AVALIAÇÃO EXPERIMENTAL E POR SIMULAÇÃO DO IEEE 802.11P E WI-FI DIRECT PARA COMUNICAÇÕES VEICULARES

Thales Teixeira de Almeida

Tese de Doutorado apresentada ao Programa de Pós-graduação em Engenharia Elétrica, COPPE, da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Doutor em Engenharia Elétrica.

Orientadores: Luís Henrique Maciel Kosmalski Costa
José Geraldo Ribeiro Júnior

Rio de Janeiro
Dezembro de 2021

AVALIAÇÃO EXPERIMENTAL E POR SIMULAÇÃO DO IEEE 802.11P E WI-FI DIRECT PARA COMUNICAÇÕES VEICULARES

Thales Teixeira de Almeida

TESE SUBMETIDA AO CORPO DOCENTE DO INSTITUTO ALBERTO LUIZ COIMBRA DE PÓS-GRADUAÇÃO E PESQUISA DE ENGENHARIA DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE DOUTOR EM CIÊNCIAS EM ENGENHARIA ELÉTRICA.

Orientadores: Luís Henrique Maciel Kosmalski Costa
José Geraldo Ribeiro Júnior

Aprovada por: Prof. Luís Henrique Maciel Kosmalski Costa
Prof. José Geraldo Ribeiro Júnior
Prof. Célio Vinicius Neves de Albuquerque
Prof. Igor Monteiro Moraes
Prof. Miguel Elias Mitre Campista

RIO DE JANEIRO, RJ – BRASIL
DEZEMBRO DE 2021

Almeida, Thales Teixeira de

Avaliação Experimental e por Simulação do IEEE 802.11p e Wi-Fi Direct para Comunicações Veiculares/Thales Teixeira de Almeida. – Rio de Janeiro: UFRJ/COPPE, 2021.

XIX, 126 p.: il.; 29, 7cm.

Orientadores: Luís Henrique Maciel Kosmalski Costa
José Geraldo Ribeiro Júnior

Tese (doutorado) – UFRJ/COPPE/Programa de Engenharia Elétrica, 2021.

Referências Bibliográficas: p. 111 – 126.

1. Redes Veiculares. 2. Vehicular Ad-hoc NETworks. 3. IEEE 802.11p. 4. Wi-Fi Direct. 5. Wi-Fi Peer-to-Peer. 6. NS-3. 7. PhySim. 8. Veins. 9. MiXiM. 10. INET. I. Costa, Luís Henrique Maciel Kosmalski *et al.* II. Universidade Federal do Rio de Janeiro, COPPE, Programa de Engenharia Elétrica. III. Título.

À minha esposa e à minha família.

Agradecimentos

Agradeço primeiramente a Deus, por nunca ter me desamparado. Agradeço aos meus orientadores Luís Henrique M. K. Costa e José G. Ribeiro Júnior. Professor Luís, obrigado por ter aceitado me orientar, pela orientação em si, pela contribuição nesta tese e por sempre ter lidado comigo de forma paciente, respeitosa e humana. Juninho, obrigado por ter me apresentado o GTA, pela orientação, pela valiosa ajuda nos experimentos práticos, e pelos momentos difíceis em que você sempre se dispôs a me ouvir. Agradeço aos professores Célio Vinicius N. de Albuquerque, Igor M. Moraes, e Miguel Elias M. Campista, por terem aceitado participar da banca de avaliação desta tese. Ao professor Miguel, agradeço também pelas contribuições nos artigos. Agradeço aos professores e colegas do GTA, pelo bom convívio e pela forma amistosa com que sempre me trataram. Em especial, agradeço ao Fernando M. Ortiz. Jovem, obrigado por ter sido um bom amigo e colega de trabalho, me ajudando em diversas situações ao longo destes anos. Agradeço ao Lucas de C. Gomes, pela valiosa contribuição em relação à implementação dos experimentos práticos com o IEEE 802.11p. Agradeço à Ana Elisa F. Leitão, pelas boas conversas ao longo do período em que dividimos a mesma sala no GTA. Agradeço ao Carlos Henrique de O. M. André, por ter me apresentado à república e por tornar a minha acomodação no Rio de Janeiro mais fácil, me dando dicas sobre trajetos, logística de transporte, etc. Agradeço também aos colegas do CEFET-MG, Campus Leopoldina – MG. Em especial, ao Alexandre M. G. de Deus, por sua habitual generosidade e suporte. Ao Douglas M. V. Silva, pelo apoio que sempre me ofereceu. Agradeço também a todos os colaboradores da Secretaria do Programa de Engenharia Elétrica da COPPE/UFRJ, por terem sido tão solícitos em todas as vezes que recorri a eles. Agradeço ao CEFET-MG e ao povo brasileiro, pela oportunidade de me conceder uma licença para capacitação. Agradeço ao Racyus D. G. Pacífico, por seu exemplo de dedicação aos estudos e pelas conversas que sempre tivemos sobre os desafios que cercam essa jornada. Agradeço também à minha esposa, Kerollayne, e à minha família. Vocês são a razão de tudo. Sem vocês nada seria possível. Muito obrigado por, em muitos momentos, terem me blindado de tal forma que eu pudesse dedicar tempo e esforços na realização desta tese. Por fim, agradeço a todos que, de alguma forma, contribuíram com esta tese e/ou torceram por mim.

Resumo da Tese apresentada à COPPE/UFRJ como parte dos requisitos necessários para a obtenção do grau de Doutor em Ciências (D.Sc.)

AVALIAÇÃO EXPERIMENTAL E POR SIMULAÇÃO DO IEEE 802.11P E WI-FI DIRECT PARA COMUNICAÇÕES VEICULARES

Thales Teixeira de Almeida

Dezembro/2021

Orientadores: Luís Henrique Maciel Kosmalski Costa
José Geraldo Ribeiro Júnior

Programa: Engenharia Elétrica

Veículos conectados estão cada vez mais próximos de se tornarem realidade, especialmente em países de alta renda. Em uma visão sistêmica, quanto maior é a parcela de veículos com capacidade de comunicação, melhor será o impacto na segurança do trânsito e na mobilidade urbana. Dentre as tecnologias disponíveis para implementação do paradigma de veículos conectados, dispositivos IEEE 802.11p – considerado por muitos o padrão de fato para comunicações veiculares – são encarados como uma das prováveis escolhas da indústria automotiva. Neste sentido, esta tese avalia o desempenho do IEEE 802.11p em experimentos com OBUs (*Onboard Units*) e RSUs (*Roadside Units*), e simulações no NS-3/PhySim e Veins/MiXiM. Uma vez que países de baixa ou média renda concentram a maior parte dos acidentes fatais no mundo, e que o investimento em sistemas inteligentes de transportes nestes países tende a ser baixo ou inexistente, também é importante avaliar opções ao IEEE 802.11p. Assim, esta tese também analisa a viabilidade do Wi-Fi Direct em oferecer conectividade em alguns cenários específicos, motivado pela ubiquidade de *smartphones* na sociedade. Para isso, foram realizados experimentos com *smartphones* e simulações no INET. Em ambos os casos, são usadas como métricas de desempenho a taxa de entrega e o tempo entre recepções de pacotes. Dado que experimentos práticos são complexos e custosos, esta tese avalia se as simulações reproduzem o comportamento obtido nos experimentos reais. Para isso, investigou-se, para um mesmo cenário em comum, o grau de equivalência dos resultados obtidos nos experimentos reais em comparação aos obtidos nas simulações. Os resultados indicam que, no geral, as simulações são capazes de refletir o comportamento obtido nos experimentos reais – apesar das esperadas diferenças em termos de valores absolutos.

Abstract of Thesis presented to COPPE/UFRJ as a partial fulfillment of the requirements for the degree of Doctor of Science (D.Sc.)

EXPERIMENTAL AND SIMULATION EVALUATION OF IEEE 802.11P AND WI-FI DIRECT FOR VEHICULAR COMMUNICATIONS

Thales Teixeira de Almeida

December/2021

Advisors: Luís Henrique Maciel Kosmalski Costa
José Geraldo Ribeiro Júnior

Department: Electrical Engineering

Connected vehicles are getting closer to reality, especially in high-income countries. In a systemic view, the greater the share of vehicles with communication capacity, the better the impact on traffic safety and urban mobility. Among the technologies available to implement the connected vehicle paradigm, IEEE 802.11p devices – considered by many to be the de facto standard for vehicular communications – are seen as one of the likely choices for the automotive industry. Therefore, this thesis evaluates the performance of IEEE 802.11p in experiments with OBUs (Onboard Units) and RSUs (Roadside Units), and simulations in NS-3/PhySim and Veins/MiXiM. Since low- and middle-income countries concentrate the majority of fatal accidents in the world, and that investment in intelligent transportation systems in these countries tends to be low or non-existent, it is also important to evaluate alternatives to IEEE 802.11p. In this case, this thesis also analyzes the feasibility of Wi-Fi Direct in offering connectivity in some specific scenarios, motivated by the ubiquity of smartphones in society. For this, experiments were carried out with smartphones and simulations on INET. For both cases, delivery rate and packet inter-reception time are used as performance metrics. Given that practical experiments are complex and costly, this thesis assesses whether simulations reproduce the behavior obtained in real experiments. To that end, we have investigated, for the same common scenario, the equivalence of the results obtained in real experiments and those obtained through simulation. The results indicate that, in general, the simulations are able to reproduce the behavior obtained in real experiments - despite the expected differences in terms of absolute values.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas

3GPP	*Third Generation Partnership Project*, p. 10
5G NR	5G *New Radio*, p. 10
ACC	*Adaptive Cruise Control*, p. 22
ACK	*ACKnowledgment*, p. 56
AC	*Access Categories*, p. 29
ADAS	*Advanced Driver Assistance Systems*, p. 2
ADS	*Alert Dissemination using Service discovery*, p. 56
AGC	*Automatic Gain Control*, p. 50
AIFS	*Arbitration Inter-Frame Spacing*, p. 29
AODV	*Ad-hoc On Demand Distance Vector*, p. 35
API	*Application Programming Interface*, p. 87
ARIB	*Association of Radio Industries and Businesses*, p. 21
AR	*Augmented Reality*, p. 26
ASPP	*Adaptive Single Presence Period*, p. 55
ASTM	*American Society for Testing and Materials*, p. 21
Abipeças	Associação Brasileira da Indústria de Autopeças, p. 1
Anatel	Agência Nacional de Telecomunicações, p. 11
BER	*Bit-Error Rate*, p. 35
BLE	*Bluetooth Low Energy*, p. 5
BO	*Beacon Observer*, p. 61

BSM	*Basic Safety Message*, p. 6
BSSID	BSS *IDentifier*, p. 60
BSS	*Basic Service Set*, p. 28
C-ACC	*Cooperative Adaptive Cruise Control*, p. 3
C-ITS	*Cooperative*-ITS, p. 21
C-V2X	*Cellular Vehicle-to-Everything*, p. 10
CAM	*Cooperative Awareness Messages*, p. 21
CAN	*Controller Area Network*, p. 16
CCA	*Clear Channel Assessment*, p. 29
CCH	*Control Channel*, p. 27
CCU	*Communications Control Unit*, p. 16
CEN	*Comité Européen de Normalisation*, p. 21
CET	*Connection Establishment Time*, p. 7
CMU	*Carnegie Mellon University*, p. 36
CP-OFDM	*Cyclic Prefix*-OFDM, p. 26
CSMA/CA	*Carrier-Sense Multiple Access with Collision Avoidance*, p. 29
CTS	*Clear to Send*, p. 56
CW	*Contention Window*, p. 29
D2D	*Device-to-Device*, p. 10
DCC	*Decentralized Congestion Control*, p. 29
DCM	*Dual Carrier Modulation*, p. 24
DEN	*Decentralized Environmental Notifications*, p. 21
DHCP	*Dynamic Host Configuration Protocol*, p. 31
DSRC	*Dedicated Short-Range Communication*, p. 3
ECC	*Electronic Communications Committee*, p. 21

EDCA *Enhanced Distributed Channel Access*, p. 29

EPC *Evolved Packet Core*, p. 26

ETC *Electronic Toll Collection*, p. 28

ETSI *European Telecommunications Standards Institute*, p. 21

FCC *Federal Communications Commission*, p. 3

FCW *Forward Collision Warning*, p. 40

FEC *Forward Error Correction*, p. 35

FR1 *Frequency Range* 1, p. 26

FR2 *Frequency Range* 2, p. 26

GAS *Generic Advertisement*, p. 32

GNSS *Global Navigation Satellite System*, p. 5

GOB *Group Owner Broadcast*, p. 55

GO *Group Owner*, p. 30

GPP *General Purpose Processor*, p. 50

GPS *Global Positioning System*, p. 45

HARQ *Hybrid Automatic Repeat Request*, p. 45

HMI *Human Machine Interface*, p. 3

IA *Intelligence Artificial*, p. 17

IBSS *Independent* BSS, p. 29

IDM *Intelligent Driver Model*, p. 34

IEEE *Institute of Electrical and Electronics Engineers*, p. 3

IE *Information Element*, p. 60

IPv6 *Internet Protocol version 6*, p. 27

IRT *Inter-Reception Time*, p. 41

ISI *InterSymbol Interference*, p. 26

ITSA	*Intelligent Transportation Society of America*, p. 21
ITS	*Intelligent Transportation Systems*, p. 2
ITU-R	ITU *Radiocommunication Sector*, p. 25
ITU-T	ITU *Telecommunication Standardization Sector*, p. 3
ITU	*International Telecommunication Union*, p. 3
IoT	*Internet of Things*, p. 17
IoV	*Internet of Vehicles*, p. 17
LDPC	*Low-Density Parity-Check*, p. 24
LED	*Light-Emitting Diode*, p. 22
LIDAR	*LIght Detection And Ranging*, p. 2
LTE-A ProSe	*Long Term Evolution Advanced Proximity Services*, p. 10
LTE	*Long Term Evolution*, p. 22
LoS	*Line-of-Sight*, p. 6
MAC	*Medium Access Control*, p. 22, 55
MANET	*Mobile Ad-hoc NETwork*, p. 14
MCS	*Modulation and Coding Schemes*, p. 45
MEC	*Multi-access Edge Computing*, p. 26
MIC	*Ministry of Internal Affairs and Communications*, p. 21
MIMO	*Massive Multiple-Input/Multiple-Output*, p. 25
MIMO	*Multiple-input and Multiple-output*, p. 24
MLME	*Extension of MAC sublayer Management Entity*, p. 28
MOBIL	*Minimizing Overall Braking Induced by Lane change*, p. 34
MiXiM	*Mixed Simulator*, p. 7
MovSim	*Multi-model open-source vehicular-traffic Simulator*, p. 34
NAN	*Neighbour Awareness Networking*, p. 109

NED *Network Description*, p. 37

NFC *Near Field Communication*, p. 5

NGC *Next-Generation Core*, p. 26

NGMN *Next Generation Mobile Networks*, p. 25

NITSA *National* ITS *Architecture*, p. 14

NLoS *Non-Line-of-Sight*, p. 7

NS-2 *Network Simulator 2*, p. 35

NS-3 *Network Simulator 3*, p. 6

NSA *Non-StandAlone*, p. 26

NoA *Notice of Absence*, p. 32

O-RAN *Open* RAN, p. 26

OAN *Opportunistic Association Networking*, p. 61

OBN *Opportunistic Beacon Networking*, p. 61

OBU *OnBoard Unit*, p. 3

OB *Opportunistic Beacon*, p. 61

OCB *Outside the Context of a* BSS, p. 28

OFDM *Orthogonal Frequency Division Multiplexing*, p. 28

OICA *International Organization of Motor Vehicle Manufacturers*, p. 2

OLSR *Optimized Link State Routing*, p. 35

OMNeT++ *Objective Modular Network Tested in C++*, p. 34

OMS Organização Mundial da Saúde, p. 1

OTcl *Object-Oriented Tool Command Language*, p. 35

OppPS *Opportunistic Power Save*, p. 32

P2P *Peer-to-Peer*, p. 30

PAR *Project Authorization Report*, p. 24

PDR *Packet Delivery Ratio*, p. 7

PHY *Physical Layer*, p. 22

PIN *Personal Identification Number*, p. 31

PIR *Packet Inter-Reception*, p. 7

PLME *Physical Layer Management Entity*, p. 28

PLR *Packet Loss Ratio*, p. 52

PRR *Packet Reception Ratio*, p. 43

PSDU *Packet Service Data Unit*, p. 69

PSID *Provider Service Identifier*, p. 28

PSP *Packet Success Probability*, p. 41

QoS *Quality of Service*, p. 29

R2V *Roadside-to-Vehicle*, p. 39

RADAR *RAdio Detection And Ranging*, p. 2

RAN *Radio Access Networks*, p. 26

RB *Resource Block*, p. 45

RLAN *Radio Local Area Network*, p. 21

RSE *Road Side Equipment*, p. 51

RSSI *Received Signal Strength Indication*, p. 49

RSU *RoadSide Unit*, p. 3

RTS *Request to Send*, p. 56

RTT *Round-Trip-Time*, p. 57

SAE *Society of Automotive Engineers*, p. 6

SA *StandAlone*, p. 26

SB-SPS *Sensing-Based Semi-Persistent Scheduling*, p. 46

SC-FDMA *Single Carrier Frequency Division Multiple Access*, p. 22

SCH	*Service Channel*, p. 27
SDK	*Software Development Kit*, p. 65
SDR	*Software-Defined Radio*, p. 40
SINR	*Signal-to-Interference-plus-Noise Ratio*, p. 35
SMARTS	*Scalable Microscopic Adaptive Road Traffic Simulator*, p. 34
SNR	*Signal-Noise Ratio*, p. 41
SOS	*Save Our Souls Services*, p. 19
SPMD	*Safety Pilot Model Deployment*, p. 51
SSID	*Service Set IDentifier*, p. 8
SUMO	*Simulation of Urban Mobility*, p. 34
Sindipeças	Sindicato Nacional da Indústria de Componentes para Veículos Automotores, p. 1
TCP	*Transmission Control Protocol*, p. 27
TDMA	*Time-Division Multiple Access*, p. 44
TG	*Task Group*, p. 21
TTL	*Time-To-Live*, p. 57
TraCI	*Traffic Control Interface*, p. 37
UDP	*User Datagram Protocol*, p. 9
UD	*Update Delay*, p. 42
UE	*User Equipment*, p. 10, 26
URLLC	*Ultra-Reliable and Low Latency Communications*, p. 25
UUID	*Universally Unique Identifier*, p. 61
V2I	*Vehicle-to-Infrastructure*, p. 3
V2P	*Vehicle-to-Pedestrian*, p. 7
V2R	*Vehicle-to-Roadside*, p. 17
V2S	*Vehicle-to-Sensor*, p. 17

