the equivalence of the results in both environments. Besides that, this assessment also serves to analyze the real communication

range of Wi-Fi Direct in the real world. Before considering Wi-Fi Direct in the vehicular environment, it is necessary to analyze whether the devices are able to communicate at the distances defined in the application requirements. For example, blind spot and lane change warnings operate within 100 m [12]. Figure 5a–d show the real range of Wi-Fi Direct based on PDR and PIR as the distance between the nodes increases.



(**a**) PDR obtained in 1st Scenario (real).

(**b**) PDR obtained in 1st Scenario (simulated).

(**c**) PIR obtained in 1st Scenario (real).

(**d**) PIR obtained in 1st Scenario (simulated).

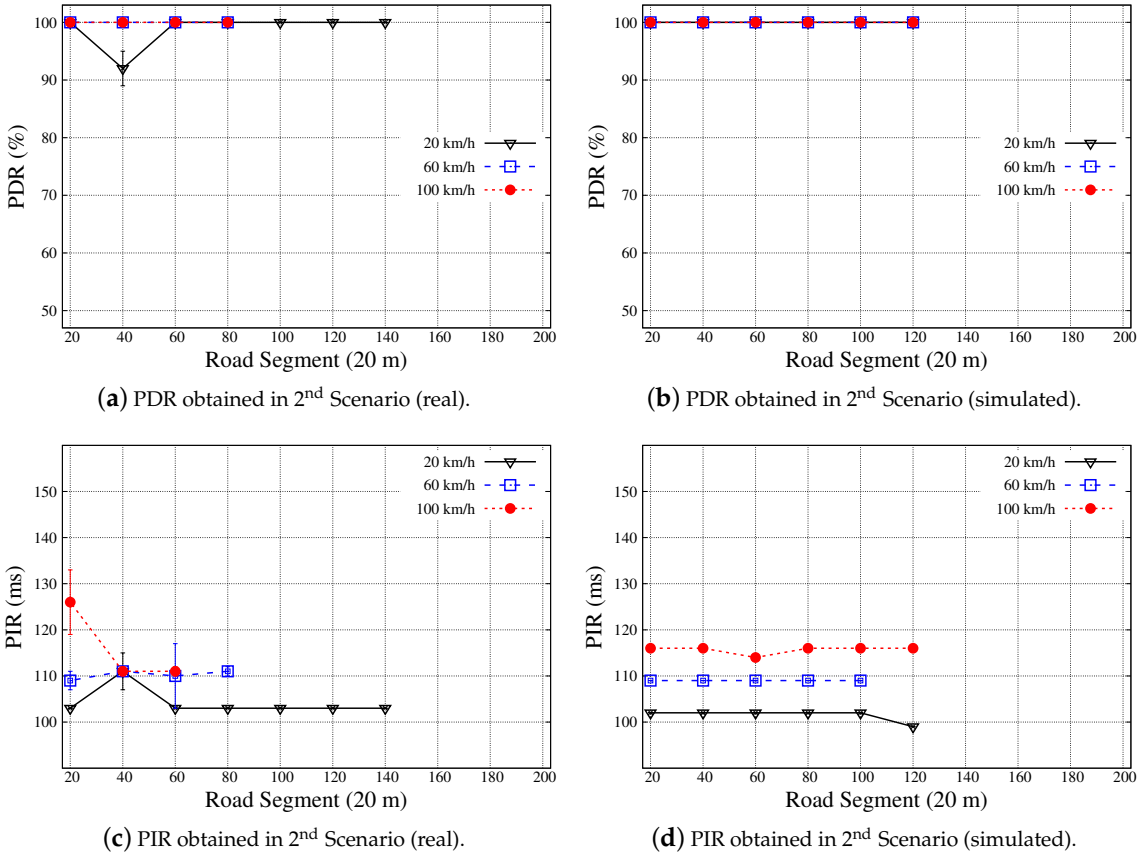
Figure 5. 1st Scenario—Real Communication Range (LoS).

In the real experiments, we observe a PDR between 50 and 100 m, which is close to 100%. On the other hand, due to large scale attenuation, the PDR drop from 110 m on is noticeable. Despite this, in all road segments, the PDR is $\geq$60%. Even in the most distant road segment (150 m), it is still possible to obtain an effective communication range. In this case, the reception level based on the PDR demonstrates to be enough to support the operation of a safety application based on VRUs. Due to the calibration, in simulations it is possible to obtain a PDR very close to the one obtained in real experiments. Despite small differences in terms of absolute value, the simulator is able to reproduce the decreasing behavior of PDR as the distance among the nodes increases.

Regarding the PIR, in both real experiments and simulations, it is possible to observe a negative correlation with the PDR, especially in the more distant road segments. The lower the PDR, the higher the PIR. Since the transmission power is fixed, the larger the distance, the stronger the radio signal attenuation, impairing the PDR and, consequently, the PIR. In a more complex scenario, this behavior indicates an alert for applications requiring communications over long distances. Despite this, in both environments, in general the PIR is slightly proportional to the generation period of BSMs (every 100 ms), which ensures an acceptable level of situational awareness to road users.

5.2. 2nd Scenario—Mobility Impact (LoS)

The second set of experiments investigates whether the CET observed impacts the performance of Wi-Fi Direct in mobility scenarios. In LoS conditions, PDR and PIR are calculated for each 20-meter road segment as the vehicle approaches the pedestrian at 20, 60 and 100 km/h. Figure 6a–d present the results obtained in both real experiments and simulations. Although in the figures the x-axis is increasing, the results represent the approach of the vehicle towards the pedestrian, starting its route 200 m away from him.



(**a**) PDR obtained in 2nd Scenario (real).

(**b**) PDR obtained in 2nd Scenario (simulated).

(**c**) PIR obtained in 2nd Scenario (real).

(**d**) PIR obtained in 2nd Scenario (simulated).

Figure 6. Impact of mobility in LoS conditions.

The results of PDR in real experiments demonstrate the impact that the long CET of Wi-Fi Direct can impose in a mobile scenario. As demonstrated in Section 5.1, in the scenario with no mobility it is possible to receive BSMs up to 150 m with at least 60% PDR. With the exception of the results obtained while the vehicle moved at 20 km/h, in the current scenario, the maximum distance at which the pedestrian (member of the group) can establish the connection with the vehicle (GO)—being able to transmit BSMs—is between 60 m and 80 m, at 60 km/h and 100 km/h. Above 80 m, the PDR is always 0. In conditions of low mobility (20 km/h), the connection is established from the road segment located between 120 and 140 m. In this case, the PDR is always $\geq$90%.

According to Won et al. [28], it is possible to calculate the risk of accidents between pedestrian and vehicle based on the time the vehicle takes to reach the pedestrian. This time is computed by the sum (1) of the driver's reaction time after receiving the alert and (2) of the time to stop the vehicle after it starts braking. These parameters are affected by the vehicle's speed, the driver's cognitive ability,

and the condition of tires, brakes, and the road. Hence, based on the time to stop the vehicle after receiving the BSM, the distance traveled can be calculated as:

$$D_{total} = d_{reaction} + d_{braking} = s_{veh}.t_{reaction} + \frac{s_{veh}^2}{2\mu g}, \quad (1)$$

where $d_{reaction}$ is the distance traveled by the vehicle during the driver's reaction time after receiving the alert triggered by the BSM, and $d_{braking}$ is the distance traveled by the vehicle after the driver starts braking, based on the vehicle's speed (s_{veh}), road friction coefficient (μ), gravity acceleration (g) and driver's reaction time ($t_{reaction}$).

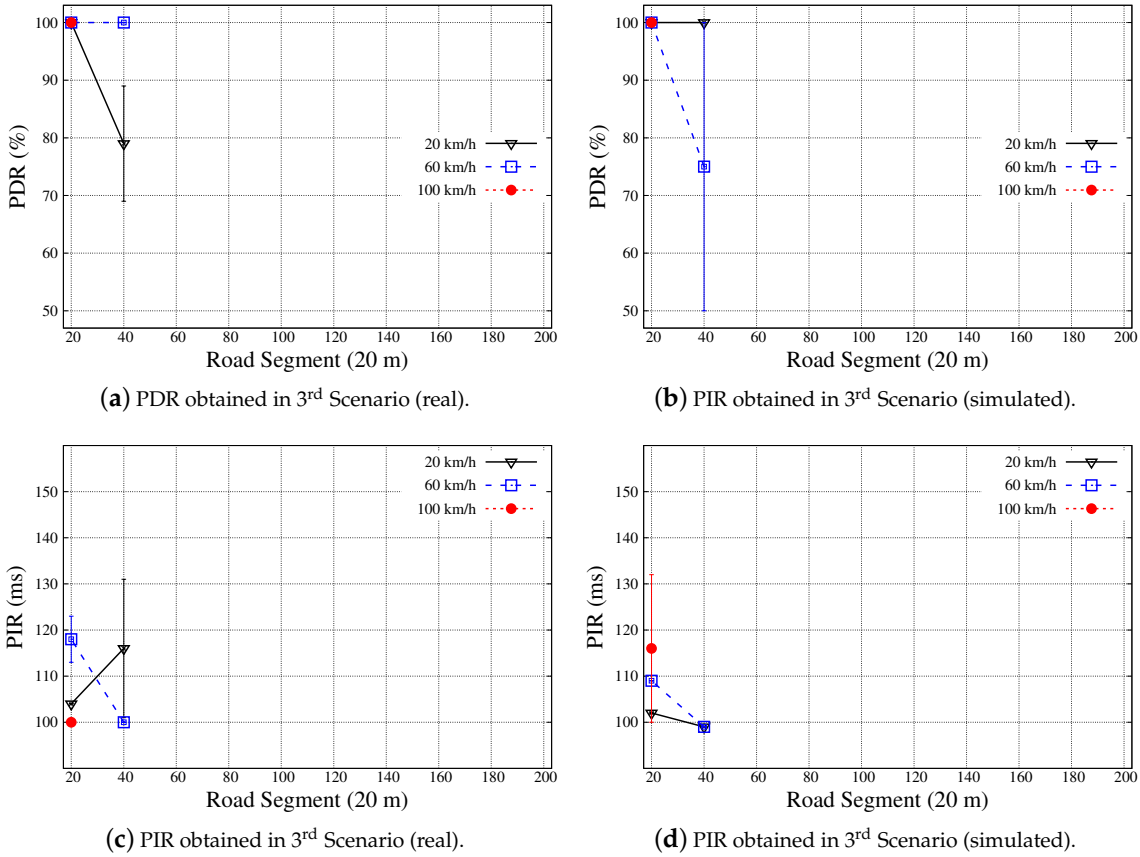
In [28], the authors aggregated RTT and other parameters in $t_{braking}$. In the current paper, instead of RTT, we add to $t_{breaking}$ a delay equivalent to the average PIR (100 ms), as well as a $t_{reaction}$ of 1 s (the same as [38]), g equal to 9.81 m/s^2, and μ equal to 0.8 (compatible with dry asphalt [39]). Considering s_{veh} as 20, 60 and 100 km/h, a distance of 8, 36, and 80 m, approximately, would be traveled, respectively, until the vehicle comes to a stop. As shown in Figure 6a, an accident between vehicle and pedestrian could be avoided at 20 and 60 km/h. At 100 km/h, on the other hand, there is an accident risk. Nevertheless, the maximum speed limit in urban areas in most countries does not exceed 60 km/h [40]. For example, in the United States and Europe, the maximum speed allowed in urban areas is 40 [41] and 50 km/h [42], respectively. Therefore, at least in low and middle mobility conditions, Wi-Fi Direct supports the V2P communication requirements.