V2V	*Vehicle-to-Vehicle*, p. 3
V2X	*Vehicle-to-Everything*, p. 17
VANET	*Vehicular Ad-hoc NETwork*, p. 2
VENTOS	*VEhicular NeTwork Open Simulator*, p. 34
VLC	*Visible Light Communication*, p. 10
VR	*Virtual Reality*, p. 26
VSC	*Vehicle Safety Communications*, p. 19
Veins	*Vehicles in Network Simulation*, p. 6
WAVE	*Wireless Access in Vehicular Environment*, p. 3
WDE	*Wi-Fi Direct Extension*, p. 55
WDMS	*Wi-Fi Direct Management System*, p. 55
WG NGV	WG *Next Generation V2V*, p. 24
WG	*Working Group*, p. 22
WHIP	*WiFiHonk Information Packet*, p. 61
WLAN	*Wireless* LAN, p. 40
WME	WAVE *Management Entity*, p. 28
WPS	Wi-Fi *Protected Setup*, p. 31
WSA	WAVE *Service Advertisement*, p. 28
WSMP	WAVE *Short Message Protocol*, p. 27
WSM	WAVE *Short Messages*, p. 27
WSU	*Wireless Safety Unit*, p. 49
eMBB	*enhanced Mobile BroadBand*, p. 25
eNodeB	*evolved Node B*, p. 16
gNB	*gNodeB*, p. 26
mMTC	*massive Machine Type Communications*, p. 25
mmWave	*millimeter-Wave*, p. 24

Capítulo 1

Introdução

O aumento da segurança no tráfego viário e a melhoria da mobilidade urbana estão entre os temas cada vez mais pautados como essenciais por governos, indústria e academia, já que o aumento no número de problemas no trânsito causa impactos negativos em diversas áreas, como economia, meio ambiente e saúde [5]. De acordo com o relatório mais recente da OMS (Organização Mundial da Saúde), de 2018, com os dados de 175 países, cerca de 1,35 milhão de pessoas morreram e outras 50 milhões ficaram feridas como resultado de lesões causadas por acidentes de trânsito [6]. Com cerca de 3,7 mil vidas perdidas diariamente, esta foi a oitava maior causa de mortes no mundo naquele período, e a principal entre jovens com idade variando de 5 a 29 anos. Somente pedestres, ciclistas e motociclistas – definidos como usuários vulneráveis das vias – representam mais de 50% de todas estas fatalidades. Ainda conforme o relatório, 88% dos pedestres trafegam em estradas inseguras, e o risco de morte após ser atropelado aumenta cerca de 4,5 vezes se a velocidade do veículo passar de 50 km/h para 65 km/h. Este problema é ainda mais grave em países de baixa ou média renda. Apesar de concentrarem 60% da frota de veículos, mais de 90% dos acidentes fatais ocorreram nestes países. Segundo a OMS, a infraestrutura viária nesses países está diretamente associada a essas fatalidades, pois muitas estradas não possuem faixas exclusivas para ciclistas ou travessias adequadas para pedestres, além de possuírem limites de velocidade elevados. Para ilustrar, em consulta feita aos dados do DATASUS, do Ministério da Saúde, em 2019 mais de 32 mil pessoas perderam a vida em decorrência de acidentes de trânsito no Brasil [7], dos quais mais de 18 mil eram usuários vulneráveis das vias. Apesar de anunciada uma redução de 7% ao ano entre 2015 e 2019 [8], este número ainda coloca o país entre os líderes mundiais de acidentes fatais de trânsito.

Quanto à mobilidade urbana, pode-se afirmar que existe uma dependência entre a piora de sua qualidade e o número cada vez maior de veículos nas vias. Por exemplo, um relatório elaborado pelo Sindipeças (Sindicato Nacional da Indústria de Componentes para Veículos Automotores) e Abipeças (Associação Brasileira da Indústria de Autopeças) [9] demonstra que, até 2020, a frota brasileira era composta por 59,1 milhões de veículos em

circulação, entre automóveis, comerciais leves, caminhões, ônibus e motocicletas. Este quantitativo coloca o Brasil entre os seis países com maior número de veículos em uso no mundo [10]. Sem considerar a frota de motocicletas em uso, o OICA (*International Organization of Motor Vehicle Manufacturers*) [11] afirma que, até 2015, existiam mais de 1,2 bilhão de veículos em circulação no mundo. Estimativas projetam até 2,8 bilhões de veículos até 2036 [12, 13]. Devido à dificuldade e ao alto custo para extensão da infraestrutura viária, especialmente em países de baixa e média renda, a acomodação de um número cada vez maior de veículos nas vias leva à ocorrência de congestionamentos que provocam prejuízos ao meio ambiente e à economia. Reunindo dados sobre 43 países, um detalhado estudo de 2019 da INRIX Analytics analisou o impacto dos congestionamentos na mobilidade urbana [14]. Tal impacto pode variar desde a perda de tempo devido ao período parado no trânsito, a prejuízos na ordem dos bilhões de dólares. Segundo o estudo, entre as cidades mais impactadas por congestionamentos, Bogotá, na Colômbia, é a líder em horas perdidas no trânsito, com média de 191 horas perdidas anualmente por motorista. O Rio de Janeiro vem logo em seguida, com média de 190 horas. Maior metrópole da América do Sul, São Paulo vem em quinto lugar, com média de 152 horas. O estudo também deixa claro o impacto econômico causado pelos congestionamentos. Através da perda de tempo no trânsito e consequente gasto com combustível e emissões de carbono, as 99 horas que o motorista americano passa, em média, parado no trânsito, são responsáveis por gerar um prejuízo anual de U$88 bilhões. Nesta mesma direção, um relatório publicado em 2017 pela mesma companhia [15] aponta uma projeção de U$2,2 trilhões até 2026 devido ao impacto causado por congestionamentos somente nos Estados Unidos. É necessário, portanto, buscar soluções para reduzir tais indicadores.

Congestionamentos ocorrem quando a demanda de viagens excede a capacidade das vias [16, 17]. Uma vez que é inviável aumentar a capacidade das vias à medida que aumenta o número de veículos, soluções baseadas em ITS (*Intelligent Transportation Systems*) surgem como uma opção viável de resolver/minimizar problemas relacionados ao trânsito [5]. Ancoradas na embarcação de dispositivos de comunicação no ambiente automotivo, tais soluções são cada vez mais consideradas por serem um fator crucial para o aumento da segurança e eficiência no trânsito [18]. Impulsionadas (1) pela incorporação de tecnologias de informação/comunicação em veículos (por parte dos fabricantes) e (2) pela alocação de um espectro sem-fio dedicado à comunicação veicular (como parte dos esforços de governos [19]), as chamadas VANETs (*Vehicular Ad-hoc NETworks*) têm como objetivos principais aumentar a eficiência e a segurança das vias [20]. De fato, o aumento da segurança no trânsito é uma das principais motivações para a pesquisa envolvendo VANETs [1]. Indo além dos tradicionais ADAS (*Advanced Driver Assistance Systems*), baseados, entre outros, na embarcação de RADAR (*RAdio Detection And Ranging*), LIDAR (*LIght Detection And Ranging*) e câmeras no veículo, a troca de informações nas redes veiculares possibilita ampliar a visão dos motoristas. Com o aumento da cons-

ciência situacional, é possível, por exemplo, detectar incidentes precocemente [21]. Em uma rede veicular, veículos são equipados com dispositivos que processam e transmitem os dados coletados por sensores como mensagens no meio sem-fio [22]. Por exemplo, por meio da troca periódica de mensagens de estado, contendo dados cinemáticos do veículo (posição, velocidade, etc.) [23], uma interface homem-máquina (HMI – *Human Machine Interface*) pode emitir um alarme sempre que um risco de colisão for detectado. Isto torna o sensoreamento baseado em redes veiculares mais efetivo que nas abordagens tradicionais [12]. Aplicações típicas de detecção de usuários vulneráveis também se beneficiariam desta troca de mensagens, já que os sensores embarcados nos veículos podem não detectá-los corretamente em situações de tráfego complexas devido ao ângulo de visão limitado. Assim, a integração com redes veiculares pode aumentar o campo de visão do motorista e permitir uma maior taxa de detecção de usuários vulneráveis das vias, como pedestres e ciclistas [21]. Segundo Arena *et al.* [24], é importante considerar o uso desenfreado de *smartphones* durante a trajetória de pedestres pela via, cuja distração motiva o desenvolvimento de um sistema de alertas também para tais usuários. Quanto à gestão de congestionamentos, aplicações que integram sensores e redes veiculares permitem que grupos de veículos se locomovam juntos pela mesma faixa na via (*platoons*), controlando sua velocidade e diminuindo a distância intra-veicular. Denominadas C-ACC (*Cooperative Adaptive Cruise Control*), tais aplicações proporcionam uma redução do consumo de combustível, das emissões de carbono e um uso otimizado da infraestrutura viária [12].

O conceito de redes veiculares foi proposto em 2003, pelo ITU (*International Telecommunication Union*)-T (*Telecommunication Standardization Sector*) [25]. Um dos fundamentos que serviu de alicerce para a consolidação do conceito de redes veiculares ocorreu em 1999, quando a agência americana FCC (*Federal Communications Commission*) definiu a alocação da faixa DSRC (*Dedicated Short-Range Communication*) de 75 MHz no espectro de 5,9 GHz para uso exclusivo de comunicações no ambiente veicular [26]. Tal comunicação depende, basicamente, de uma OBU (*OnBoard Unit*) e de uma RSU (*Road-Side Unit*). Enquanto a OBU é embarcada nos veículos, as RSUs são instaladas ao longo da infraestrutura viária, permitindo, entre outros, o prolongamento da rede veicular e o acesso à Internet. Por meio da comunicação V2V (*Vehicle-to-Vehicle*) e V2I (*Vehicle-to-Infrastructure*), é possível municiar motoristas com informações sobre o tráfego em tempo real, bem como gerar alertas de perigos pela recepção de informações de segurança [22]. Nesta direção, a pilha de protocolos WAVE (*Wireless Access in Vehicular Environment*), formada pela família 1609 e pelo padrão IEEE 802.11p, começou a ser proposta pelo IEEE (*Institute of Electrical and Electronics Engineers*) em meados de 2007 [26]. Baseado no IEEE 802.11a e com padronização em 2010 [27], o IEEE 802.11p foi o primeiro padrão desenvolvido visando a comunicação direta entre veículos [28]. Considerado por muitos o padrão de fato para comunicações veiculares, o IEEE 802.11p é uma das principais tecnologias candidatas a permitir a implementação real das redes veiculares [21]. De fato, países

como Alemanha, Austrália e Estados Unidos já iniciaram a implantação do DSRC [29–32].

Por outro lado, países de baixa ou média renda são os mais impactados em termos de acidentes fatais. Além disso, suas cidades estão entre as mais prejudicadas por congestionamentos. Uma vez que a implementação em larga-escala do DSRC em países de mais alta renda ainda não está completa, presume-se que a presença das redes veiculares em países de baixa ou média renda ainda demande que desafios específicos sejam superados. Em termos do financiamento da infraestrutura de comunicação viária, segundo Rhoades *et al.* [33], um dos principais obstáculos à implantação de OBUs e RSUs é o custo de cada unidade. Por exemplo, na listagem realizada por Singh *et al.* [34] dos projetos de veículos conectados por país até 2019, não consta nenhum da América do Sul. Além disso, para que aplicações de segurança baseadas na comunicação entre veículos funcionem de maneira satisfatória, é necessário que pelo menos 60% dos veículos em circulação estejam equipados com uma tecnologia de rádio [35, 36]. Ainda em 2011, Miucic *et al.* [37] afirmaram que poderia levar décadas para que uma taxa de penetração de 95% de dispositivos DSRC fosse alcançada, levando em conta que somente os veículos novos, durante sua fabricação, fossem embarcados com tais dispositivos [2]. Tal dificuldade de implantação pode estar associada à falta de um padrão DSRC universal (há diferenças entre o padrão europeu, japonês e americano) [38], bem como à falta de aplicações que atraiam o interesse dos condutores [2]. Assim, junto aos esforços direcionados ao desenvolvimento, padronização, avaliação e implementação de dispositivos compatíveis com a faixa DSRC, como OBUs e RSUs IEEE 802.11p, também é importante analisar dispositivos alternativos e com menor custo de implementação para atender à demanda por redes veiculares em países cujo volume de investimento é limitado [39, 40]. Neste sentido, devido à sua versatilidade e natureza ubíqua [41], mesmo em países de baixa ou média renda, o uso de *smartphones* pode servir como uma alternativa de baixo custo às OBUs [2]. Para se ter uma ideia, um relatório de outubro de 2019 estima que a taxa de penetração global de *smartphones* em proporção com a população mundial seja de 44,9% até 2020 [2, 42], totalizando mais de 3,5 bilhões de usuários [43]. A China é o país com o maior número de usuários, com mais de 850 milhões até 2019, seguida por Índia (345 milhões) e Estados Unidos (260 milhões). O Brasil possui o quarto maior número de usuários, totalizando mais de 96 milhões [44].

Em termos de poder computacional, *smartphones* modernos superam muitos dos supercomputadores do passado recente [45]. Para ilustrar, com um aplicativo denominado DreamLab, um projeto de pesquisa lançado em 2018 pela Fundação Vodafone e pelo Imperial College London integra inteligência artificial com o poder de processamento ocioso de milhares de *smartphones* para realizar cálculos enquanto os mesmos estão conectados à rede Wi-Fi, reduzindo o tempo de pesquisa de anos para alguns meses [46] – inclusive sendo usado para acelerar pesquisas envolvendo a COVID-19 [47]. Dotados de uma tecnologia de rádio para prover conectividade ao ambiente veicular, dispositivos portados no

interior de veículos poderiam permitir que algumas aplicações específicas colaborassem com o aumento da segurança e da eficiência no trânsito, especialmente em países cuja implementação de soluções de ITS compatíveis com o IEEE 802.11p ainda não esteja ocorrendo devido à falta de aporte financeiro. Apesar dos esforços entre as fabricantes Honda e Qualcomm levar, em 2014, ao desenvolvimento de um *smartphone* compatível com o IEEE 802.11p [48], a literatura ainda aponta a inexistência de um *smartphone* nativamente compatível com tal tecnologia [41]. Das tecnologias disponíveis nos *smartphones*, como NFC (*Near Field Communication*) BLE (*Bluetooth Low Energy*) e redes celulares [2], o Wi-Fi Direct, introduzido em 2010 pela Wi-Fi Alliance [1] e disponível para Android desde a versão 4.0 (*Ice Cream Sandwich*) [38], pode representar uma opção ao IEEE 802.11p para alguns cenários e condições específicas. Pelo Wi-Fi Direct, poderia ser possível integrar pedestres e ciclistas à rede veicular [40]. Para ilustrar, no estudo realizado por Sewalkar *et al.* [41], 82% das soluções de ITS baseadas na comunicação entre veículos e usuários vulneráveis das vias usavam *smartphones*. Por exigir um *hardware* dedicado que possui, entre outros, uma maior potência de transmissão, definitivamente o DSRC é superior ao Wi-Fi Direct [39]. Conforme Rhoades *et al.* [33], o objetivo de métodos alternativos não é substituir o IEEE 802.11p, mas preencher a lacuna entre uma solução de ITS ideal e o estado atual das tecnologias. Integrando bom poder computacional, suporte a sensores como acelerômetro, giroscópio, GNSS (*Global Navigation Satellite System*), além de câmeras e tecnologia de rádio, os *smartphones* modernos podem permitir coletar, processar e transmitir dados cinemáticos, possibilitando a operação de algumas aplicações no contexto das redes veiculares, como aquelas envolvendo veículos e pedestres [41]. Inclusive, em uma conferência realizada em 2017, a Broadcom anunciou um novo *chip* GNSS com precisão de até 30 cm [49]. Atualmente, *smartphones* comerciais, como o Xiaomi Mi 8, já contam com tal capacidade de georreferenciamento [50, 51].

Assim, é possível imaginar o impacto positivo esperado na sociedade moderna a partir da completa implementação das redes veiculares no mundo real. É fundamental, porém, que antes da completa integração em sistemas reais [52], esforços de pesquisa sejam realizados por academia, indústria e governo como forma de avaliar o desempenho de dispositivos, protocolos e padrões de comunicação. Por conta das características do ambiente veicular, onde trocas de dados devem ser realizadas em altas velocidades relativas, com reduzido tempo de contato entre os nós, muitas vezes feitas no limite do alcance do enlace e com obstáculos que podem obstruir o sinal transmitido, é necessário avaliar a rede através de algumas métricas de desempenho. Assim, devido à complexidade e custo de testes práticos [53], onde um grande número de veículos e dispositivos de comunicação, além de pessoal capacitado e local apropriado são necessários, torna-se fundamental que tal avaliação se dê não apenas por meio de experimentos reais, mas também por meio de simulações. Enquanto as simulações permitem a avaliação em larga-escala, os dados obti-

[1] https://www.wi-fi.org/wi-fi-direct

dos em experimentos reais auxiliam na evolução dos modelos de rede, colaborando para a melhoria de protocolos [54]. Mesmo atualmente, ainda é limitado o número de trabalhos que avaliam tecnologias de rádio como o IEEE 802.11p ou o Wi-Fi Direct em condições reais de mobilidade, com veículos se locomovendo em alta velocidade, principalmente se comparado às avaliações por simulações. Dadas algumas simplificações dos modelos de simulação que visam reduzir a demanda computacional, é importante investigar, para um mesmo cenário em comum, o grau de equivalência dos resultados obtidos por um ambiente de simulação em comparação aos obtidos em testes práticos. Tal etapa é importante, já que os resultados sintéticos de simulações podem não refletir todas as situações encontradas no mundo real [55].

1.1 Proposta

A proposta desta tese pode ser dividida entre dois objetivos principais: (1) avaliar o desempenho do padrão IEEE 802.11p usando OBUs e RSUs comerciais; e (2) analisar a viabilidade do Wi-Fi Direct para alguns cenários e condições específicas usando *smartphones*. Em ambos os casos, o mesmo conjunto de métricas de desempenho é analisado, com base em resultados obtidos a partir de testes de campo em um ambiente controlado usando veículos reais, e com base em resultados obtidos a partir de simulações. Assim, o intuito é verificar a fidelidade das ferramentas de simulação em termos de reproduzir o comportamento das redes de comunicação reais.