The range obtained at 20 km/h is smaller in simulations than in real experiments. Moreover, in the simulations, the increase in the vehicle speed does not impact the PDR as it does in real experiments. As shown in Figure 6b, the connection establishment and, consequently, the transmission of BSMs is performed while the vehicle is in the road segment between 100 and 120 m away from the pedestrian. Regardless the speed (20, 60 or 100 km/h), in this road segment the PDR is always 100%. According to the simulation results, the accident could be avoided in any mobility condition. Due to the relationship between the increase in the node speed and the Doppler shift—which supposedly causes an increase in the BER (Bit Error Rate)—the lack of influence of mobility in PDR may be associated with the absence, in the simulator, of a module that models this phenomenon.

Regarding the PIR, it is possible to note a slight correlation with the PDR in both real experiments and simulations. Where the PDR is close to or equal to 100%, the PIR is similar to the generation period of BSMs (100 ms). Specifically in simulations, it is possible to observe a trade-off between increasing vehicle speed and a small increase in PIR. Nevertheless, despite this small increase, the PIR is still proportional to the generation period of BSMs. This result is important, since it demonstrates that, once the connection is established, Wi-Fi Direct is capable of meeting the requirement of safety applications [14]. In other words, this result indicates that the vehicle can be aware of the pedestrian's position on the road.

5.3. 3rd Scenario—Mobility Impact (NLoS)

The third set of experiments analyzes the performance of Wi-Fi Direct in a scenario with mobility and under NLoS conditions. Again, the vehicle moves at 20, 60 and 100 km/h towards the pedestrian, but this time a large vehicle (a 4 × 4 truck) is positioned between the vehicle and the pedestrian. As in the previous scenario, PDR and PIR are calculated every 20 m. Figure 7a–d plot the obtained results.



(**a**) PDR obtained in 3rd Scenario (real).

(**b**) PIR obtained in 3rd Scenario (simulated).

(**c**) PIR obtained in 3rd Scenario (real).

(**d**) PIR obtained in 3rd Scenario (simulated).

Figure 7. Impact of mobility in NLoS conditions.

As shown in Figure 7a, in real experiments, the difference in PDR is clear compared to the scenario with LoS. In the current scenario, the strong attenuation on the radio signal causes, at best, the pedestrian to complete the connection establishment and start the transmission of BSMs only in the road segment between 20 and 40 m, with the vehicle moving at 20 or 60 km/h. This result indicates that, under NLoS conditions, the long CET prohibits the use of Wi-Fi Direct in VANETs. Based on the distances calculated in Section 5.2 to stop the vehicle after receiving an alert (8, 36 and 80 m), under NLoS conditions, there is a great risk that an accident between vehicle and pedestrian cannot be avoided at 60 and 100 km/h. With small differences, the same behavior can be seen in the simulation results (Figure 7b). The similar results obtained in both real experiments and simulations show that the effect of the obstacle on communication is well modeled.

With regard to PIR, Figure 7c shows, once again, a slight correlation with PDR in real experiments. On the other hand, as Figure 7d shows, the simulations do not show correlation between the two metrics. Nevertheless, the trade-off between increasing vehicle speed and increasing PIR remains in simulations. Finally, despite the reduction in PDR, in both environments, in the segment between 20 to 40 m, the PIR remained proportional to the generation period of BSMs.

As a conclusion, the use of Wi-Fi Direct in realistic environments, under NLoS conditions, is challenging, mainly due to the long CET of native operation of this technology. Thus, solutions that minimize the CET are needed to allow the use of this technology as an alternative to 802.11p in VANETs.

6. Proposed Transmission Method for Wi-Fi Direct

Motivated by the results described in the previous section, we investigate a transmission method for Wi-Fi Direct based on beacon stuffing to improve the delivery of alerts under NLoS conditions. Originally proposed in [23], the beacon stuffing method consists of overloading fields in the beacon

to carry information. In [23], the information embedded in the beacon is disseminated as a string of bytes containing: (1) the identifier of the message; (2) the fragment number; (3) a flag that informs the existence of more fragments; and (4) the contents of the message. Three techniques are proposed to embed the message in a beacon: (1) SSID Concatenation; (2) BSSID Concatenation; and (3) Beacon Information Element. The last two techniques require root privileges.

In our proposed method, the 32-byte field referring to the device name in Wi-Fi Direct is modified. Using the Reflection API in Java, we change the name of the device, and not the SSID as in [23,27]. Even using the Reflection API to modify the SSID of the group created by the GO in Wi-Fi Direct (through `setNetworkName` method), the SSID perceived on the receiver is always the same. Consequently, it is not possible to carry information in an opportunistic way by modifying the SSID in Wi-Fi Direct. In the proposed method the device name is filled in with the device ID, its geographical coordinates (latitude and longitude), speed, and travel direction. Such values provide the basic information needed by a safety application designed to prevent accidents among vehicles and pedestrians. The goal is to evaluate a transmission method that does not require root privileges, making implementation possible in the real world, at the same time, it privileges the ubiquitous nature of smartphones.

On the transmitter side, the method consists of: (1) collect the data that composes the BSM (latitude, longitude, direction, speed); (2) build the BSM with collected data, in addition to an ID for the device; (3) modify the 32-byte field of the device name by the content of the created BSM; (4) remove any Wi-Fi Direct communication group previously created and, shortly thereafter, (5) create a new Autonomous group. This procedure is performed periodically, every 1 s. Since, immediately after the creation of the Autonomous group, the GO transmits beacons every 100 ms, at most 10 beacons would be sent containing the BSM embedded in the device name. In tests performed on a computer running the monitor mode on the network interface, the reception rate of the beacons sent through this technique sometimes showed small delays, due to the periodical removal and creation of the Autonomous group.

The periodic removal and creation of the Autonomous group is necessary because otherwise the device discovery performed at the receiver is not able to show the updated device name (that is, the most updated location data carried opportunistically by the BSM) as changed/renewed/reset by the transmitter (GO). In tests carried out with smartphones, even if the device name is changed by the most current BSM content, but the Autonomous group created by the transmitter is not removed and created again, the receiver always shows the same name that was initially received. After removing and creating a new group, Android always refreshes the SSID assigned. We assume that the change of the SSID by Android after the removal and creation of a new group enable the receiver to consider the device as a new device discovered, leading to show the device name updated.

On the receiving side, the method consists of: (1) collect periodically the data of GPS (latitude, longitude, direction, speed) of the vehicle and (2) continuously run the Wi-Fi Direct device discovery method. Given the operation mode of Wi-Fi Direct, especially with respect to the device discovery (as exemplified in Section 2), we assume that the discovery of data transmitted by the GO on the receiver will happen when (1) the transmitter sends beacons on the same channel that the receiver chose to listen to in the Listen step, or (2) when the receiver receives probe responses from the GO after sending (in the Search step) probe requests on the same channel that GO is operating. For continuous operation, we have configured Android's `PeerListListener` method to restart whenever the application detects its interruption. This ensures continuous execution of the method and, consequently, the reception of BSMs propagated.

The evaluation of the proposed method is carried out in a simple scenario, where smartphones are placed side by side and 1000 BSMs are transmitted by the GO. That is, for 1000 s, the name of the device is changed, as well as the Autonomous group is removed and created every 1 s, allowing the `PeerListListener` method running on the receiver to present the updated device name (BSM). Our initial goal is to evaluate the transmission method based on the beacon stuffing, therefore, the real