A avaliação do IEEE 802.11p é realizada usando OBUs e RSUs comerciais. Os experimentos são realizados com base no envio, em *broadcast*, de BSMs (*Basic Safety Messages*). As BSMs, definidas no padrão SAE (*Society of Automotive Engineers*) J2735 [34], são um tipo de mensagem utilizada para a transmissão periódica de informações do estado do veículo, como posição, direção, velocidade e aceleração [22]. Este envio periódico, conhecido como *beaconing* periódico, é a base para a operação de aplicações de segurança em redes veiculares [23, 56]. Através da recepção de BSMs é possível prever a ocorrência de colisões entre veículos. A avaliação consiste de cenários com linha de visada (LoS – *Line-of-Sight*), sem interferência e com transmissões do tipo V2I, onde o veículo transmite BSMs para uma RSU, e V2V, onde as BSMs são transmitidas de um veículo para outro, unidirecionalmente. O impacto de diferentes modulações suportadas pelo IEEE 802.11p, além da influência de diferentes velocidades empregadas pelo veículo também é analisado. Os resultados da experimentação prática são comparados com aqueles obtidos nos simuladores de rede NS-3 (*Network Simulator 3*)[2] [57], cujas operações da camada física são realizadas pelo módulo PhySim[3] [58, 59], e Veins (*Vehicles in Network Simulation*)[4] [60],

[2]https://www.nsnam.org/
[3]https://dsn.tm.kit.edu/english/software_461.php
[4]https://veins.car2x.org/

cuja camada física é tratada pelo *framework* MiXiM (*Mixed Simulator*)[5] [61, 62]. O objetivo é avaliar a equivalência entre o ambiente real e simulado. Um simulador que mimetiza o comportamento obtido por uma aplicação em um teste prático permite maior confiabilidade aos resultados da avaliação de cenários de maior escala.

Já a análise de viabilidade do Wi-Fi Direct é realizada usando *smartphones* comerciais. Os experimentos contam com o envio periódico, em *unicast*, de mensagens de segurança contendo dados cinemáticos. Diferente da avaliação do IEEE 802.11p, a análise de viabilidade do Wi-Fi Direct se dá, principalmente, quanto ao impacto do tempo para estabelecimento da conexão, ou CET (*Connection Establishment Time*) [2]. Ademais, a análise do Wi-Fi Direct consiste de cenários com e sem linha de visada (NLoS – *Non-Line-of-Sight*), também sem interferência, mas com transmissão do tipo V2P (*Vehicle-to-Pedestrian*), onde um pedestre transmite mensagens de segurança a um veículo que se aproxima. O objetivo é analisar a viabilidade do Wi-Fi Direct em permitir a operação de uma aplicação de prevenção de colisão envolvendo veículo e pedestre. Esta análise se dá quanto ao impacto do CET em diferentes velocidades empregadas pelo veículo. Um CET longo pode fazer com que a mensagem de segurança não seja recebida em tempo hábil no veículo, diminuindo a janela de atuação da aplicação e, consequentemente, fazendo com que o tempo disponível para que o veículo pare por completo após o acionamento dos freios seja insuficiente. Como no IEEE 802.11p, os resultados dos testes práticos com Wi-Fi Direct foram comparados aos obtidos no módulo de simulação do *framework* INET[6] [63]. Novamente, o objetivo é avaliar a equivalência entre os ambientes.

Na avaliação de desempenho do IEEE 802.11p, assim como na análise de viabilidade do Wi-Fi Direct, a forma de medir a similaridade entre os resultados da experimentação prática e simulações se dá através da análise das seguintes métricas:

- **Alcance da Comunicação:** a distância na qual é possível receber mensagens de segurança. É medido com base na taxa de entrega de mensagens de segurança em função da distância entre transmissor e receptor.

- **PDR (*Packet Delivery Ratio*)**: indica o percentual de mensagens de segurança recebidas em função do total de mensagens de segurança transmitidas.

- **PIR (*Packet Inter-Reception*) *time***: intervalo entre a recepção de duas mensagens de segurança. Indica o nível de conscientização situacional [23], já que por meio da recepção destas mensagens, o motorista se torna consciente da posição, velocidade e demais dados dos veículos ao seu redor. Segundo Elbatt *et al.* [64], diferente da latência fim-a-fim, que não é adequada para capturar o desempenho de aplicações de segurança baseadas em transmissões periódicas em *broadcast* – já que consi-

[5] http://mixim.sourceforge.net/
[6] https://inet.omnetpp.org/

dera apenas pacotes entregues com sucesso –, o PIR permite capturar o impacto das sucessivas perdas e colisões de pacotes no desempenho.

Após avaliar se os resultados obtidos pelo INET eram equivalentes aos do teste prático feito na análise de viabilidade do Wi-Fi Direct, é feita a avaliação, por simulações, de um método simples de transmissão de mensagens de segurança por meio da inserção do conteúdo da mensagem no nome do dispositivo Wi-Fi Direct, nome este que é propagado na rede através da transmissão de quadros de controle (como *beacons*). Este método é baseado em uma técnica denominada *beacon-stuffing* [65]. Por meio desta técnica, é possível modificar, por exemplo, o SSID (*Service Set IDentifier*) de uma rede Wi-Fi, ou no caso do Wi-Fi Direct, o nome do dispositivo. Este método pode ser especialmente interessante para transmissão de pequenas quantidades de dados [66]. Mesmo que o método em questão possa aumentar o tempo entre recepções das mensagens de segurança em comparação ao tempo entre mensagens transmitidas após o estabelecimento da conexão (devido à alternância entre fases do Wi-Fi Direct na etapa de descoberta de nós na rede), a avaliação se baseia na premissa de que a recepção de apenas uma mensagem é suficiente para garantir a atuação da aplicação de segurança, conforme destacado por Dhondge *et al.* [67]. A avaliação também se dá em um cenário com condições NLoS e transmissão V2P, porém desta vez em um ambiente com interferência gerada por transmissões concorrentes de outros nós. Neste caso, a métrica avaliada é o número de mensagens de segurança recebidas durante o trajeto do veículo em direção ao pedestre.

1.2 Delimitação

Devido ao custo e à complexidade de realização de testes práticos com veículos e dispositivos reais, a avaliação do IEEE 802.11p consistiu de apenas dois veículos, bem como duas OBUs e uma RSU. Naturalmente, os resultados das métricas avaliadas não seriam os mesmos de uma rede veicular em uma situação de tráfego intenso, com centenas ou milhares de veículos ocupando um dado perímetro da via. Como a avaliação é baseada em uma aplicação de *beaconing* periódico, onde as BSMs são transmitidas com frequência e potência de transmissão fixas, um dos eventos que poderia acontecer em um cenário com alta densidade seria o *broadcast storm* – que satura a largura de banda do canal devido ao excesso de transmissões em *broadcast* [22]. No IEEE 802.11p, o *broadcast storm* gera um aumento de colisões entre as mensagens transmitidas, levando à perda das mensagens e, desta forma, ao menor nível de conscientização situacional. Por isso, a escalabilidade oferecida pelas simulações é a principal motivação para a avaliação da equivalência entre os resultados dos testes práticos e das simulações. O mesmo vale para os testes práticos realizados na análise de viabilidade do Wi-Fi Direct.

Com relação à análise de viabilidade do Wi-Fi Direct, é importante mencionar que a

necessidade de tocar na tela do dispositivo para seleção do nó ao qual se deseja conectar foi desconsiderada nos experimentos. Isto foi feito pois a conexão pode ser feita invocando o método de conexão do Wi-Fi Direct e passando diretamente o ID do dispositivo desejado. Por exemplo, este ID pode ser obtido após filtrar, entre os dispositivos descobertos na rede, aquele que possui em seu nome uma *string* que identifica uma dada aplicação, como uma aplicação que transmite um fluxo de vídeo em tempo real para o auxílio à ultrapassagem de um veículo cujo motorista está com a visão bloqueada devido à presença de um veículo de grande porte à frente. O mesmo se deu para a transmissão das mensagens de segurança. Tão logo a conexão foi estabelecida, o pedestre transmitiu as mensagens via *socket* UDP (*User Datagram Protocol*) ao veículo, sem que fosse necessário tocar na tela para iniciar a transmissão. De igual modo, o atraso da interação do usuário com a tela para aceitar, por meio do clique de um botão, o estabelecimento da conexão, também foi desconsiderado. Durante os experimentos, o aceite da conexão já havia sido dado no dispositivo. De acordo com o nosso conhecimento, o aceite da conexão é um requisito de segurança obrigatório, que só pode ser ignorado fazendo *root* no dispositivo e modificando o Android. Deve-se ressaltar também que a análise de viabilidade do Wi-Fi Direct não propõe uma aplicação de prevenção de colisão entre veículo e pedestre. Apesar do envio de mensagens de segurança em um cenário V2P, nenhum tratamento foi feito para identificar o risco de colisão após a recepção da mensagem. Há apenas uma análise *offline*, onde foi avaliado se seria possível parar o veículo em tempo, após a recepção da mensagem, com base nos dados cinemáticos do pedestre. Assume-se que, após a recepção, uma aplicação alertaria o motorista do risco de colisão. Diferente de [68], questões envolvendo consumo de bateria, gatilhos de início da aplicação e critérios para envio dos alertas – típicas de uma aplicação para prevenção de colisões envolvendo *smartphones* – não foram consideradas.

Também é importante destacar a simplicidade do método de transmissão baseado no *beacon-stuffing* [65]. Ao contrário de [65–67, 69], não há definição de quantos bytes são necessários para acondicionar campos como ID do emissor da mensagem, ID da mensagem, *payload*, etc. Na avaliação do método, feita em um pequeno cenário real e por meio de simulações, apenas uma *string* de dados fixa – onde apenas o campo ID/contador da mensagem era incrementado – foi usada para representar alguns campos cinemáticos que compõem uma mensagem de segurança padrão. O objetivo foi apenas avaliar se o método seria capaz de transmitir dados via modificação do nome do dispositivo Wi-Fi Direct, verificando se tal modificação seria percebida na recepção (teste prático), além de verificar se seria possível aumentar a distância de recepção dos alertas enviados em condições NLoS (simulações), em comparação à distância obtida com o método baseado na formação de grupo. Não foi levado em conta as especificidades que um protocolo de comunicação exige, como gatilhos de ativação/desativação do método de transmissão, definição de campos/codificação/tamanho dos dados a serem inseridos no nome do dispositivo Wi-Fi Direct, mecanismos de alternância entre estados visando comunicação bidirecional, ar-

mazenamento para retransmissão de alertas, entre outros. Por exemplo, diferente de [69] que usa Base94 como codificador, no método avaliado nesta tese nenhuma técnica foi utilizada para otimizar o uso do espaço de 32 bytes disponíveis para compor os dados da mensagem de segurança a ser disseminada na rede. Além disso, a avaliação, feita através de testes práticos, se deu em um cenário simples, com os *smartphones* posicionados lado a lado durante o experimento, sem interferência e com a coleta de dados georreferenciados via receptor GNSS desabilitada. O motivo para desativar a coleta de dados georreferenciados foi eliminar possíveis problemas de desempenho causados por especificidades de *hardware*.

1.3 Justificativa

Segundo Shimizu *et al.* [70], Anwar *et al.* [28] e Masini *et al.* [71], as principais tecnologias de rádio candidatas a levar conectividade aos veículos são as baseadas em DSRC (IEEE 802.11p) e redes celulares (LTE-V2X). Segundo Singh *et al.* [34], lançada em 2014 pelo 3GPP (*Third Generation Partnership Project*) através da *Release* 12, e com revisão feita na *Release* 13, a tecnologia LTE-A ProSe (*Long Term Evolution Advanced Proximity Services*) permite comunicação direta do tipo D2D (*Device-to-Device*). Nesta tecnologia, UEs (*User Equipments*) podem se comunicar diretamente via rede celular sem a necessidade de intermediação através da estação base. Porém, segundo os autores, a comunicação D2D das *Releases* 12 e 13 não é adequada para as condições de alta mobilidade e densidade do ambiente veicular. Já o C-V2X (*Cellular Vehicle-to-Everything*), lançado em 2016 na *Release* 14 pelo 3GPP, é uma evolução da versão LTE-A ProSe. Também conhecida como LTE-V2X, foi projetada especificamente para permitir a comunicação direta entre veículos. Segundo Masini *et al.* [71], o LTE-V2X se caracteriza como a primeira solução baseada em redes celulares que permite a alocação de recursos e a comunicação direta, em condições de alta mobilidade, sem que seja necessário que o UE esteja dentro da cobertura celular fornecida pela estação base. Além do DSRC e redes LTE-A ProSe e LTE-V2X, o advento de tecnologias como VLC (*Visible Light Communication*), IEEE 802.11ad, IEEE 802.11bd e 5G NR (*New Radio*), permitirá uma revolução nos sistemas inteligentes de transporte, definindo um novo marco na direção de veículos.

Apesar disso, a avaliação do IEEE 802.11p se deu por algumas razões. Concluído em 2010 e revisado em 2012 [34], o IEEE 802.11p é visto como o padrão de comunicação mais maduro para veículos conectados. Ao contrário do C-V2X, cujos primeiros experimentos foram feitos no fim de 2017 [72], ao longo de pelo menos 10 anos diferentes tipos de dispositivos (como OBUs e RSUs) e módulos de simulação compatíveis com o IEEE 802.11p foram desenvolvidos. Isto permitiu que seu comportamento fosse estudado em diferentes trabalhos, por testes práticos e simulações. O resultado é que o IEEE 802.11p é considerado bastante confiável [28]. Embora algumas tecnologias como

o 5G NR e IEEE 802.11bd sejam superiores ao IEEE 802.11p, é difícil prever quando as mesmas estarão disponíveis para uso. Por exemplo, conforme o edital do leilão de frequências aprovado pela Anatel (Agência Nacional de Telecomunicações), a previsão é que todas as cidades do Brasil com mais de 30 mil habitantes tenham o 5G apenas por volta de julho de 2029 [73]. Já o IEEE 802.11p, por já ser uma tecnologia pronta para uso [28], pode de imediato ser implementado em veículos. Por exemplo, há diversas fabricantes de *chips* compatíveis com o padrão IEEE 802.11p atualmente, como ARADA Systems, Cohda Wireless, Kapsch TrafficCom e Marvell [74]. A Cohda Wireless[7], cujo *hardware* foi usado em 60% dos experimentos visando a comunicação entre veículos, está no mercado desde 2004[8]. Inclusive, suas soluções contendo *chips* compatíveis com o padrão IEEE 802.11p foram implementadas pela Volkswagen no Golf de oitava geração [75, 76]. Por fim, dada a premissa de conexão total baseada em redes heterogêneas, tecnologias como o IEEE 802.11p ainda terão espaço mesmo após o advento do 5G, complementando-o especialmente para aplicações de segurança de curto alcance, como prevenção de colisões [12].

Já o uso do Wi-Fi Direct, no contexto dos *smartphones*, como opção ao IEEE 802.11p para alguns cenários também se deu por algumas razões. Primeiro, por sua alta disponibilidade. Segundo Khan *et al.* [77], a maior parte dos *smartphones* Android suporta o Wi-Fi Direct. Como já mencionado, o Wi-Fi Direct está disponível para Android desde a versão 4.0, de 2011 [38]. Além disso, em comparação às demais tecnologias de rádio disponíveis em *smartphones* (NFC, BLE e redes celulares), o Wi-Fi Direct possui algumas vantagens. Em termos de alcance, o NFC não é cogitado devido ao alcance $\leq$10 cm [2]. Segundo Frank *et al.* [78], o alcance do BLE é de até 100 m, e experimentos com veículos em condições reais de tráfego mostraram que este variou entre 60 m e 100 m [2, 78]. Enquanto isso, o Wi-Fi Direct oferece um alcance teórico de até 200 m [77]. Já em relação à taxa de transferência, enquanto a taxa máxima do BLE é de apenas 1 Mbps [79, 80], no Wi-Fi Direct é 250 Mbps [77], quase 10 vezes superior à taxa máxima do IEEE 802.11p [79]. Além disso, segundo Jeong *et al.* [79], a latência fim-a-fim no Wi-Fi Direct é inferior à obtida no 4G. Conforme Park *et al.* [81], em alguns casos a latência fim-a-fim obtida por redes celulares pode não ser adequada para aplicações de segurança com requisitos estritos de latência ($\leq$100 ms) [2]. É importante mencionar que o estabelecimento de conexão é desafiador em áreas rurais, já que mesmo a comunicação por redes celulares tende a sofrer com desconexões. Por outro lado, por sua comunicação local que não exige infraestrutura, o Wi-Fi Direct poderia ser usado mesmo onde não há cobertura celular. O Wi-Fi Direct também não onera os usuários em termos da carga gerada na rede, como em redes celulares. Por exemplo, Zeadally *et al.* [12] mencionam que, implementada a rede 5G, os custos desta implementação deverão ser repassados aos interessados em usar as soluções disponíveis.

[7] https://cohdawireless.com/

[8] https://cohdawireless.com/about-cohda-wireless/about/

Baseado no exemplo dado por Jeong *et al.* [2], dada uma BSM de 50 bytes transmitida à taxa de 10 Hz, uma carga de 1,72 MB por hora seria gerada. Assim, o custo para o usuário e a sobrecarga da rede celular devem ser considerados. Também é importante ressaltar que o Wi-Fi Direct é projetado, geralmente, para ambientes estacionários [79], o que leva à necessidade de avaliar a viabilidade de uso em veículos por meio da análise do CET.

Por fim, devido ao custo financeiro e à complexidade de escalar testes práticos contendo um grande número de veículos, dispositivos de comunicação, pessoal capacitado e local apropriado, a maior parte dos trabalhos envolvendo a comunicação entre veículos em larga-escala – com centenas ou milhares de nós – é feita por meio de simulações. Desta forma, é importante avaliar a equivalência dos resultados obtidos por simuladores de rede em comparação àqueles obtidos por meio de testes práticos. Isto poderia ser útil aos pesquisadores interessados em redes veiculares, contribuindo para o desenvolvimento e avaliação de novos protocolos e algoritmos no ambiente de simulação.

1.4 Objetivos

São objetivos desta tese:

- Avaliar o desempenho do IEEE 802.11p por meio da transmissão periódica e em *broadcast* de BSMs. A avaliação será feita com base em experimentos reais usando OBUs e RSUs comerciais, além de simulações executadas nos simuladores NS-3/PhySim e Veins/MiXiM. Um dos objetivos é avaliar a equivalência dos resultados obtidos em ambos os ambientes. Nas simulações, os parâmetros de configuração serão definidos de forma a tentar refletir as mesmas condições encontradas nos experimentos reais, como efeitos da mobilidade e aumento da distância entre os veículos.

- Analisar a viabilidade do Wi-Fi Direct em redes veiculares por meio da transmissão em *unicast* de mensagens de segurança. Com base em um cenário de travessia de pedestres em uma via com tráfego de veículos, a avaliação será realizada usando *smartphones* comerciais, além de simulações no módulo de simulação do *framework* INET. Como no IEEE 802.11p, um dos objetivos é avaliar a equivalência dos resultados em ambos os ambientes. Novamente, os parâmetros das simulações serão definidos de forma a tentar refletir as condições dos experimentos reais. Neste contexto, um método de transmissão baseado em *beacon-stuffing* [65] também será avaliado.

1.5 Estrutura do Texto

O restante deste documento está organizado da seguinte forma. No Capítulo 2 é feita uma revisão bibliográfica que contempla a fundamentação teórica desta tese, enquanto no

Capítulo 3 são mostrados os trabalhos que serviram de inspiração para o seu desenvolvimento. Os Capítulos 4 e 5 detalham, respectivamente, o modo de configuração e os resultados dos experimentos práticos e simulações da avaliação de desempenho do IEEE 802.11p. Já os Capítulos 6 e 7 apresentam, respectivamente, o modo de configuração e os resultados da análise de viabilidade do Wi-Fi Direct. Por fim, o Capítulo 8 aborda as conclusões finais e os trabalhos futuros.

Capítulo 2

Fundamentação Teórica

Este capítulo apresenta os conceitos fundamentais que auxiliam o entendimento desta tese. Inicialmente, são apresentados os principais conceitos envolvendo redes veiculares, como suas diferenças para MANETs (*Mobile Ad-hoc NETwork*), arquitetura, tipos de comunicação, bem como categorias de aplicações. Dado que uma década se passou desde a padronização do IEEE 802.11p, é realizada uma análise para situá-lo frente a tecnologias emergentes, em especial, o 5G NR. O capítulo segue apresentando as especificações técnicas do IEEE 802.11p e do Wi-Fi Direct. Por fim, uma visão geral sobre a simulação de redes veiculares é apresentada, com detalhes dos simuladores NS-3/PhySim, Veins/MiXiM e INET.

2.1 Redes Veiculares

Segundo Singh *et al.* [34], o primeiro vislumbre da comunicação entre veículos aconteceu em 1939, na Feira Mundial de Nova York, por meio do modelo proposto por Norman Bel Geddes na exibição "Futurama". Um protótipo deste sistema viria a ser construído pela General Motors em 1960. Ao passo em que veículos começavam a ser embarcados com processadores e sensores [33], a possibilidade de tornar real a comunicação entre veículos já era uma ideia que existia entre os pesquisadores desde a década de 80 [19], quando as primeiras soluções de ITS começaram a ser propostas. Segundo Singh *et al.* [34], em 1986 foi fundado o primeiro programa de pesquisa dos Estados Unidos com foco em ITS, denominado "California PATH Program". Inclusive, o NITSA (*National* ITS *Architecture*), que guia o planejamento e a implementação de ITS nos Estados Unidos [82], define a comunicação sem-fio como um fator preponderante para permitir a implementação de soluções de ITS [34]. Dos projetos iniciais desenvolvidos nas décadas de 80 e 90, passando pela realidade iminente dos veículos autônomos, a comunicação entre veículos passou por inúmeras transformações e desafios. Muitos, inclusive, ainda precisam ser superados para que a conectividade no ambiente veicular leve ao aumento da segurança e da eficiência

no trânsito. Antes encarada como um tipo de MANET [83] devido às suas características em comum – como a comunicação realizada por nós em condições de mobilidade –, as redes veiculares são entendidas hoje como um tipo de rede com características próprias e desafios únicos no âmbito da comunicação, mas com potencial de salvar vidas e melhorar a mobilidade urbana.

2.1.1 Distinções entre Redes Veiculares e MANETs

Ações de governos, academia e indústria possibilitaram que alguns países, como Alemanha, Austrália e Estados Unidos, atualmente já contem parcialmente com uma infraestrutura instalada para permitir a comunicação entre veículos equipados com OBUs. Entre outros, isto se deve ao fato de que o investimento em soluções de ITS tem se mostrado uma alternativa mais viável em comparação a medidas tradicionais, como a ampliação de vias de forma a comportar o crescente número de veículos. Por exemplo, na cidade de Ludwigsburg, na Alemanha, todos os semáforos/cruzamentos foram equipados com RSUs modelo MK5 da Cohda Wireless, enquanto caminhões de bombeiros e veículos de resgate foram equipados com OBUs de mesmo modelo [29]. O objetivo foi garantir a prioridade de passagem destes veículos em situações de emergência. Entretanto, no contexto das implementações reais, é necessário considerar algumas características que diferenciam as redes veiculares das tradicionais MANETs, já que tais características podem impor desafios à efetiva implementação destas redes em um ambiente tão dinâmico como o veicular. Segundo Al-Sultan *et al.* [22] e Hartenstein *et al.* [19], as principais diferenças entre as duas redes são:

- Mobilidade previsível: o movimento dos nós (veículos) nas redes veiculares está restrito à topologia e aos limites impostos pelas vias, à obrigatoriedade de obedecer a elementos de sinalização e controle de trânsito (placas, semáforos), e de se adaptar ao movimento dos demais veículos (condições de trânsito).

- Sem restrições de energia e alto poder computacional: o consumo de energia não é um fator restritivo nas redes veiculares, dado que a bateria dos veículos oferece às OBUs uma fonte de energia quase inesgotável. Além disso, veículos modernos contam com razoável capacidade de memória, processamento e armazenamento, além de tecnologias avançadas de antena e receptor GNSS, os quais melhoram a qualidade da transmissão sem-fio e a acurácia dos dados de georreferenciamento.

- Densidade variável e rápidas mudanças na topologia da rede: a densidade da rede veicular é variável, mudando de acordo com a densidade de veículos na via. Além disso, as altas velocidades relativas, características do ambiente veicular, podem levar a rápidas mudanças na topologia da rede, fazendo com que o enlace sem-fio seja afetado pelo alcance da comunicação e pelo sentido de direção dos veículos.

- Impacto na propagação de rádio: nas redes veiculares, aspectos ambientais como a alocação de antenas em condições de altura adequadas e a atenuação do sinal provocada pela reflexão das ondas no metal dos veículos devem ser considerados.

2.1.2 Arquitetura das Redes Veiculares

A arquitetura das redes veiculares pode ser caracterizada pelos diferentes componentes e domínios de comunicação que permeiam a conectividade entre veículos e possibilitam a operação de soluções de ITS. Segundo Sing *et al.* [34] e Al-Sultan *et al.* [22], quatro domínios de comunicação podem ser definidos:

- Domínio intra-veicular: inclui CCU (*Communications Control Unit*), OBU e HMI. Contando com diferentes interfaces de rádio, a CCU permite a interação com várias tecnologias de acesso ao meio sem-fio, como DSRC, Wi-Fi e redes celulares. Ela também habilita a integração de receptores GNSS, RADAR, câmera e LIDAR, bem como o uso, na OBU, de dados coletados por meio da rede CAN (*Controller Area Network*) do veículo. Já a OBU conta com recursos computacionais de *hardware* (processamento, memória, armazenamento e capacidade de comunicação) e *software* que permitem a execução de soluções de ITS. Também são funções da OBU a transmissão confiável de dados, questões relacionadas à segurança, mobilidade IP, entre outros. Nesta tese, assume-se que CCU e OBU fazem parte da mesma unidade física. Por fim, a HMI, usando os recursos da OBU e CCU, orienta os motoristas através de alarmes sonoros ou visuais, por exemplo, relacionados à atuação de uma aplicação de segurança.

- Domínio *ad-hoc*: neste domínio, formado por veículos e RSUs, a criação da rede se dá de forma espontânea. A RSU, normalmente instalada ao longo da infraestrutura viária ou em locais específicos como cruzamentos, é um dispositivo compatível com o IEEE 802.11p mas que também pode ser equipado com outras interfaces de rede, permitindo a integração da rede veicular com uma rede infraestruturada. As principais funções da RSU são: (1) estender o alcance de comunicação da rede *ad-hoc*, retransmitindo mensagens para OBUs ou outras RSUs; (2) executar aplicações de segurança, como alertas indicando a presença de zonas de trabalho na via; e (3) fornecer acesso à Internet para OBUs.

- Domínio infraestruturado: formado por dispositivos sem-fio instalados na infraestrutura viária – como RSUs (DSRC), estações base (*evolved Node B* – eNodeB) e APs Wi-Fi –, ligados a uma rede cabeada infraestruturada formada por *switches*, roteadores, etc. O objetivo desta ligação é permitir a conectividade entre veículos e o domínio de serviços.

- Domínio de serviços: fornece serviços aos veículos usando o domínio infraestruturado. Os serviços podem ser de dois tipos: (1) relacionados ao trânsito, fornecidos por autoridades que administram a via; e (2) genéricos, como o acesso à Internet fornecido às OBUs.

2.1.3 Tipos de Comunicação em Redes Veiculares

A implementação de redes veiculares permite reduzir a formação de congestionamentos e tornar o ato de dirigir mais confortável. Acima de tudo, um dos principais benefícios é o aumento da segurança nas vias, caracterizado pela prevenção de acidentes. Estes benefícios só são alcançados por intermédio da troca de mensagens contendo informações cinemáticas relevantes, como a posição, direção e velocidade de um veículo. Conforme Al-Sultan *et al.* [22] e Sing *et al.* [34], baseado nas entidades envolvidas nesta troca de mensagens, a comunicação em uma rede veicular pode ser categorizada como:

1. *Vehicle-to-Vehicle*, ou V2V: caracteriza-se pela comunicação direta entre veículos, sem o suporte de uma infraestrutura, como uma RSU. Consiste na transmissão de dados coletados e processados por sensores embarcados no veículo, enviados como mensagem usando os recursos de comunicação da OBU. O termo VANET também é empregado para caracterizar esta comunicação *ad-hoc* entre veículos.

2. *Vehicle-to-Infrastructure*, ou V2I: caracteriza-se pela comunicação entre veículos e dispositivos instalados ao longo da infraestrutura, como RSUs, visando promover a conectividade em condições de baixa densidade de veículos, oferecer acesso à Internet para OBUs, ou outras aplicações que requeiram comunicação com a infraestrutura da via, como semáforos inteligentes.

   A Figura 2.1 apresenta um cenário com exemplos de comunicação V2V e V2I.

Além dos dois tipos de comunicação clássicos mencionados, o advento do paradigma de IoV (*Internet of Vehicles*) também fez surgir o tipo de comunicação denominado V2X (*Vehicle-to-Everything*). Segundo Ji *et al.* [25], a comunicação V2X se dá pela interseção entre soluções de ITS com a presença massiva de dispositivos IoT (*Internet of Things*), de tecnologias como o 5G, e da aplicação de conceitos como *big data* e IA (*Intelligence Artificial*). Ainda segundo Ji *et al.*, a comunicação V2X consiste na troca de dados entre os veículos e todas as entidades que podem afetá-lo. Assim, além dos tipos V2V e V2I, compõem o V2X a comunicação entre veículos e a infraestrutura viária (V2R – *Vehicle-to-Roadside*), veículos e sensores (V2S – *Vehicle-to-Sensors*), e veículos e pedestres (V2P).

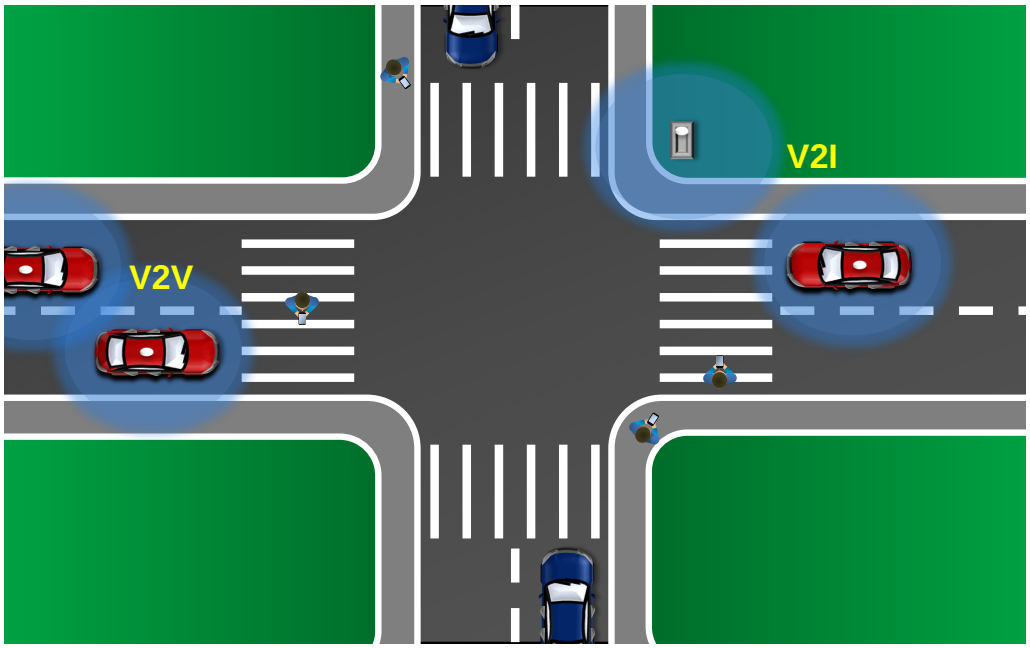

Figura 2.1: Cenário com comunicações V2V e V2I.

2.1.4 Categorias de Aplicações em Redes Veiculares

A capacidade de comunicação entre veículos e as demais entidades, como RSUs, possui o poder de promover as soluções de ITS. Aplicações baseadas em redes veiculares são fonte de valiosa informação para motoristas e outros usuários da via, podendo por exemplo ser usadas para prever colisões e evitar rotas com congestionamentos. De acordo com Al-Sultan *et al.* [22] e Sharma *et al.* [20], é possível classificar as aplicações em redes veiculares como:

- Aplicações de segurança: tem como meta aumentar a segurança da via a partir da prevenção de acidentes. Para isso, dois tipos de mensagens são disseminadas: *beacons* periódicos e mensagens direcionadas a eventos. *Beacons* são transmitidos periodicamente carregando dados do transmissor, como posição, velocidade e sentido de direção do veículo. Obtidas por sensores, estas informações podem ser usadas pelo receptor para calcular uma possível colisão. Já mensagens direcionadas a eventos possuem alta prioridade e são enviadas após a detecção de uma condição perigosa, como um acidente. Aplicações de segurança podem ser categorizadas como:
  - Prevenção de colisões em interseções: previne colisões em cruzamentos como forma de reduzir acidentes. Exemplos: *Traffic Signal Violation Warning*, *Stop Sign Violation Warning*, *Left Turn Assistant*, e *Intersection Collision Warning*.
  - Segurança pública: facilita o trânsito de veículos relacionados à segurança pública. Por exemplo, ao tornar a chegada de veículos de emergência (como ambulâncias) ao local do acidente o mais breve possível, uma vez que atrasos

não podem ser tolerados. Exemplos: *Approaching Emergency Vehicle Warning*, *Emergency Vehicle Signal Preemption*, *SOS (Save yOur Souls) Services*, e *Post-Crash Warning*.

  - Sinalização estendida: evita acidentes enviando alertas aos motoristas sobre a importância de focar na sinalização. Exemplos: *Curve Speed Warning*, *Wrong Way Driver Warning*, *Low Bridge Warning*, e *Work Zone Warning*.
  - Manutenção e diagnóstico do veículo: alerta os motoristas sobre a necessidade de realizar uma manutenção no veículo. Exemplos: *Safety Recall Notice* e *Just-in-Time Repair Notification*.
  - Informações de outros veículos: aumenta a segurança usando informações obtidas via comunicação V2V e V2I. Exemplos: *Cooperative Forward Collision Warning*, *Emergency Electronic Brake Lights*, *Lane Change Warning* e *Cooperative Adaptive Cruise Control*.

- Aplicações de entretenimento e conforto: têm como meta tornar o ato de dirigir mais confortável e melhorar a eficiência do trânsito. Por exemplo, informa aos motoristas as condições de trechos futuros, possibilitando a alteração da rota. Também permitem que informações sobre pontos de interesse, como hotéis disponíveis, sejam disseminadas na rede. Exemplos: *Intelligent Parking Navigation System*, *Internet Service Provisioning*, *Road Congestion Management*, e *Electronic Toll Collection*.

É possível afirmar que a principal motivação em prover a comunicação entre veículos está em reduzir o número de acidentes de trânsito. Ao contrário de aplicações de entretenimento e conforto, aplicações de segurança possuem requisitos de operação mais estritos. Segundo Hartenstein *et al.* [19] e Karagiannis *et al.* [84], o Consórcio VSC (*Vehicle Safety Communications*) define que aplicações de segurança devem possuir latência máxima de 100 ms, frequência de transmissão de 10 Hz e alcance de comunicação mínimo de 150 m. A Figura 2.2 ilustra uma aplicação de segurança (*Lane Change Warning*). No primeiro momento, a mudança de faixa do veículo vermelho (ID 2) o coloca em rota de colisão com o veículo verde (ID 1), já que ambos não possuem capacidade de comunicação. Já no segundo momento, pela troca de BSMs, o veículo identifica o risco de colisão, e aguarda o melhor momento para mudar de faixa.

2.1.5 Redes Veiculares: Hoje – Veículos Conectados

É possível definir que, em diferentes níveis, estamos vivendo a era dos veículos conectados. Segundo Singh *et al.* [34], por meio da comunicação V2X, veículos conectados se comunicam uns com os outros e com as demais entidades do ambiente veicular. Com isso, aplicações podem fornecer informações valiosas para motoristas e demais ocupantes do veículo, além de pedestres, ciclistas e agências de transporte. Ao contrário dos veículos

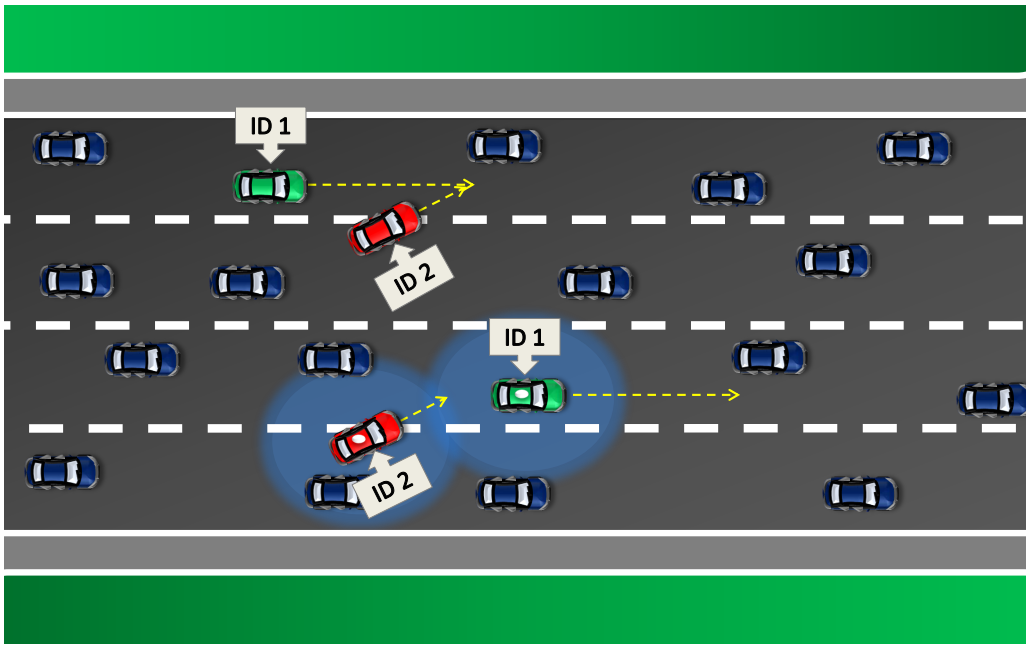

Figura 2.2: Exemplo de uma aplicação de auxílio para troca de faixa.

autônomos – ou autônomos e ao mesmo tempo conectados –, veículos conectados ainda requerem algum tipo de interação do motorista, dado que não possuem um grau de autonomia completa. Por exemplo, na aplicação de alerta de mudança de faixa (Figura 2.2), existe o risco de colisão se o motorista tenta mudar de faixa. Neste caso, um alarme será acionado se houver qualquer perigo em continuar a manobra, possibilitando ao motorista aguardar o momento mais seguro. Aplicações deste tipo, também conhecidas como Dia 1 e Dia 1.5 [71], são baseadas principalmente na troca de mensagens contendo dados cinemáticos coletados por sensores, cujo volume transmitido é suportado pela maioria, se não todas, tecnologias de rádio disponíveis atualmente.