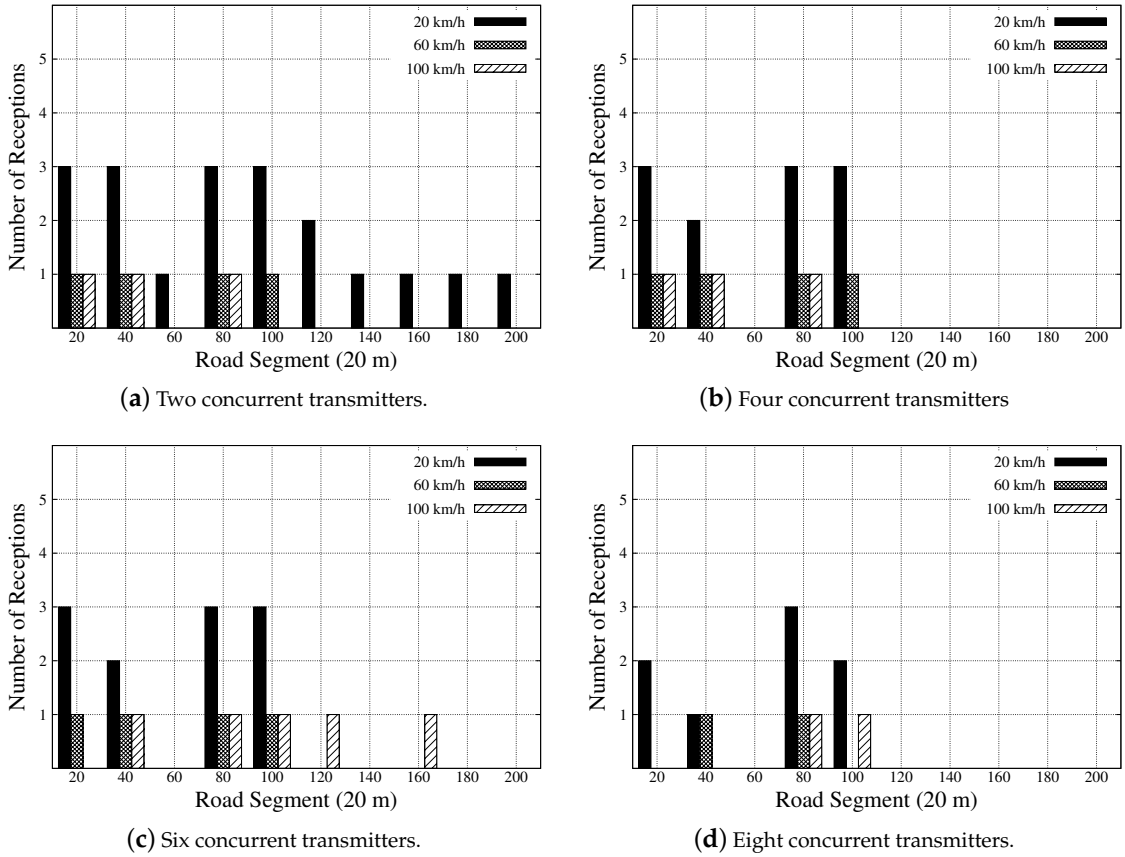
test with smartphones is carried out in an environment without interference and with the GPS data collection disabled in both devices. The reason for disabling GPS data collection is to eliminate possible performance problems caused by hardware specificities. The obtained results indicate that it is possible to obtain a PDR of 99% in this scenario. This means that the receiver is able to know the updated device name (BSM) 99% of the time. With respect to PIR, the results indicate that it is possible to obtain a PIR of around 1 s, proportional to the BSM generation rate. It is worth noting that, in the process of removing/creating the Autonomous group of Wi-Fi Direct, the channel defined by the GO may be different from the channel that was previously used. Nevertheless, when we set the network interface in monitor mode, in the vast majority of times the GO chose the same operating channel that was being used before removing/creating the Autonomous group. Natively, during the creation of the Autonomous group on Wi-Fi Direct, it is not possible to define the channel used by the GO.

We evaluate the transmission method based on beacon stuffing in the Wi-Fi Direct simulation model available on INET. In the simulations, the role of GO is played by the node modeled as the pedestrian. This node, after creating an Autonomous group, starts transmitting beacons every 100 ms. Following the observation of the real tests using smartphones—where, in the vast majority of times, the GO has always chosen the same operating channel, even after removing/creating the Autonomous group—in the simulations the GO always transmits beacons on the same channel. The beacons transmitted by GO are modified in order to carry the information present in the BSM. As the beacons are transmitted every 100 ms, in order to simulate the method of changing the device name every 1 s (as in the real test), the message ID is incremented every 10 beacons transmitted. As mentioned earlier, we assume that the GO can also be discovered by the receiver after sending probe responses. In this way, the GO also sends the BSM content via probe responses after receiving a probe request.

In the node modeled as vehicle, the node initially performs an active scan on the social channels. If no Wi-Fi Direct communication group is identified, the node continuously performs device discovery, which consists of the listen and search steps. The WPS provisioning step was disabled in the simulations. In the vehicle, only the first BSM received is accounted for, i.e., repeated BSMs (with the same message ID) are discarded. This is necessary to simulate the behavior of the application on smartphones, in which `PeerListListener` method is only called if the received BSM has a different content compared to the previous one (meaning that the device name has been changed). In the node modeled as vehicle, BSM receptions can take place in the function that handles both beacons and probe responses received.

In order to evaluate the transmission based on beacon stuffing in an environment with interference, four simulation scenarios—varying the number of transmitters (GO) transmitting beacons periodically on the same operation channel—are executed. In all cases, there is only one node modeled as a vehicle (receiver). The results show the number of BSMs received in each 20 m segment, based on the BSMs transmitted by the pedestrian (GO) located closest to the obstacle. All pedestrians (the GO located closest to the obstacle and others acting as interference) are positioned 3 m away from each other. Figure 8a–d presents the number of receptions in the scenario with NLoS conditions and interference. Ten rounds are performed for each scenario evaluated.

As can be seen—with the exception of the scenario with eight concurrent transmitters—it is possible to receive, at least, one BSM in the vehicle, indicating the pedestrian's position and speed with at least 100 m of distance for speeds of 20 and 60 km/h. Given the calculation of the vehicle's braking distance (shown in Equation (1)), the reception of the BSM at this point of the road allows the driver to know the pedestrian's presence and stop the vehicle in time. Since with just one BSM it is possible to estimate the risk of an accident between vehicle and pedestrian, the transmission method for Wi-Fi Direct based on beacon stuffing [23] can potentially cope with the long CET, especially in NLoS conditions.



(**a**) Two concurrent transmitters.

(**b**) Four concurrent transmitters

(**c**) Six concurrent transmitters.

(**d**) Eight concurrent transmitters.

Figure 8. Information transmission over WiFi Direct based on beacon stuffing.

7. Conclusions

Focusing the immediate support to communication between vehicles and VRUs, this paper analyzed the performance of Wi-Fi Direct through real measurements using smartphones. The obtained results of these measurements were then compared to those obtained by the Wi-Fi Direct simulation model available on framework INET of the OMNeT++ simulator. Our goal was to investigate the simulation model accuracy and enable large-scale evaluation. Considering the V2P scenario, the real communication range, packet delivery rate and packet inter-reception time were evaluated. The impact of different vehicle speeds, as well as LoS and NLoS conditions on the communication were investigated.

The results indicate that it is possible to obtain a fair range, up to 150 m (with PDR $\geq$ 60%) with Wi-Fi Direct. In the scenario with mobility and LoS conditions, despite the CET of Wi-Fi Direct, it is possible to receive BSMs at 140 and 80 m, respectively, with the vehicle moving at 20 and 60–100 km/h. In this case, according to the collision risk calculation, it is possible to avoid an accident between vehicle and pedestrian at 20 and 60 km/h. On the other hand, in the NLoS scenario, due to the radio signal attenuation and the long CET, the maximum distance at which it is possible to receive BSMs is 40 m to 20 km/h and 60 km/h. Therefore, in NLoS conditions, Wi-Fi Direct may not be viable for V2P safety applications. In general, the simulator was able to reproduce the PDR behavior obtained in real experiments. Regarding PIR, in general in both environments it was possible to observe a negative correlation of this metric with the PDR.

Motivated by the previous results, a transmission method based on beacon stuffing [23] was evaluated in order to enable Wi-Fi Direct on VANETs. In this method, the 32-byte field of the device name is replaced with the data relevant from the BSM. The obtained results indicate that this method can be a good option in scenarios with NLoS conditions, since it was possible to receive at least one BSM at a safe braking distance.

As future work, it is intended to carry out real experiments aiming to evaluate the proposed method in a realistic vehicular environment. In addition, with a focus on increasing the accuracy of geographic coordinates, one of the goals is to explore the vehicle's embedded CAN (Controller Area Network) and integrate the dead reckoning technique with GPS. Finally, we will investigate the performance of Wi-Fi Aware (Neighbor Awareness Networking), and analyze the possibility of using this technology for safety applications in VANETs.

Author Contributions: Conceptualization, methodology, simulations, validation and investigation, T.T.d.A.; resources and real experiments, T.T.d.A. and J.G.R.J.; writing—original draft preparation, T.T.d.A.; writing—review, editing and supervision, J.G.R.J., M.E.M.C. and L.H.M.K.C.; funding acquisition, M.E.M.C. and L.H.M.K.C. All authors have read and agreed to the published version of the manuscript.

Funding: This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior—Brazil (CAPES)—Finance Code 001. It was also partially funded by CNPq (grant numbers 304142/2017-4, 311169/2018-0, and 432566/2018-0), FAPERJ (grant numbers E-26/202.932/2017 and E-26/202.689/2018) and FAPESP (grant number 15/24494-8).

Acknowledgments: The authors would like to thank the municipality of Leopoldina—MG, Brazil, for allowing the real experiments to be carried out at the deactivated airport located in this city.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

BER	Bit Error Rate
BLE	Bluetooth Low Energy
BSM	Basic Safety Message
BSS	Basic Service Set
BSSID	Basic Service Set IDentifier
C-V2X	Cellular V2X
CAM	Cooperative Awareness Messages
CAN	Controller Area Network
CET	Connection Establishment Time
DEN	Decentralized Environmental Notifications
GO	Group Owner
LoS	Line-of-Sight
NFC	Near Field Communication
NLoS	Non-Line-of-Sight
OBU	On-Board Unit
P2P	Peer-To-Peer
PDR	Packet Delivery Rate
PIR	Packet Inter-Reception time
RSU	RoadSide Unit
RTT	Round-Trip-Time
SSID	Service Set IDentifier
TTL	Time-To-Live
V2P	Vehicle-to-Pedestrian
VANET	Vehicular Ad-hoc NETworks
VRU	Vulnerable Road Users
WHO	World Health Organization
WPS	Wi-Fi Protected Setup

References

1. World Health Organization. Road Traffic Injuries. 2019. Available online: https://www.who.int/publications-detail/global-status-report-on-road-safety-2018 (accessed on 4 June 2020).
2. Arena, F.; Pau, G. An Overview of Vehicular Communications. *Future Internet* **2019**, *11*, 27.
3. *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service*; European Telecommunications Standards Institute (ETSI): Sophia Antipoli, France, 2019; ETSI EN 302 637-2.