Aplicações com algum nível de autonomia, como aplicações para controle de movimento de grupo, que usam sensores e dados externos para controlar o comportamento de veículos e motoristas em conjunto, também são suportadas. Um exemplo são aplicações *platooning* (ou comboio), que mantêm veículos encadeados dinamicamente visando economizar combustível e maximizar o uso do espaço viário a partir do controle da velocidade e da distância entre os veículos [35]. Por exemplo, em [85], testes iniciais envolvendo veículos em diferentes casos de uso de um *platoon*, como entrar e sair do grupo, manobras de curva em S, entre outros, foram feitos pela Cohda Wireless, fabricante de *hardware* compatível com C-V2X e IEEE 802.11p. Segundo Singh *et al.* [34], as principais tecnologias de rádio na era dos veículos conectados são baseadas no DSRC (IEEE 802.11p), seguido por LTE-A ProSe e C-V2X (LTE-V2X). Em menor grau, as tecnologias compatíveis com VLC (baseadas na comunicação por luz visível), pelos desafios a serem superados para tornar seu uso viável. Wi-Fi e LTE/LTE-A (*Releases* 8 a 12) também podem ser citados. A seguir, uma descrição das principais tecnologias para veículos conectados é apresentada.

DSRC/IEEE802.11p

Segundo Karagiannis *et al.* [84], os primeiros serviços de ITS – como cobrança automática de pedágio – dos Estados Unidos usavam um espectro de frequências pequeno, entre 902 MHz e 928 MHz. Isto levou ao NITSA a solicitar à FCC, em 1997, a alocação de um espectro de 75 MHz na faixa de 5,9 GHz para DSRC. Esta ação permitiu que, em 1999, o espectro de 75 MHz na faixa de 5,85 GHz a 5,925 GHz fosse alocado para uso exclusivo das aplicações de ITS, especialmente para comunicações confiáveis de baixa latência [34]. Ainda segundo Karagiannis *et al.*, a partir de 2002, a ITSA (*Intelligent Transportation Society of America*), entre outras, recomendou à FCC a adoção de um padrão exclusivo de acesso à faixa DSRC, usando as especificações da ASTM (*American Society for Testing and Materials*) com base no IEEE 802.11 (ASTM E2213-02). Em 2004, o TG (*Task Group*) p iniciou o desenvolvimento de um padrão baseado no IEEE 802.11, dando origem ao padrão IEEE 802.11p. Junto à família IEEE 1609, o IEEE 802.11p forma a pilha de protocolos WAVE. Conforme Singh *et al.* [34], na Europa, a faixa DSRC é alocada pelo ECC (*Electronic Communications Committee*), e os padrões são desenvolvidos por ETSI (*European Telecommunications Standards Institute*) e CEN (*Comité Européen de Normalisation*). Quatro são usados: (1) ITS-G5A, 30 MHz na faixa de 5,875 GHz a 5,905 GHz, para aplicações de segurança e eficiência de trânsito; (2) ITS-G5B, 20 MHz na faixa de 5,855 GHz e 5,875 GHz, para aplicações sem foco em segurança; (3) ITS-G5C, limitado à V2I e que compartilha a banda RLAN (*Radio Local Area Network*); e (4) ITS-G5D, 10 MHz na faixa de 5,905 GHz e 5,915 GHz, para aplicações C-ITS (*Cooperative-ITS*) futuras. Similar às BSMs, o ETSI também padronizou o uso de CAMs (*Cooperative Awareness Messages*), que informam o estado do ambiente, e DENs (*Decentralized Environmental Notifications*), para notificações de emergência [35]. Segundo Singh *et al.* [34], no Japão, a faixa DSRC é alocada pelo MIC (*Ministry of Internal Affairs and Communications*), enquanto os padrões são desenvolvidos pela ARIB (*Association of Radio Industries and Businesses*). O espectro de 80 MHz, na faixa de 5,770 GHz a 5,850 GHz é usado pelos padrões ARIB STD-T55 e ARIB STD-T75, apenas para comunicação V2I, e ARIB STD-T88, para V2V e V2I. Além destes três, em 2011 a faixa entre 755,5 MHz e 764,5 MHz foi alocada para o ARIB STD-T109. Visando várias aplicações ITS, o padrão permite maior alcance, operação em condições NLoS e comunicação V2V e V2I.

LTE-A ProSe e C-V2X (LTE-V2X)

Segundo Singh *et al.* [34], nas *Releases* 12 e 13 do 3GPP, foi lançado o conceito de comunicação D2D. Baseado em serviços de proximidade, tal comunicação se caracteriza pela troca de dados feita diretamente entre UEs de uma rede celular, sem a intermediação de uma estação base. Ainda segundo Singh *et al.*, apesar de ter sido projetada com foco em serviços comerciais e de segurança pública, a comunicação LTE-A ProSe vem rece-

bendo melhorias visando suportar aplicações de segurança baseadas na comunicação entre veículos. Já o C-V2X (*Release* 14) – ou LTE-V2X –, uma evolução do LTE-A ProSe, foi projetado especificamente para o ambiente veicular. Segundo Masini *et al.* [71], o LTE-V2X também é denominado *sidelink*, com suas interfaces de comunicação sendo denominadas PC5. Como no IEEE 802.11p, a camada PHY do LTE-V2X é baseada em OFDM, enquanto a camada MAC é baseada em SC-FDMA (*Single Carrier Frequency Division Multiple Access*), conforme *uplink* do LTE. No LTE-V2X, os recursos são alocados de forma direta, e a comunicação ocorre sem que seja necessário estar dentro da cobertura de um eNodeB. Ainda segundo Masini *et al.* [71], em termos da forma como os recursos são alocados, são definidos dois diferentes modos: Modo 3 e Modo 4, sendo que ambos são baseados em comunicação direta (V2V). No Modo 3, ou alocação controlada, os recursos são definidos e alocados pela rede, requerendo que o nó esteja dentro da área de cobertura de algum eNodeB. No Modo 4, ou alocação fora-da-cobertura, cada nó seleciona os recursos a serem usados para comunicação. No Modo 4, a natureza distribuída se assemelha ao modo de operação no IEEE 802.11p. Desde a *Release* 14, o 3GPP tem adicionado melhorias à rede LTE (*Long Term Evolution*) de forma a oferecer comunicação V2X. Segundo Singh *et al.* [34], o objetivo principal do C-V2X é ser capaz de permitir a operação de todas as aplicações ITS suportadas pelo IEEE 802.11p. Por exemplo, desde a *Release* 14, o C-V2X possui suporte à banda de 5,9 GHz.

VLC/IEEE 802.15.7

Segundo Singh *et al.* [34], o VLC/IEEE 802.15.7 é baseado na comunicação por luz visível, na faixa de 380 THz a 800 THz. A comunicação por VLC é feita modulando LEDs (*Light-Emitting Diodes*) em alta velocidade. Ainda segundo Singh *et al.*, ao contrário de tecnologias baseadas em rádio-frequência (como DSRC e C-V2X), tecnologias baseadas em VLC possuem, entre outros, menor complexidade, custo e consumo de energia, além de serem imunes à interferência por radiofrequência. Além disso, apesar da incipiência, pesquisadores veem potencial na comunicação por LEDs para permitir aplicações V2X no futuro, como ACC (*Adaptive Cruise Control*), prevenção de colisões e até direção com algum nível de autonomia. Na comunicação entre veículos, dispositivos compostos por LEDs (como farol e luzes traseiras) e demais fontes de iluminação presentes na infraestrutura viária (como semáforos) funcionariam como um transmissor. Como receptores, poderiam ser usados sensores de imagem e fotodiodos. As camadas PHY (*Physical Layer*) e MAC (*Medium Access Control*) da comunicação por VLC são definidas no padrão IEEE 802.15.7, como parte do WG (*Working Group*) IEEE 802.15. Conforme Singh *et al.*, algumas limitações ainda precisam ser superadas para tornar viável o uso desta tecnologia no ambiente veicular. Por exemplo, a propagação em condições climáticas adversas, como chuva e neblina, que pode afetar o desempenho da comunicação, o baixo alcance de transmissão (inferior a 100 m) e o baixo suporte à mobilidade.

2.1.6 Redes Veiculares: Amanhã – Veículos Conectados e Autônomos

Segundo Singh *et al.* [34], seis níveis de automação de veículos – 0 a 5 – são definidos pelo SAE [86]. No nível 0 não há automação, e todas as manobras são realizadas pelo motorista. No nível 1, um ADAS auxilia o motorista em alguns momentos na direção e na frenagem/aceleração, mas não os dois simultaneamente. No nível 2, esta simultaneidade é permitida em alguns casos, porém é exigido que o motorista permaneça atento e com as mãos ao volante. No nível 3, um ADS (*Advanced Driver System*) pode, em alguns casos, executar todas as manobras de direção, porém o motorista deve estar pronto para retomar o controle quando solicitado pelo sistema. Já no nível 4, um ADS realiza, em alguns casos, todas as manobras de direção. Por fim, no nível 5 a direção é completamente autônoma. Os níveis 3, 4 e 5 ainda estão em fase de pesquisa, enquanto o nível 2 já está disponível. Inclusive, alguns protótipos já foram capazes de se locomover por centenas de milhares de quilômetros de forma autônoma [21]. Nesta direção, Singh *et al.* [34] descreve os testes feitos por Google e Tesla com veículos autônomos. Nestes testes, as decisões de direção são tomadas com base apenas nos dados coletados pelos próprios sensores dos veículos. Sem considerar os dados coletados por outros veículos, a capacidade de sensoreamento fica limitada. Portanto, além de sensores para detecção do ambiente, é necessário que veículos autônomos sejam equipados com tecnologias de rádio capazes de permitir a comunicação com outros veículos da via. Com isso, a consciência situacional é aumentada, permitindo aos veículos autônomos verem além de sua capacidade de sensoreamento. Singh *et al.* definem este paradigma como veículos autônomos e conectados, compostos por LIDAR, RADAR, câmeras, receptores GNSS de alta precisão e tecnologia de rádio V2X.

Projeta-se que, até 2040, 75% do tráfego seja representado por veículos autônomos [87, 88]. De acordo com Bila *et al.* [21], um sistema de direção autônoma consiste de medição, análise e execução. Na medição, dados são capturados por sensores visando detectar, entre outros, pedestres e obstáculos na via. A análise destes dados permitirá a tomada de decisão, e após isso, a execução de uma ação por parte de atuadores. Segundo Singh *et al.* [34], na etapa de medição, o volume de dados gerados pelos sensores embarcados nos veículos autônomos é da ordem de Terabytes por hora. Isto significa uma taxa de geração de dados na ordem de Gbps, muito superior à capacidade das tecnologias de rádio para veículos conectados, como DSRC (IEEE 802.11p), C-V2X (*Release* 14) e VLC (IEEE 802.15.7), que é da ordem de Mbps. Segundo Masini *et al.* [71], no futuro, aplicações V2X não serão baseadas apenas na troca de dados cinemáticos. Segundo os autores, a direção cooperativa, no qual se enquadra a direção autônoma, é uma das áreas que tecnologias de rádio emergentes precisarão lidar, já que o IEEE 802.11p e LTE-V2X não são capazes de atender aos seus requisitos de latência e confiabilidade. Por exemplo, requisitos estritos de veículos autônomos, como latência de 1 ms e PDR próxima a 100%, não são atendidos pelas tecnologias atuais. Neste sentido, Bila *et al.* [21] vislumbram que,

com o aumento de veículos autônomos, os limites de velocidade das cidades poderão ser elevados como forma de aumentar o fluxo de tráfego viário. Segundo os autores, neste ambiente dinâmico, a detecção de objetos usando processamento de imagem em tempo real – feita remotamente e usando *big data* – exigiria, entre outros, comunicações V2X confiáveis, especialmente em termos de latência. Assim, tecnologias emergentes como IEEE 802.11ad, IEEE 802.11bd e 5G NR despontam com potencial para permitir que o paradigma de veículos autônomos e conectados se torne real. A seguir, são apresentadas as descrições destas tecnologias.

IEEE 802.11ad

Segundo Singh *et al.* [34], o IEEE 802.11ad é uma tecnologia baseada na comunicação por mmWave (*millimeter-Wave*). Com espectro na faixa de 30 GHz a 300 GHz, por meio da comunicação mmWave é possível obter canais com ampla largura de banda. O padrão IEEE 802.11ad define os protocolos das camadas PHY e MAC. Por fazer uso da faixa não-licenciada de 60 GHz e com canais com 2,16 GHz de largura, taxas de dados de até 7 Gbps são alcançadas com esta tecnologia. Entretanto, ainda segundo Singh *et al.*, somente pequenas distâncias, de até 10 m, são cobertas pelo padrão. Além disso, o sinal transmitido a 60 GHz requer propagação em LoS, o que torna o sinal sensível aos efeitos gerados pela mobilidade e obstáculos. Por fim, conforme apontado pelos autores, o IEEE 802.11ad foi projetado para ambientes *indoor*, e seu uso em condições de alta mobilidade como o ambiente veicular pode requerer uma revisão no padrão.

IEEE 802.11bd

Para acompanhar a próxima geração de comunicações V2X, o IEEE iniciou, em 2019, sob o WG NGV (WG *Next Generation V2V*) do IEEE 802.11, o TG bd [71], responsável por desenvolver o padrão IEEE 802.11bd – considerado uma evolução do IEEE 802.11p. Segundo Anwar *et al.* [28], conforme o relatório de autorização do projeto (PAR – *Project Authorization Report*), entre os objetivos do IEEE 802.11bd, estão a retrocompatibilidade e interoperabilidade com o IEEE 802.11p, maior confiabilidade, com a redução de colisões e melhora do desempenho em condições de alto *Doppler shift*, e suporte a velocidades de até 250 km/h. Ainda segundo os autores, altas taxas de dados poderiam ser alcançadas usando um esquema de codificação avançado como LDPC (*Low-Density Parity-Check*), MIMO (*Multiple-Input and Multiple-Output*), modulação 256 QAM e canais de 20 MHz. Já um melhor alcance de comunicação (duas vezes maior que no IEEE 802.11p) poderia ser obtido usando DCM (*Dual Carrier Modulation*) e modos de extensão de alcance (baseado no aumento da duração dos símbolos OFDM), ambos adotados do IEEE 802.11ax. Na análise teórica feita em [28], apesar de inferior ao 5G NR-V2X, os resultados de desempenho do IEEE 802.11bd em termos de alcance e vazão foram substancialmente me-

lhores em comparação ao IEEE 802.11p, especialmente em cenários com alto *Doppler shift*. Segundo Anwar *et al.*, isto se deve, principalmente, ao uso de *midambles*, símbolos de referência que são inseridos entre os símbolos de dados para melhorar a estimativa do canal. No IEEE 802.11bd, a frequência de inserção dos *midambles* depende do Doppler *shift* e da modulação. Nas modulações MCS0 a MCS4, a inserção ocorre após cada nove símbolos OFDM. Nas demais modulações, a inserção se dá após cada quatro símbolos.

5G NR

Por permitir conexões mais rápidas e confiáveis com alta largura de banda e mínima latência [89], a implementação do 5G é encarada como fundamental para permitir que o paradigma de veículos autônomos e conectados se torne realidade. Segundo Singh *et al.* [34], nos casos de uso definidos por diferentes organizações como NGMN (*Next Generation Mobile Networks*), *The 5G Forum of Korea*, ITU-R (ITU *Radiocommunication Sector*) e 3GPP SMARTER, a direção autônoma sempre é considerada. Segundo os autores, as principais responsáveis pela padronização do 5G são ITU-R e 3GPP. Enquanto o ITU-R define os requisitos, o 3GPP cuida das propostas tecnológicas para atendê-los. Por exemplo, no documento "IMT-2020", o ITU-R definiu, para vários casos de uso, as capacidades de comunicação do 5G em termos de taxa de pico de dados, taxa sustentável, densidade de conexão, latência, etc. Segundo a Keysight Technologies [89], três casos de uso são definidos: eMBB (*enhanced Mobile BroadBand*), que define, essencialmente, a capacidade da rede 5G NR, baseado nas taxas de pico e média; mMTC (*massive Machine Type Communications*), que define o suporte à conexão de bilhões de dispositivos IoT e sensores; e URLLC (*Ultra-Reliable and Low Latency Communications*), para os casos de uso baseados na comunicação em tempo real, como veículos autônomos. Segundo Singh *et al.* [34] e Zeadally *et al.* [12], espera-se que o 5G suporte taxas de pico de até 20 Gbps, sustentável de 100 Mbps, densidade de conexão de 10^6 dispositivos/km^2 e latência de 1 ms com *jitter* garantido, o que permitirá às aplicações uma tomada de decisão em tempo real. Para efeitos de comparação, o 4G oferece taxas de pico de 1 Gbps, sustentável de 10 Mbps, densidade de conexão de 10^5 dispositivos/km^2 e latência de 10 ms. Conforme Zeadally *et al.*, além de veículos, o 5G permitirá a integração de importantes atores ao ambiente veicular, como pedestres, ciclistas e motociclistas.

Segundo a Keysight Technologies [89], a *Release* 15 – primeiro padrão implementável do 5G desenvolvido pela 3GPP – consiste em atender principalmente aos casos de uso eMBB. Entre outros, taxas mais altas podem ser obtidas em frequências de até 52,6 GHz e canais que, combinados, podem chegar a 800 MHz de largura. Além disso, a taxa também pode ser melhorada via otimização do sinal por meio de técnicas como *massive* MIMO (*Massive Multiple-Input/Multiple-Output*) e *beam-steering*, que consiste em transmissões direcionais. Ainda de acordo com a Keysight, na *Release 15* também é possível obter uma latência mais baixa, atendendo parcialmente aos casos URLLC. Isto é obtido usando *mini-*

slots, que possuem duração menor em termos da quantidade de símbolos OFDM suportados em comparação a um *slot* padrão, como no 4G. Além disso, também é possível minimizar os efeitos da propagação do atraso (*delay spread*) e da ISI (*InterSymbol Interference*) no canal por meio da técnica denominada CP (*Cyclic Prefix*)-OFDM. Como o padrão está em constante evolução pelo 3GPP, visando atender aos requisitos URLLC, como controle de movimento para automação fabril, direção remota e AR (*Augmented Reality*)/VR (*Virtual Reality*), algumas melhorias foram adicionadas na *Release 16*. Por exemplo, em MEC (*Multi-access Edge Computing*), gerenciamento de interferência, MIMO, eficiência energética, entre outros [89]. Segundo Singh *et al.* [34], a *Release* 16 tem como foco atender a todos os casos de uso do IMT-2020, o que deverá possibilitar, entre outros, a direção autônoma completa. Segundo Masini *et al.* [71], a *Release* 16, de 2019, permitirá soluções com requisito de latência $\leq$3 ms, e confiabilidade de até 99,999%.

Conforme a Keysight Technologies [89], o 5G pode operar em dois modos: NSA (*Non-StandAlone*), que faz uso do rádio 4G LTE, da rede EPC (*Evolved Packet Core*) e eNodeB; e SA (*StandAlone*), que usa o 5G NR e conecta diretamente ao 5G NGC (*Next-Generation Core*). No NSA, onde foram concentrados os primeiros esforços de migração do 5G, o objetivo é fornecer uma maior largura de banda e conectividade confiável para eMBB. Já o SA concentra um importante recurso do 5G: o *network slicing*, que divide a rede em redes menores visando atender aos requisitos específicos de latência, confiabilidade, mobilidade e taxa. Segundo Zeadally *et al.* [12], isto é fundamental para comunicações entre veículos, pois cada *slice* da rede é uma rede fim-a-fim independente. Com isso, provedores de serviços poderão customizar cada *slice* como uma rede padronizada para atender aos requisitos específicos de uma dada aplicação. Ainda segundo Zeadally *et al.*, um *slice* poderia ser usado para suportar aplicações de veículos autônomos, cujos requisitos de latência (em torno de 1 ms) e de entrega (próxima de 100%) são estritos. De igual modo, um outro *slice* poderia ser usado por aplicações de multimídia, cujo requisito principal é uma alta vazão, necessária para vídeos de alta resolução. Além disso, o *network slicing* separa logicamente as funções da rede. Com isso, recursos como largura de banda e *buffers* de dispositivos são reservados.

Quanto à frequência de operação, segundo a Keysight Technologies [89], dois intervalos são definidos: FR1 (*Frequency Range* 1), entre 410 MHz a 7,125 GHz; e FR2 (*Frequency Range* 2), entre 24,25 GHz e 52,6 GHz (mmWave). Em termos de componentes de comunicação, a rede 5G NR é formada por UEs (*User Equipments*) – dispositivos móveis como *smartphones* –, e estações base denominadas gNB (*gNodeB*), que podem ser de três tipos: (1) C, com conectores de antena; (2) O, sem conectores de antena; e (3), que usa uma abordagem híbrida. Ainda segundo a Keysight Technologies, outro ponto importante consiste na migração da arquitetura RAN (*Radio Access Networks*) – redes baseadas em *hardware/software* de propósito específico – para O-RAN (*Open* RAN) – baseadas em nuvem e virtualização. Quem lidera esta iniciativa são as operadoras AT&T, China Mobile,

Deutsche Telekom, NTT DOCOMO e Oragne, que juntas formam a O-RAN *Alliance*. Entre os objetivos da O-RAN, estão permitir que novos serviços entrem em produção mais rapidamente via virtualização das funções de rede (limitado na RAN tradicional), bem como oferecer flexibilidade a partir da desagregação da estação base em vários elementos, onde cada um pode vir de um fornecedor diferente graças à maior interoperabilidade entre componentes e à definição clara de protocolos.

2.2 IEEE 802.11p/WAVE

Conforme mencionado na Subseção 2.1.5, visando uma faixa de frequências exclusiva para redes veiculares, em 1999 um espectro de 75 MHz na faixa de 5,9 GHz (5,850,GHz a 5,925 GHz) foi alocado pela FCC, nos Estados Unidos. Como mostra a Figura 2.3, este espectro de 75 MHz é dividido em sete canais de 10 MHz, além de 5 MHz para uso futuro. Dos sete canais disponíveis para uso, apenas o CCH (*Control Channel*), com ID 178, é de uso exclusivo para aplicações de segurança. Dos outros seis SCHs (*Service Channels*), os de ID 172 e ID 184 são reservados para uso especial, como aplicações de emergência para preservação da vida ou segurança pública. Por fim, os demais canais de serviço (IDs 174, 176, 180 e 182) podem ser usados tanto por aplicações de segurança, quanto por aplicações de entretenimento ou conforto [26]. A partir de 2004, o TG p iniciou o desenvolvimento de um padrão de comunicação para utilizar o espectro DSRC e permitir comunicações entre veículos. Isto levou ao desenvolvimento do IEEE 802.11p e da pilha WAVE.

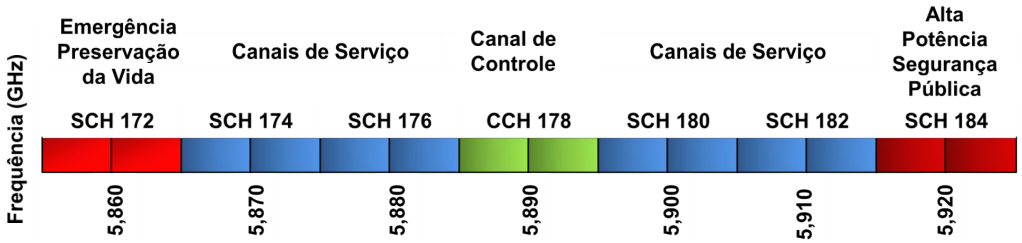

Figura 2.3: Espectro DSRC de 75 MHz para uso de redes veiculares – Baseado em [1].

Segundo Singh *et al.* [34], além do padrão IEEE 802.11p, a pilha WAVE é composta pelos padrões IEEE 1609.2, IEEE 1609.3, IEEE 1609.4, IEEE 1609.11 e IEEE 1609.12. Em resumo, conforme Singh *et al.*, o IEEE 1609.2 é responsável por questões envolvendo segurança, como na transmissão de mensagens de segurança, pelas OBUs, ou de anúncios de serviços disponíveis, pelas RSUs. O IEEE 1609.3 é responsável por serviços na camada de rede e de transporte, como a transmissão de mensagens usando UDP/TCP (*Transmission Control Protocol*) sobre IPv6 (*Internet Protocol version 6*), ou WSMP (WAVE *Short Message Protocol*). Ao contrário do tráfego UDP/TCP sobre IPv6 (restrito aos SCH), a transmissão de WSMs (WAVE *Short Messages*) usando WSMP é indicada para aplicações de segurança e pode ser feita em qualquer canal. Com o WSMP, também é possível definir

o número do canal e a potência usada na transmissão de WSMs. Outra mensagem usada pelo WSMP são as WSAs (WAVE *Service Advertisements*), com as quais RSUs anunciam serviços às OBUs. O IEEE 1609.4 cuida da operação multicanal, possibilitando a troca entre CCH e SCH. O acesso ao canal pode ser contínuo, alternado (requer sincronização) ou imediato (por uma certa duração). Já o IEEE 1609.11 define, entre outros, os requisitos da troca de dados para pagamento eletrônico, como em aplicações do tipo ETC (*Electronic Toll Collection*) usando OBUs e RSUs. Por fim, o IEEE 1609.12 registra os identificadores usados nos padrões IEEE 1609. Por exemplo, ainda segundo Singh *et al.*, o IEEE 1609.12 define três tipos de PSID (*Provider Service Identifier*) para aplicações baseadas em BSMs. Com base no PSID gravado no cabeçalho da WSM (que carrega a BSM no *payload*), o receptor é capaz de distinguir, por exemplo, se as BSMs são derivadas de OBUs embarcadas em veículos rastreáveis, como trens. Singh *et al.* também destacam os serviços de gerenciamento. Tais serviços são responsáveis, por exemplo, pela sincronização de tempo para coordenação de canais, e pela geração e monitoramento de WSAs. Segundo os autores, as duas principais entidades de gerenciamento são o MLME (*Extension of MAC sublayer Management Entity*) e WME (WAVE *Management Entity*). Jafari *et al.* [90] também cita a PLME (*Physical Layer Management Entity*).

Já o padrão IEEE 802.11p é um aperfeiçoamento do IEEE 802.11a para redes veiculares, e é responsável por definir as operações nas camadas PHY e subcamada MAC. Como no IEEE 802.11a, a camada PHY do IEEE 802.11p também é baseada no OFDM (*Orthogonal Frequency Division Multiplexing*). Entretanto, como mencionado na Seção 2.2, são utilizados canais com 10 MHz, e não 20 MHz, como no IEEE 802.11a [26]. De acordo com Li *et al.* [91], esta modificação faz com que a duração do símbolo OFDM no IEEE 802.11p seja o dobro (6.4 μs) em comparação ao IEEE 802.11a (3.2 μs), o que leva a um intervalo de guarda maior (1.6 μs contra 0.8 μs), e fornece desempenho em canais que variam rapidamente [72]. Por exemplo, segundo Li *et al.* [91], isto oferece ao IEEE 802.11p, entre outros, uma maior tolerância ao Doppler *shift* provocado pelas altas velocidades dos veículos. Por sinal, o IEEE 802.11p possui suporte a alta mobilidade, permitindo transmissões a até 200 km/h, e alcance de comunicação de 300 m a 1.000 m [22]. O IEEE 802.11p suporta oito esquemas de modulação: BPSK ½, BPSK ¾, QPSK ½, QPSK ¾, 16QAM ½, 16QAM ¾, 64QAM ⅔ e 64QAM ¾, associados, respectivamente, às taxas de 3 Mbps, 4.5 Mbps, 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps e 27 Mbps [18]. É possível combinar dois SCHs de 10 MHz para formar um canal com 20 MHz de largura de banda, possibilitando alcançar taxas de até 54 Mbps [34].

Um dos principais recursos de comunicação do IEEE 802.11p é a capacidade de trocar dados em modo OCB (*Outside the Context of a* BSS). Segundo Jiang *et al.* [26], em redes Wi-Fi, as estações só são capazes de se comunicarem umas com as outras por intermédio de um ponto de acesso. Para isso, é necessário primeiro fazer parte do BSS (*Basic Service Set*) controlado pelo ponto de acesso, o que só é possível após algumas etapas,

como o sensoreamento de *beacons*, e posterior autenticação e associação com o ponto de acesso. Segundo os autores, mesmo o modo *ad-hoc* do IEEE 802.11, ou IBSS (*Independent* BSS), também executa algumas etapas para estabelecimento da conexão. Entretanto, dadas as altas velocidades relativas do ambiente veicular, o tempo disponível para troca de dados pode ser muito curto. Por exemplo, considerando dois veículos se locomovendo em direções opostas a 80 km/h, e um alcance de comunicação típico de uma rede Wi-Fi de aproximadamente 300 m em área aberta, o tempo de contato entre os dados veículos seria entre 6 s a 7 s. Nos experimentos realizados por Ribeiro Júnior *et al.* [92], o intervalo de tempo entre a detecção do ponto de acesso e a associação do veículo variou entre 6 s e 11 s, em uma via com velocidade máxima de 40 km/h. O modo OCB do IEEE 802.11p permite que os veículos se comuniquem diretamente, sem precisarem antes fazer parte de um BSS. Deste modo, etapas como sensoreamento, autenticação, e associação não são executadas, o que permite a troca de dados imediata, mesmo em condições de alta mobilidade [72].

Na camada MAC, o IEEE 802.11p usa o mecanismo CSMA/CA (*Carrier-Sense Multiple Access with Collision Avoidance*). Segundo Masini *et al.* [71] e Heinovski *et al.* [93], no CSMA/CA, um nó que deseja transmitir dados primeiro deve realizar uma CCA (*Clear Channel Assessment*) antes de acessar o canal, como forma de tentar detectá-lo como livre. Segundo Heinovski *et al.* [93], isto significa tentar detectar uma transmissão em andamento ou uma dada potência mínima no canal. Se for detectado que o meio está livre, o pacote é transmitido após o nó aguardar por um intervalo de tempo AIFS (*Arbitration Inter-Frame Spacing*). Segundo Masini *et al.* [71], isto é necessário para levar em conta potenciais atrasos na propagação de nós distantes. Se for detectado que o canal está ocupado, o nó executa um *backoff* aleatório, que consiste em adiar a tentativa de acesso ao meio por um intervalo de tempo de 0 a CW (*Contention Window*). Ainda segundo Masini *et al.* [71], isto é necessário para reduzir as chances de uma colisão ocorrer, uma vez que permite aos nós iniciarem a próxima etapa de sensoreamento para transmissão de forma aleatória. Segundo Masini *et al.*, mesmo distribuído e não requerendo sincronização para operar, devido ao acesso aleatório do CSMA/CA, em condições de alta densidade de veículos o número de colisões pode ser muito alto já que a quantidade de nós tentando transmitir aumenta. Isto pode levar à escassez dos recursos do canal, devido a problemas como terminal escondido/exposto. Para lidar com isso, mecanismos para adaptação da transmissão também podem ser usados no IEEE 802.11p. Por exemplo, o padrão SAE J2945 define um mecanismo DCC (*Decentralized Congestion Control*) para controle de congestionamento descentralizado no canal [70].

Além da operação multicanal, as operações da extensão da subcamada MAC também permitem tráfego com diferentes níveis de QoS (*Quality of Service*). Isto é baseado no IEEE 802.11e EDCA (*Enhanced Distributed Channel Access*). Segundo Singh *et al.* [34], no EDCA, classes de tráfego distintas possuem prioridades distintas. Isto é feito por meio de quatro categorias de acesso, ou ACs (*Access Categories*): (1) AC3, para tráfego de voz;

(2) AC2, vídeo; (3) AC1, melhor esforço; e (4) AC0, *background*. Cada AC possui uma fila. Dentre as quatro ACs, a AC3 é a que possui a maior prioridade, podendo ser usada para priorizar o tráfego de uma aplicação de segurança na rede veicular. Conforme Grafling *et al.* [94] e Jafari *et al.* [90], todos os canais usados pelo IEEE 802.11p implementam as quatro ACs. Ainda segundo os autores, cada quadro é categorizado em uma AC diferente, dependendo do seu tráfego de origem, e colocado na respectiva fila das AC. Antes do acesso ao meio via CSMA/CA acontecer, dois procedimentos de contenção são realizados: (1) entre ACs, em cada canal; e (2) entre canais (o CCH possui a maior prioridade). Parâmetros de temporização AIFS e CW, usados em cada AC de cada canal, definem a prioridade de acesso ao meio de cada classe de tráfego.

2.3 Wi-Fi Direct

Definido pela Wi-Fi Alliance em 2010 e disponível para Android a partir da versão 4.0 [38], o Wi-Fi Direct, ou Wi-Fi P2P (*Peer-to-Peer*), é uma tecnologia de rádio que visa comunicações do tipo D2D por meio do Wi-Fi. De acordo com Khan *et al.* [77], com taxas de dados de até 250 Mbps e alcance máximo teórico de até 200 m, diversas áreas podem se beneficiar do uso do Wi-Fi Direct, como comunicações de emergência e disseminação de alertas. De acordo com Jeong *et al.* [2], com base nas especificações do padrão SAE J2735, uma aplicação como alerta de mudança de faixa pode ser suportada com base no alcance do Wi-Fi Direct. Como mencionado no Capítulo 1, o Wi-Fi Direct não poderia substituir o IEEE 802.11p. Por exemplo, com uma menor potência de transmissão em comparação ao IEEE 802.11p [39], além das restrições de operação em cenários de alta mobilidade por conta do longo CET, claramente o Wi-Fi Direct não reúne as condições para servir como principal tecnologia de rádio para soluções de ITS. Apesar disso, como observado em [40], ele ainda pode funcionar como um método alternativo de comunicação para cenários contendo algumas condições específicas.

Segundo Camps-Mur *et al.* [3], o Wi-Fi Direct é baseado nas redes Wi-Fi infraestruturadas. Com isso, funções típicas destas redes, como o suporte à QoS, economia de energia e segurança, são herdadas pelo Wi-Fi Direct. A comunicação via Wi-Fi Direct se dá após o estabelecimento de um grupo de comunicação P2P. Este grupo é semelhante ao BSS de uma rede Wi-Fi [77], possuindo inclusive a figura do ponto de acesso. Esse papel é desempenhado pelo dispositivo denominado GO (*Group Owner*), enquanto os clientes do grupo atuam de forma semelhante às estações do BSS. O processo de estabelecimento do grupo P2P se dá após a etapa de descoberta dos dispositivos ser concluída. Após isso, como no Wi-Fi Direct os papéis dos dispositivos não são fixos, a definição sobre quem atuará como GO ou cliente do grupo P2P se dá por meio de negociação. Uma vez que o GO fora definido, e que o grupo P2P já fora estabelecido, outros dispositivos podem se juntar ao grupo em questão, tal qual no BSS das redes Wi-Fi. Segundo Iskounen *et al.* [63], um grupo P2P

pode conter mais de dois dispositivos, porém apenas os dois primeiros podem se descobrir e negociar o papel de GO. Os demais apenas detectam o GO e ingressam no grupo existente. Segundo Camps-Mur *et al.* [3], existem três modos de estabelecer um grupo P2P: (1) *Standard*; (2) *Autonomous*; e (3) *Persistent*. Independente do modo, a primeira etapa a ser executada é o *Scan* da rede, onde os treze canais do Wi-Fi são sensoreados em busca de grupos P2P ou redes Wi-Fi existentes.

Conforme Camps-Mur *et al.* [3], no modo *Standard*, após o *Scan* da rede, os dispositivos iniciam o *Discovery*, visando localizar outros dispositivos Wi-Fi Direct. O *Discovery* é dividido em duas fases: *Listen* e *Search*. No *Listen*, os dispositivos selecionam um dos três canais sociais (1, 6 ou 11) na faixa de 2,4 GHz como canal de escuta, e aguardam por *probe requests* enviados por dispositivos na fase *Search*. Após a recepção de um *probe request*, o dispositivo na fase *Listen* responde com um *probe response*. Já no *Search*, como adiantado, são enviados *probe requests* em cada um dos três canais sociais como forma de realizar um *scan* ativo na rede. A recepção de um *probe request* e o envio subsequente de um *probe response* caracteriza uma descoberta bem sucedida. Os dispositivos alternam entre as fases *Listen* e *Search*, e o tempo de permanência em cada fase varia entre 100 ms e 300 ms. Por seu caráter estocástico, o *Discovery* pode ser uma das principais causas de um longo CET. Após a descoberta, os dispositivos negociam quem assumirá o papel de GO. Esta etapa consiste em um *three-way handshake* (*GO Negotiation Request/Response/Confirmation*), onde um parâmetro numérico denominado GO *Intent Value* é enviado. Variando de 0 a 15, o dispositivo que enviar o *Intent Value* de maior valor será definido como GO. Empates são resolvidos por meio de um bit de desempate, incluído no *GO Negotiation Request*. Nesta etapa também é definido o canal de operação do grupo P2P. Já na próxima etapa, denominada provisionamento WPS (Wi-Fi *Protected Setup*), os dispositivos estabelecem uma conexão segura via WPS, por meio da inserção de um PIN (*Personal Identification Number*) ou do clique de um botão no dispositivo P2P, de forma a aceitar a conexão. Esta etapa é composta de duas fases. Na Fase 1, o GO (definido como *Registrar*) é responsável por gerar e emitir as credenciais da rede para o cliente (definido como *Enrolle*). O WPS é baseado no WPA-2 com criptografia AES de 256 bits [77]. Na Fase 2, o cliente (*Enrolle*) se desassocia e se reconecta usando suas novas credenciais. Por fim, o GO fornece endereços IP aos clientes por meio de um servidor DHCP (*Dynamic Host Configuration Protocol*). A Figura 2.4 exemplifica a operação do modo *Standard*.