4. *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service*; European Telecommunications Standards Institute (ETSI): Sophia Antipoli, France, 2019; ETSI EN 302 637-3.
5. *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 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009); IEEE: Piscataway, NJ, USA, 2010; pp. 1–51, doi:10.1109/IEEESTD.2010.5514475.
6. Miucic, R.; Bai, S. Performance of Aftermarket (DSRC) Antennas Inside a Passenger Vehicle. *SAE Int. J. Passeng. Cars Electron. Electr. Syst.* **2011**, *4*, 150–155, doi:10.4271/2011-01-1031.
7. Balasundram, A.; Samarasinghe, T.; Dias, D. Performance Analysis of Wi-Fi Direct for Vehicular Ad-hoc Networks. In Proceedings of the 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Bangalore, India, 6–9 November 2016; pp. 1–6.
8. Sewalkar, P.; Seitz, J. Vehicle-To-Pedestrian Communication for Vulnerable Road Users: Survey, Design Considerations, and Challenges. *Sensors* **2019**, *19*, 358.
9. Statista. Global Smartphone Penetration Rate as Share of Population from 2016 to 2020. 2019. Available online: https://www.statista.com/statistics/203734/global-smartphone-penetration-per-capita-since-2005/ (accessed on 4 June 2020).
10. Khan, M.A.; Cherif, W.; Filali, F.; Hamila, R. Wi-Fi Direct Research-Current Status and Future Perspectives. *J. Netw. Comput. Appl.* **2017**, *93*, 245–258.
11. Frank, R.; Bronzi, W.; Castignani, G.; Engel, T. Bluetooth Low Energy: An Alternative Technology for VANET Applications. In Proceedings of the 2014 11th Annual Conference on Wireless On-Demand Network Systems and Services (WONS), Obergurgl, Austria, 2–4 April 2014; pp. 104–107.
12. Jeong, S.; Baek, Y.; Son, S.H. A Hybrid V2X System for Safety-Critical Applications in VANET. In Proceedings of the 2016 IEEE 4th International Conference on Cyber-Physical Systems, Networks, and Applications (CPSNA), Nagoya, Japan, 6–7 October 2016; pp. 13–18.
13. Hartenstein, H.; Laberteaux, L.P. A Tutorial Survey on Vehicular Ad Hoc Networks. *IEEE Commun. Mag.* **2008**, *46*, 164–171, doi:10.1109/MCOM.2008.4539481.
14. CAMP Vehicle Safety Communications Consortium. *Vehicle Safety Communications Project: Task 3 Final Report: Identify Intelligent Vehicle Safety Applications Enabled by DSRC*; National Highway Traffic Safety Administration, US Department of Transportation: Washington, DC, USA, 2005.
15. Touati, F.; Tabish, R.; Mnaouer, A.B. A Real-Time BLE Enabled ECG System for Remote Monitoring. *APCBEE Procedia* **2013**, *7*, 124–131.
16. Jeong, S.; Baek, Y.; Son, S.H. Hierarchical Network Architecture for Non-Safety Applications in Urban Vehicular Ad-Hoc Networks. *Sensors* **2019**, *19*, 4306.
17. Park, Y.; Ha, J.; Kuk, S.; Kim, H.; Liang, C.J.M.; Ko, J. A Feasibility Study and Development Framework Design for Realizing Smartphone-based Vehicular Networking Systems. *IEEE Trans. Mob. Comput.* **2014**, *13*, 2431–2444.
18. Zhang, H.; Wang, Y.; Tan, C.C. WD2: An Improved WiFi-Direct Group Formation Protocol. In Proceedings of the 9th ACM MobiCom Workshop on Challenged Networks, Maui, HI, USA, 7–11 September 2014; pp. 55–60.
19. Chaki, P.; Yasuda, M.; Fujita, N. Seamless Group Reformation in WiFi Peer to Peer Network using Dormant Backend Links. In Proceedings of the 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2015; pp. 773–778.
20. Sun, W.; Yang, C.; Jin, S.; Choi, S. Listen Channel Randomization for Faster Wi-Fi Direct Device Discovery. In Proceedings of the IEEE INFOCOM 2016—The 35th Annual IEEE International Conference on Computer Communications, San Francisco, CA, USA, 10–14 April 2016; pp. 1–9.
21. Camps-Mur, D.; Garcia-Saavedra, A.; Serrano, P. Device-to-Device Communications with Wi-Fi Direct: Overview and Experimentation. *IEEE Wirel. Commun.* **2013**, *20*, 96–104.
22. Iskounen, S.; Nguyen, T.M.T.; Monnet, S. WiFi-Direct Simulation for INET in OMNeT++. *arXiv* **2016**, arXiv:1609.04604.