Já os modos *Autonomous* e *Persistent* possuem uma operação mais simples. Ainda conforme Camps-Mur *et al.* [3], no modo *Autonomous*, um dispositivo cria um grupo P2P de forma autônoma, assumindo o papel de GO e definindo um canal de operação. Neste modo, assim que o grupo P2P é criado, o GO inicia a transmissão de *beacons* como forma de anunciar sua presença na rede. Em comparação ao modo *Standard*, outros dispositivos podem se juntar ao grupo após um *scan* na rede, migrando diretamente para o provisionamento WPS e configuração IP. Já o modo *Persistent* é caracterizado pela re-instanciação

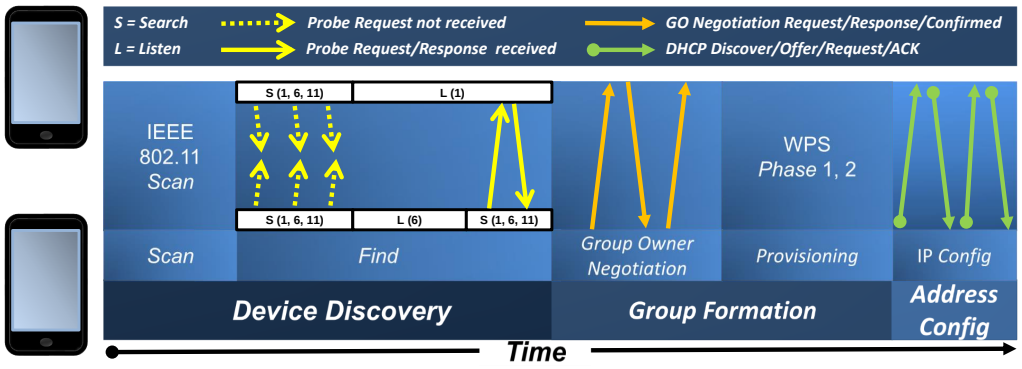

Figura 2.4: Etapas de operação no modo *Standard* – Baseado em [2, 3].

de um grupo P2P que existira anteriormente. Isto se dá através de uma *flag* presente nos *beacons*, *probe responses* e quadros trocados durante a negociação do GO. Por meio desta *flag*, é possível declarar um grupo que está sendo criado como persistente. Com isso, se após a etapa de *Discovery*, um dispositivo reconhece já ter formado um grupo com o dispositivo que fora descoberto, é possível re-instanciar o grupo por meio da troca de quadros de convite (*two-way handshake*). Além das funções exercidas anteriormente, os dispositivos também armazenam as credenciais de rede usadas nas comunicações do grupo P2P, o que permite otimizar futuras re-instanciações. Em comparação ao modo *Standard*, a etapa de negociação do GO no modo *Persistent* é substituída pela troca de quadros de convite, e a duração do provisionamento WPS é reduzida devido ao armazenamento prévio das credenciais. Neste caso, apenas a Fase 2 da etapa de provisionamento WPS é executada.

Ainda segundo Camps-Mur *et al.* [3], entre as etapas de descoberta de dispositivos e a negociação do GO, o Wi-Fi Direct permite a execução de um recurso opcional na camada de enlace denominado *Service Discovery*. No *Service Discovery*, um dispositivo implementando o Wi-Fi Direct pode consultar quais são os serviços suportados pelos outros dispositivos na rede e usar isso como critério para decidir se prossegue ou não com o estabelecimento do grupo. Estas consultas/respostas são geradas por protocolos de camadas superiores, como UPnP ou Bonjour, e são transportados para a camada de enlace usando o protocolo GAS (*Generic Advertisement*), do padrão IEEE 802.11u. Conforme Shahin *et al.* [95], antes de estabelecer um grupo P2P, um dado dispositivo pode enviar um quadro de consulta/requisição para descobrir os serviços suportados por um outro dispositivo. Após a recepção deste quadro, o outro dispositivo responde/anuncia seus serviços por meio da transmissão de um quadro contendo um registro de seus serviços armazenados.

Por fim, segundo Camps-Mur *et al.* [3], o Wi-Fi Direct define dois modos de economia de energia do GO: (1) OppPS (*Opportunistic Power Save*); e (2) NoA (*Notice of Absence*). No OppPS, o GO anuncia uma janela de tempo (*CTWindow*) dentro de cada *beacon* ou *probe response*. Esta janela define o período, após a recepção do *beacon*, que o GO permanecerá ativo. Se após este período o GO determinar que os clientes estão em modo de economia de energia, o GO migra para este estado até o próximo *beacon*. Por outro

lado, o GO permanece ativo enquanto houver um cliente ativo. Já no NoA, o GO anuncia períodos de ausência nos quais os clientes não podem transmitir. Como no OppPS, estes períodos são definidos nos *beacons* ou *probe responses*. Quatro parâmetros são considerados para definir os períodos de ausência: (1) duração do período; (2) intervalo de tempo entre períodos consecutivos; (3) tempo de início do período após recepção do *beacon*; e (4) total de períodos programados.

2.4 Simulações de Redes Veiculares

Como mencionado na Seção 1.3, dados o custo e recursos requeridos por testes práticos realísticos em redes veiculares, a maior parte dos trabalhos envolvendo a comunicação entre veículos em larga-escala é feita via simulações. Além de serem uma importante ferramenta de cunho educacional [96], simuladores são úteis para modelar e analisar protótipos do mundo real sob diferentes condições e parâmetros, de uma forma simples, rápida, escalável e econômica [97], especialmente quando comparado com implementações de redes reais compostas por múltiplos computadores, roteadores e enlaces [98]. Via simulações, é possível estudar, por exemplo, o comportamento de novos protocolos de roteamento, bem como aplicações voltadas para a disseminação de mensagens de emergência, antes de sua implementação real [98]. Por exemplo, é possível avaliar a eficiência de um novo protocolo de roteamento com base na proporção de mensagens entregues com sucesso, em diferentes cenários (urbanos e rurais), sem limitação de tempo, e repetindo os experimentos sempre que for necessário [99], algo que seria difícil por experimentação prática. No contexto das redes veiculares, simuladores podem ser divididos entre: (1) simuladores geradores de mobilidade para veículos; (2) simuladores de rede de propósito geral; e (3) simuladores específicos para redes veiculares.

Geradores de mobilidade geram *traces* de mobilidade realística de veículos. De acordo com Martinez *et al.* [98], modelos de tráfego podem ser classificados como macroscópicos, microscópicos e mesoscópicos. Modelos macroscópicos modelam o tráfego em larga escala, permitindo saber, por exemplo, o número de veículos por hora passando por uma dada posição da via [19]. Ainda segundo Martinez *et al.* [98], modelos microscópicos modelam as características individuais de veículos e motoristas, como o critério de um motorista ao fazer uma ultrapassagem. Já modelos mesoscópicos combinam parte das características dos modelos macroscópicos e microscópicos. Por seu nível de detalhe, modelos microscópicos são mais apropriados para redes veiculares. Já os simuladores de rede modelam o comportamento da rede de comunicação. No contexto das redes veiculares, simuladores de rede podem ser usados para avaliar a comunicação entre veículos, usando por exemplo o IEEE 802.11p. Segundo Grzybek *et al.* [99], também é importante considerar as características da propagação do sinal de rádio, que pode ser impactada pela dinamicidade do ambiente veicular. Por fim, simuladores específicos para redes veiculares permitem simu-

lar tanto o tráfego quanto a rede [98], onde a posição do veículo gerada pelo simulador de tráfego é refletida na posição do nó no simulador de rede [99]. Neste sentido, é importante que tais simuladores permitam que veículos/motoristas respondam às mensagens trocadas na rede, como um alerta de colisão [98]. Segundo Ahmed *et al.* [97], uma desvantagem dos *traces* é que eles só permitem analisar o efeito da mobilidade na rede, mas não o contrário. Pode-se citar como exemplos de geradores de mobilidade: SUMO (*Simulation of Urban Mobility*) [100], SMARTS (*Scalable Microscopic Adaptive Road Traffic Simulator*) [101] e MovSim (*Multi-model open-source vehicular-traffic Simulator*) [102]. Como simuladores de rede: NS-3, OMNeT++ (*Objective Modular Network Tested in C++*) [103] e Mininet [104]. Por fim, são exemplos de simuladores de redes veiculares: Veins e VENTOS (*VEhicular NeTwork Open Simulator*) [105]. Todos os simuladores citados são de uso gratuito e código-fonte aberto.

Nesta tese, a escolha do NS-3/PhySim para avaliação do IEEE 802.11p se deu pela sua popularidade na academia. Quanto ao Veins/MiXiM, a escolha se deu por este ser um simulador específico para redes veiculares. Já a escolha do INET para avaliação do Wi-Fi Direct se deu pelo módulo do Wi-Fi Direct neste simulador considerar todas as etapas do protocolo até a formação do grupo P2P. Quanto ao NS-3, apesar de seu propósito geral, o mesmo possui um módulo compatível com o IEEE 802.11p, além de modelos de propagação adequados para redes veiculares. Apesar do uso nesta tese do PhySim na camada PHY, o NS-3 por si só é usado em diversos trabalhos no contexto veicular, como o projeto iTetris [99]. Como gerador de mobilidade dos veículos no NS-3/PhySim, foi utilizada a implementação dos modelos microscópicos propostos por Treiber *et al.*, IDM (*Intelligent Driver Model*) [106] e MOBIL (*Minimizing Overall Braking Induced by Lane change*) [107], feita por Arbabi *et al.* [108] para o NS-3. O IDM e MOBIL definem, respectivamente, a velocidade de um veículo com base no veículo da frente (*car-following*) [99], e os critérios de incentivo/segurança para mudanças de faixa [109]. Já no Veins/MiXiM e INET, a mobilidade foi gerada pelo SUMO, que modela, entre outros, ultrapassagens e mudanças de faixa por meio do modelo *car-following* de Krauß [99, 109]. A geração de mobilidade consistiu, basicamente, de movimentar o veículo em linha reta a uma dada velocidade, o que pode levar a resultados otimistas na avaliação [99]. Dado que um dos focos desta tese é analisar a capacidade de mimetização dos simuladores, a já mencionada complexidade de realização de testes práticos leva à configuração de cenários de pequena-escala, que no caso desta tese, são refletidos nas simulações para efeitos de comparação. É importante ressaltar que, dada a simplicidade dos cenários reais desta tese, compostos por apenas um veículo que se locomove em direção a um(a) RSU/veículo/pedestre, os recursos de mobilidade oferecidos pelo IDM/MOBIL e SUMO não foram explorados.

2.4.1 NS-3/PhySim

O NS-3 é um simulador de redes baseado em eventos discretos cujo foco é a operação das camadas 2, 3 e 4 do modelo OSI [96]. Uma evolução do NS-2 (*Network Simulator 2*), o NS-3 difere de seu predecessor em vários quesitos. Segundo Henderson *et al.* [57], apesar de serem escritos em C++, o NS-3 não utiliza *scripts* OTcl (*Object-Oriented Tool Command Language*) para descrever simulações, e sim *Python*. O NS-3 também é considerado mais escalável e modular. Além disso, suporta a integração com *testbeds*, além de permitir o rastreamento e coleta de dados estatísticos por meio de *callbacks*, sem precisar reconstruir o núcleo da simulação. Segundo Grzybek *et al.* [99], comparado ao NS-2, o NS-3 é mais fácil de usar, e possui uma vasta documentação e uma ampla comunidade de usuários/desenvolvedores que garante sua continuidade – a cada três meses uma nova versão é lançada. Como mencionado na Seção 2.4, a escolha pelo NS-3 se deu por sua popularidade. Para exemplificar, uma busca feita em 02/2021 no Google Scholar[1] pelo termo "*ns-3 simulator*" retornou mais de 29 mil resultados (contando falsos positivos) [110]. O NS-3 pemite simulações de redes IP e não-IP, suportando, entre outros, modelos como Wi-Fi, WiMAX, LTE, e protocolos como OLSR (*Optimized Link State Routing*) e AODV (*Ad-hoc On Demand Distance Vector*). Além disso, desde a versão 3.19 (3.33 é a atual) o NS-3 passou a integrar módulos do IEEE 802.11p. Entretanto, de acordo com o nosso conhecimento, ao menos no período de execução das simulações, o NS-3 não possuía um modelo que considerasse o efeito que a mobilidade dos veículos poderia gerar na comunicação de uma rede veicular, devido, por exemplo, ao Doppler *shift*. Desta forma, como forma de considerar este efeito nas simulações, decidiu-se por utilizar nesta tese um módulo de camada PHY desenvolvido para o NS-3, denominado PhySim [58, 59].

Segundo Papanastasiou *et al.* [58] e Mittag *et al.* [59], autores do PhySim, na camada PHY padrão do NS-3, o pacote é tratado como uma unidade indivisível, que deve ser recebido ou não em sua totalidade, decisão esta que é baseada em modelos analíticos da SINR (*Signal-to-Interference-plus-Noise Ratio*) e BER (*Bit-Error Rate*). Etapas como a codificação e processamento do sinal, bem como os efeitos do canal nos bits individuais não são considerados. Com isso, não é possível determinar erros individuais em bits. Já no PhySim, o pacote é transformado em bits e, depois, em um sinal composto por amostras de tempo complexas. Isto é feito atuando como um emissor/receptor real durante a codificação/decodificação do sinal. Desta forma, efeitos das camadas inferiores, como os provocados pela velocidade dos nós, são capazes de impactar o quadro. No PhySim, o processo de transformação do pacote em bits, e depois, em amostras de tempo complexas, começa assim que o método *SendPacket()* é chamado pela camada MAC, e consiste na aplicação, entre outros, de *interleaving*, FEC (*Forward Error Correction*) e modulação OFDM, que resultarão nos símbolos OFDM – compostos de preâmbulo, cabeçalho do si-

[1] https://scholar.google.com/

nal e *payload* – a serem transmitidos no canal. No módulo que simula o canal sem-fio, os modelos de propagação, como desvanecimento de pequena-escala (*small-scale fading*) e perda de percurso (*path-loss*), são aplicados na sequência de amostras de tempo complexas, e o atraso de propagação é aplicado. Após isso, a sequência de amostras é passada para a camada PHY do receptor via método *StartReceive()*, onde se inicia o processo de decodificação (transformação em bits). Nesta etapa, a sequência de amostras é adicionada a um módulo responsável por controlar todos os quadros (possíveis interferências) sendo recebidos no momento. Após o término, entre outros, do preâmbulo, da detecção/sincronização do sinal, da decodificação do cabeçalho do sinal, e da demodulação OFDM, a decisão sobre a recepção do pacote é feita comparando os bits transmitidos com aqueles que foram recebidos.

Em [58, 59], a camada PHY do PhySim foi validada por meio da comparação dos resultados de simulações com os obtidos por uma interface OFDM IEEE 802.11 comercial, baseada no *chipset* Atheros AR5112, no emulador de rede CMU (*Carnegie Mellon University*). Compatível com o IEEE 802.11g, o dispositivo opera na frequência de 2,4 GHz, com canais de 20 MHz. Como métrica de desempenho, os autores consideraram a taxa de recepção de quadros. Na validação, são usados modelos de propagação de perda de percurso e desvanecimento de pequena-escala. Além disso, as transmissões são feitas usando pacotes de 500 bytes, em um ambiente sem interferência, em diferentes velocidades relativas, taxas de dados, entre outros. Os resultados indicaram que as curvas obtidas pelo PhySim foram similares àquelas obtidas no emulador de rede CMU. Além disso, os resultados também indicaram uma redução da taxa de recepção de quadros conforme a velocidade relativa dos nós aumentou. Tal comportamento não foi obtido pelo NS-3 padrão. Além disso, no NS-3 padrão, resultados mais otimistas no cenário que aplica a perda de percurso foram obtidos. É importante destacar, por outro lado, que o modelo da camada PHY no PhySim exige um maior esforço computacional. Segundo o manual do PhySim [111], apesar de incorporar modelos de canais sofisticados, considerar os efeitos de múltiplos caminhos de forma mais precisa, além do Doppler *shift*, dependendo dos parâmetros usados, as simulações no PhySim podem ser até 10 mil vezes mais lentas que as simulações usando a camada PHY padrão do NS-3. Além disso, no PhySim, operações multi-canal não são suportadas.

2.4.2 Veins/MiXiM

O Veins é um *framework* para simulação de redes veiculares, que resolve o problema de uso de *traces* de mobilidade apontado por Ahmed *et al.* [97]. Neste simulador, não só a influência da mobilidade na rede pode ser modelada, mas também o inverso. Por exemplo, é possível modelar que um motorista mude a rota do veículo após a recepção de um alerta de colisão. Segundo Sommer *et al.* [60], isto é devido ao acoplamento bidirecional entre

os tráfegos de rede e viário, usando os simuladores OMNeT++ e SUMO. O OMNeT++, simulador de rede baseado em eventos discretos e no uso de componentes, é responsável pela comunicação entre os nós da rede veicular. No OMNeT++, os cenários da rede são representados por módulos escritos em C++, cujo relacionamento e comunicação são armazenados como arquivos NED (*Network Description*). Por meio do *framework* INET, módulos OMNeT++ que representam protocolos como TCP, UDP, IPv4, entre outros, podem ser usados. Já o SUMO simula o tráfego viário em nível microscópico, usando o modelo de mobilidade *car-following* de Stefan Krauß. O Veins age como um *gateway* entre o OMNeT++ e o SUMO [112]. Por meio de conexões TCP, para cada veículo criado no SUMO, o Veins instancia um nó de rede na simulação do OMNet++. Isto é possível usando o protocolo TraCI (*Traffic Control Interface*), que permite modificar a posição, velocidade e direção do nó de rede com base nos dados recuperados no SUMO. Entre os recursos incluídos no Veins para comunicação entre veículos – como ETSI ITS-G5, e redes 4G e 5G via *framework* INET, e VLC via MATLAB/SIMULINK –, modelos compatíveis com o IEEE 802.11p, IEEE 1609.4 (operação multi-canais), acesso ao canal com QoS via EDCA, entre outros também estão disponíveis. O Veins também conta com modelos de propagação e de ganhos de antena, como uma versão mais realística do modelo *Two-Ray Ground Model*, denominado *Two-Ray Interference Model*.