23. Chandra, R.; Padhye, J.; Ravindranath, L.; Wolman, A. Beacon-Stuffing: Wi-fi without Associations. In Proceedings of the Eighth IEEE Workshop on Mobile Computing Systems and Applications, Tucson, AZ, USA, 8–9 March 2007; pp. 53–57.
24. Henderson, T.R.; Lacage, M.; Riley, G.F.; Dowell, C.; Kopena, J. Network Simulations with the NS-3 Simulator. *SIGCOMM Demonstr.* **2008**, *14*, 527.
25. Manamperi, W.; Samarasinghe, T.; Dias, D. Enhancing the Wi-Fi Direct Protocol for Data Communication in Vehicular Ad-hoc Networks. In Proceedings of the 2018 21st International Conference on Intelligent Transportation Systems (ITSC), Maui, HI, USA, 4–7 November 2018; pp. 812–817.
26. Shahin, A.A.; Younis, M. Alert Dissemination Protocol using Service Discovery in Wi-Fi Direct. In Proceedings of the 2015 IEEE International Conference on Communications (ICC), London, UK, 8–12 June 2015; pp. 7018–7023.
27. Dhondge, K.; Song, S.; Choi, B.Y.; Park, H. WiFiHonk: Smartphone-Based Beacon Stuffed WiFi Car2X-Communication System for Vulnerable Road User Safety. In Proceedings of the 2014 IEEE 79th Vehicular Technology Conference (VTC Spring), Seoul, Korea, 18–21 May 2014; pp. 1–5.
28. Won, M.; Shrestha, A.; Eun, Y. Enabling WiFi P2P-based Pedestrian Safety App. *arXiv* **2018**, arXiv:1805.00442.
29. Carpenter, M.G.; Moury, M.T.; Skvarce, J.R.; Struck, M.; Zwicky, T.D.; Kiger, S.M. *Objective Tests for Forward Looking Pedestrian Crash Avoidance/Mitigation Systems, Final Report*; Technical Report; National Highway Traffic Safety Administration: Washington, DC, USA, 2014.
30. Masini, B.M.; Silva, C.M.; Balador, A. The Use of Meta-Surfaces in Vehicular Networks. *J. Sens. Actuator Netw.* **2020**, *9*, 15.
31. Neto, J.B.P.; Gomes, L.C.; Ortiz, F.M.; Almeida, T.T.; Campista, M.E.M.; Costa, L.H.M.; Mitton, N. An Accurate Cooperative Positioning System for Vehicular Safety Applications. *Comput. Electr. Eng.* **2020**, *83*, 106591.
32. IEEE Spectrum. Superaccurate GPS Chips Coming to Smartphones in 2018. 2017. Available online: https://spectrum.ieee.org/tech-talk/semiconductors/design/superaccurate-gps-chips-coming-to-smartphones-in-2018 (accessed on 4 June 2020).
33. ASUSTeK Computer Inc. ZA550KL: User's Guide. 2018. Available online: https://dlcdnets.asus.com/pub/ASUS/ZenFone/ZA550KL/PG13969_ZA550KL_EM_WEB.pdf (accessed on 4 June 2020).
34. Bloessl, B.; O'Driscoll, A. A Case for Good Defaults: Pitfalls in VANET Physical Layer Simulations. In Proceedings of the 2019 Wireless Days (WD), Manchester, UK, 24–26 April 2019; pp. 1–6.
35. Rappaport, T.S. *Wireless Communications: Principles and Practice*; Prentice Hall PTR: Upper Saddle River, NJ, USA, 1996; Volume 2.
36. MicroWaves 101. Magnetic Materials. 2020. Available online: https://www.microwaves101.com/encyclopedias/magnetic-materials (accessed on 4 June 2020).
37. Pande, K.; Nair, V.; Gutierrez, D. Plasma enhanced metal-organic chemical vapor deposition of aluminum oxide dielectric film for device applications. *J. Appl. Phys.* **1983**, *54*, 5436–5440.
38. Renda, M.E.; Resta, G.; Santi, P.; Martelli, F.; Franchini, A. IEEE 802.11 p VANets: Experimental Evaluation of Packet Inter-Reception Time. *Comput. Commun.* **2016**, *75*, 26–38.
39. Wong, J.Y. *Theory of Ground Vehicles*; John Wiley & Sons: New York, NY, USA , 2008.
40. World Health Organization. Speed Laws and Enforcement by Country/Area. 2019. Available online: http://www9.who.int/violence_injury_prevention/road_safety_status/2018/Table_A4_Speed.pdf (accessed on 4 June 2020).
41. Federal Highway Administration. Speed Limit Basics. 2020. Available online: https://safety.fhwa.dot.gov/speedmgt/ref_mats/fhwasa16076/fhwasa16076.pdf (accessed on 4 June 2020).
42. European Comission. Current Speed Limit Policies. 2020. Available online: https://ec.europa.eu/transport/road_safety/specialist/knowledge/speed/speed_limits/current_speed_limit_policies_en (accessed on 4 June 2020).