A camada PHY no Veins é modelada pelo MiXiM [61, 62], que permite modelar sinais complexos, nas dimensões de tempo, espaço e frequência, e também suporta modelos de propagação de perda de percurso e desvanecimento de pequena-escala. Segundo Köpke *et al.* [62] e Wessel *et al.* [61], a camada PHY do MiXiM é composta de cinco partes: (1) *AnalogueModels*, que simulam a atenuação (*shadowing*, *fading* e *path loss*) de um sinal; (2) *Radio*, que simula os estados de um rádio físico, como o tempo que ele leva pra mudar de modo Tx para Rx, bem como os efeitos do estado na recepção do sinal, como a falha de recepção se o rádio estiver em modo Tx; (3) *ChannelInfo*, que mantém um controle das mensagens (*AirFrames*) atualmente no canal; (4) *Decider*, que classifica (como ruído ou interferência) e demodula (calcula os erros de bits) um *AirFrame* recebido, e informa o estado do canal para a camada MAC; e (5) *BasePhyLayer*, que integra todos os componentes citados. Em resumo, a transmissão de *Airframes* requer apenas a definição de parâmetros e cálculo do atraso de propagação. Já a recepção é um pouco mais complexa. Assim que os primeiros bits do *AirFrame* são recebidos, ele é adicionado no módulo *ChannelInfo*. O objetivo é rastrear interferências entre *AirFrames* que ocupam o canal em um mesmo intervalo de tempo, de forma a permitir o cálculo do SINR pelo *Decider*. Ainda na camada PHY do receptor, os *AnalogueModels* aplicam modelos de perda de propagação ao módulo *Signal* contido no *AirFrame* de forma a gerar a atenuação do sinal. O *AirFrame* é então repassado ao *Decider*, que define quando tomará a decisão sobre recebê-lo/processá-lo, ou tratá-lo como ruído. No *AirFrame*, o módulo *Signal* é composto por módulos *Mapping* que descrevem as propriedades físicas do sinal, como

potência de transmissão e taxa de bits (adicionados na camada MAC do transmissor), atenuações (*AnalogueModels*) e potência de recepção (produto das atenuações e potência de transmissão), usada pelo *Decider* para cálculo da SINR e análise dos erros de bits. Tais propriedades físicas definem o sinal variando no tempo e, opcionalmente, no espaço e na frequência.

2.4.3 INET

Em [63], Iskounen *et al.* implementaram um módulo de simulação para Wi-Fi Direct no *framework* INET. Baseado no OMNeT++, o INET permite que protocolos, agentes e modelos de aplicações sejam usados nas simulações. No INET, protocolos como UDP (transporte), IPv4 (rede), 802.11 (enlace), bem como modelos de aplicação para geração de tráfego, como UDP, podem ser definidos. O INET também permite modelar fenômenos da camada física, como interferência e ruído, zonas de sombra causadas por obstáculos, e a atenuação do sinal com base em um modelo de propagação [113]. Na implementação de Iskounen *et al.*, as principais etapas executadas pelo protocolo foram consideradas, como a descoberta de dispositivos, a negociação para definição do GO e a formação do grupo P2P, contemplando inclusive o provisionamento WPS. A implementação foi baseada nos modelos *ad-hoc* e infraestruturado do IEEE 802.11, disponíveis no INET. Segundo os autores, no INET, um módulo que simula uma interface de rede IEEE 802.11 possui quatro camadas: (1) *agent*; (2) *management*; (3) MAC; e (4) PHY, responsáveis, respectivamente, por (1) controlar, por meio do módulo `Ieee80211AgentSTA`, o comportamento da estação IEEE 802.11 na rede; (2) implementar funções e gerar quadros de gerenciamento, como *beacons* e *probe requests*, além de manter módulos de acordo com o papel desempenhado pelo nó na rede (`Ieee80211MgmtSTA`, `Ieee80211MgmtAP`, `Ieee80211MgmtAdhoc`); (3) implementar, por meio do módulo `Ieee80211Mac`, o protocolo CSMA/CA; e (4) modelar, por meio do módulo `Ieee80211Radio`, a propagação do sinal no meio sem-fio. Com base nos módulos disponíveis na camada (2) no INET, os autores implementaram um novo módulo denominado `Ieee80211MgmtSTAWifiDirect`, responsável pelo encapsulamento e desencapsulamento, e pela troca de quadros visando, por exemplo, o estabelecimento do grupo P2P. Apesar de abstrações, a etapa de provisionamento WPS (fases 1 e 2) também foi implementada, consistindo na troca de N quadros de autenticação, onde N é um valor definido nas simulações. A entrada de um dispositivo Wi-Fi Direct em um grupo P2P existente também foi considerada, tendo como base o envio, ao GO do grupo P2P, de um *Provision Discovery Request*. Após a recepção de um *Provision Discovery Response*, o dispositivo migra para a etapa de provisionamento WPS.

Como mencionado na Subseção 2.4.1, para simulações de redes veiculares, além de levar em conta a redução da potência do sinal devido ao aumento da distância entre os nós, um importante fator a ser considerado é o efeito da velocidade do veículo na re-

cepção dos quadros. Apesar de aceito na literatura que o IEEE 802.11p é robusto ao Doppler *shift*, entende-se que é importante considerar o efeito da mobilidade nas simulações. Na camada PHY do PhySim, compatível com o IEEE 802.11p, além da perda de percurso gerada pelo aumento da distância entre os nós, o efeito do desvanecimento de pequena-escala no sinal devido à mobilidade do veículo também pode ser considerado. Diferentes intensidades de desvanecimento podem ser geradas a partir das diferentes velocidades dos veículos [58]. Nesta tese, para cálculo da perda de percurso e do desvanecimento de pequena-escala no PhySim, foram utilizados os modelos de propagação `PhySimLogDistancePropagationLoss` e `PhySimRicianPropagationLoss`, respectivamente. Mesmo não sendo usado nesta tese, cabe ressaltar que o PhySim também dispõe de um robusto modelo de propagação específico para diversos cenários (desfiladeiros urbanos, ruas suburbanas e vias expressas) e configurações (cruzamento e mesma direção) do contexto veicular, denominado `PhySimVehicularChannelPropagationLoss`. Este modelo foi baseado em experimentos reais, feitos com base em comunicações V2V e R2V (*Roadside-to-Vehicle*). Do mesmo modo, como mencionado na Subseção 2.4.2, a camada PHY do MiXiM também oferece suporte a modelos de propagação de perda de percurso e desvanecimento de pequena-escala. Nesta tese, para isso foram usados os modelos `SimplePathLossModel` e `JakesFading`, respectivamente. Cabe ressaltar que, nas simulações do INET, apenas o modelo `LogNormalShadowing` foi considerado.

Este capítulo apresentou, entre outros, os principais conceitos por trás das redes veiculares, os detalhes técnicos do IEEE 802.11p e Wi-Fi Direct, bem como algumas características dos simuladores NS-3/PhySim, Veins/MiXiM e INET. No capítulo seguinte, serão mostrados os trabalhos da literatura que inspiraram o desenvolvimento desta tese.

Capítulo 3

Trabalhos Relacionados

Este capítulo apresenta os trabalhos que serviram de inspiração para o desenvolvimento desta tese. Primeiro, são apresentados os trabalhos relacionados à avaliação do desempenho do IEEE 802.11p. Em seguida, são mostrados aqueles que têm como objetivo analisar a viabilidade do Wi-Fi Direct no ambiente veicular. Em todos os casos, são considerados trabalhos que cuja análise é feita por meio de simulações e/ou experimentos reais.

3.1 Avaliação do Desempenho do IEEE 802.11p

Dadas as muitas facilidades que decorrem do uso de ambientes sintéticos, como redução de custos, repetibilidade e reprodutibilidade dos experimentos, não há dúvidas de que a avaliação por simulações ainda é o método mais atraente, no qual são baseadas a maioria das avaliações. Assim, os resumos de alguns trabalhos que avaliam o IEEE 802.11p sob algum aspecto via simulações são apresentados. Estas discorrem sobre diversas plataformas, como NS-2, NS-3, Veins, MATLAB, e QualNet. Também são feitas breves descrições de alguns trabalhos que fazem uso de experimentação prática. São descritos trabalhos práticos que utilizam dispositivos de comunicação comerciais com *hardware* IEEE 802.11p dedicados, baseados em interfaces WLAN (*Wireless* LAN) modificadas para operar no modo IEEE 802.11p, e transceptores SDR (*Software-Defined Radio*).

Em [64], ElBatt *et al.* avaliam uma aplicação de segurança FCW (*Forward Collision Warning*) em simulações no QualNet, onde modelos IEEE 802.11a foram adaptados para refletir o DSRC. O cenário consiste de uma via bidirecional com 1.920 veículos. Em uma direção, os veículos se locomovem entre 33 km/h e 49 km/h. Na outra, se encontram parados devido a um incidente. Todos os veículos possuem rádio DSRC, antenas omnidirecionais, e atuam como transceptores. Cada veículo transmite 290 pacotes UDP de 100 bytes no CCH, à 6 Mbps, e com taxa de 10 Hz. Dada a natureza de aplicações FCW, só são considerados veículos posicionados à frente do receptor. Além disso, para evitar o efeito de borda, a recepção não considera veículos nos últimos 150 m de cada extremidade da

via. Usando protótipos reais de rádio DSRC, os autores também derivaram uma estimativa da curva BER com base na SNR (*Signal-to-Noise Ratio*), ruído dos rádios, e expoente de perda de percurso do canal. Um modelo de canal que leva em conta tais estimativas foi adotado nas simulações. A avaliação consistiu, para os eventos de transmissão/recepção de um dado par de veículos, da análise do IRT (*Inter-Reception Time*), que é similar ao PIR, número cumulativo de recepções, PSP (*Packet Success Probability*), que é similar à PDR, e da latência por pacote, em cenários com baixa e alta densidade de veículos. Segundo a análise dos resultados feita pelos autores, devido à menor interferência, o desempenho da PSP e do IRT foram superiores em baixa densidade. Neste cenário, o IRT máximo foi, em média, 238 ms, enquanto a PSP foi de 98,6%. Isto indica um IRT 56% inferior e uma PSP 12% superior em comparação ao cenário com alta densidade. Além disso, com menos veículos disputando o canal, a latência ficou restrita majoritariamente ao atraso de transmissão (pouca probabilidade de *backoff* na camada MAC). Os autores também avaliaram a PSP com relação à distância. Neste caso, para um dado veículo, foram considerados os pacotes transmitidos por veículos em um raio de até 150 m. Novamente, enquanto que em alta densidade a PSP variou de 93% para 38% entre 0 m e 150 m, em baixa densidade ela sempre se manteve próxima de 100%. Por fim, para melhorar o desempenho do *broadcast* em cenários de alta densidade, foi avaliada a adaptação (1) da taxa de pacotes e (2) do alcance da transmissão. Com base na PSP e no IRT, os resultados de (1) sugeriram um intervalo de transmissão ideal em torno de 100 ms. Já para (2), foi sugerido o uso de uma potência de transmissão mínima para alcançar o veículo de interesse em cenários de alta densidade de veículos.

Em [90], Jafari *et al.* avaliam o desempenho do padrão IEEE 802.11p e da pilha WAVE com base na implementação dos parâmetros fundamentais de tais modelos no NS-2. O cenário de avaliação consistiu de uma via unidirecional contendo nove veículos dispostos em três faixas, cujas velocidades máximas eram 80 km/h, 100 km/h e 130 km/h. Uma ambulância, posicionada 100 m atrás dos últimos veículos da via, se locomovia a 150 km/h, transmitindo pacotes à taxa de 5 Hz. A mobilidade dos veículos foi gerada pelo simulador de tráfego VanetMobiSim. A avaliação consistiu na análise da vazão, latência fim-a-fim, e perda de pacotes. Também foram avaliados o impacto da variação da velocidade e do tamanho dos pacotes (250, 500 e 1000 bytes). Segundo a análise dos resultados feita pelos autores, a recepção foi bem-sucedida para todos os veículos cuja distância para a ambulância era inferior a 138 m. Em tais distâncias, não houve perda de pacotes, nem diferenças significativas na vazão obtida com pacotes de 250 bytes (entre 1,8 kbps e 2,2 kbps). A análise também indica que a vazão e a perda de pacotes não são impactadas pela variação da velocidade. Ainda para pacotes de 250 bytes, um compromisso entre o aumento da distância e o aumento da latência fim-a-fim foi identificado. Por outro lado, assim como ocorreu para a vazão e a perda de pacotes, a variação da velocidade não impactou a latência. Um compromisso entre o aumento do pacote e o aumento da vazão média e da latência fim-

a-fim também foi identificado, apesar do aumento da vazão ter ocorrido em menor grau para os veículos mais distantes da ambulância.

Em [114], Rashdan *et al.* analisam o desempenho do IEEE 802.11p, em aplicações de prevenção de colisão em interseções, por meio de simulações no Veins. O objetivo principal é analisar o efeito de condições NLoS (geradas por prédios) e interferência nas comunicações V2V feitas em interseções. A avaliação consistiu de dois tipos de cenários, baseados em uma interseção (1) aberta, sem prédios nas quatro esquinas, e (2) fechada, com prédios em todas as esquinas. Para ambos os cenários, avaliou-se o impacto da densidade de tráfego (baixa, com 15 veículos/km/faixa, e alta, com 110 veículos/km/faixa), potência de transmissão (13 dBm e 23 dBm), e taxa de dados (3 Mbps, 6 Mbps, e 18 Mbps). Nas simulações, veículos se locomovem em direção às interseções com velocidade máxima de 60 km/h, por todas as quatro vias de 1 km e 6 faixas, e em todas as direções. Todos os veículos transmitem CAMs de 338 bytes à 10 Hz. A avaliação se deu com base na análise do UD (*Update Delay*), que é similar ao PIR. De forma a evitar o efeito de borda, são consideradas apenas as recepções ocorridas quando transmissor e receptor estavam a 200 m do centro da interseção. Segundo a análise dos resultados feita pelos autores, em interseções abertas e para transmissões feitas à 6 Mbps, o aumento da densidade de tráfego degrada a comunicação V2V. A probabilidade de perder 10 CAMs consecutivas aumenta por um fator de 117, ao usar uma potência de transmissão de 23 dBm, e por um fator de 38, ao usar 13 dBm. Enquanto isso, a densidade do tráfego aumenta por um fator de 8. Tais resultados podem ser atribuídos à interferência. Em interseções fechadas e para transmissões feitas à 6 Mbps, as condições NLoS geradas pelas obstruções de prédios leva à uma redução do alcance. Ao mesmo tempo, tais obstruções diminuem a interferência no canal e melhoram o desempenho do UD, especialmente em condições de alta densidade de veículos. Além disso, uma melhora no desempenho do UD também foi observada ao usar taxas de dados mais altas. De acordo com os autores, o uso de modulações mais altas diminuem o tempo de transmissão do pacote devido à maior eficiência espectral. Consequentemente, isto reduz a interferência e leva a um menor número de colisões, o que por sua vez reduz o UD. A interferência foi apontada pelos autores como a principal causa da perda de pacotes.

Em [115], Shagdar *et al.* avaliam o desempenho baseado na transmissão de CAMs sobre IEEE 802.11p em aplicações C-ACC por meio de um modelo teórico e simulações. O modelo teórico proposto, uma cadeia de Markov, é baseado no EDCA do IEEE 802.11p, e considera as probabilidades de obter acesso ao canal, de ter um pacote para transmitir, do canal estar ocioso, da transmissão ser bem-sucedida entre membros do *platoon*, bem como o tempo médio de serviço do canal. Já o modelo no NS-3 modela um *platoon* de cinco veículos que se locomovem em um trecho de via de 1000 m. O objetivo é avaliar a probabilidade de transmissão de CAMs entre membros do *platoon*, considerando que o canal também é compartilhado por veículos comuns. Cada veículo envia CAMs de 400 bytes, com potência de 23 dBm, à taxa de 10 Hz. Segundo a análise dos resultados feita pelos

autores, com base nos resultados do modelo e das simulações, é possível observar o impacto da alta densidade de veículos em aplicações de conscientização cooperativa. Em tais condições, um veículo 500 m distante do transmissor obteve uma PDR em torno de 20%. Por outro lado, devido ao efeito de captura – a capacidade de decodificar o pacote frente a interferências –, as comunicações entre membros do *platoon* permitem uma PDR em torno de 65% nas mesmas condições. O modelo também foi integrado ao SIMULINK para avaliar o impacto das transmissões de CAMs na estabilidade do encadeamento de veículos em um *platoon*, em um cenário com mais de 300 veículos comuns no trecho de 1000 m, onde todos transmitiam CAMs à 10 Hz. A análise dos autores indica o benefício de aplicações C-ACC, baseadas na transmissão de CAMs sobre IEEE 802.11p, na estabilidade do *platoon*, especialmente se comparado à abordagem baseada apenas em ACC. Por exemplo, ao contrário do que ocorre com C-ACC, com ACC cada veículo leva alguns segundos para ajustar sua velocidade de acordo com a velocidade do veículo à frente. Os autores ponderam, porém, que apesar da melhora devido ao uso do IEEE 802.11p, o *platoon* não é totalmente estável.

Em [116], Noor-A-Rahim *et al.* avaliam o desempenho do *broadcast*, em interseções, de mensagens de segurança baseadas no IEEE 802.11p por meio de um estudo analítico e simulações no NS-3. Usando um modelo de perda de percurso e desvanecimento prático para cenários com condições de LoS e NLoS, a interseção foi dividida em sete áreas diferentes, considerando os alcances de comunicação e detecção da portadora, que variam de acordo com a posição do transmissor. O cenário de avaliação consiste em uma área de 300 m x 300 m, com a interseção definida no centro da mesma. A posição dos transceptores varia de 1 m a 150 m, a partir do centro da interseção. Pelo estudo analítico, foram analisadas a PRR (*Packet Reception Ratio*) e a latência de acesso ao canal, com base nas posições dos transceptores. Nas simulações, a densidade de veículos foi variada, e apenas os resultados da recepção de pacotes da fila AC0 do EDCA foram considerados. No geral, a análise dos resultados feita pelos autores indica que, devido à limitação do alcance e às colisões provocadas por terminais ocultos, a PRR no centro da interseção é baixa quando o transmissor se encontra distante do centro da interseção. Por outro lado, quando o transmissor se encontra no centro da interseção, a PRR nas demais áreas tende a ser maior já que a transmissão é detectada por todos os veículos. Com relação à latência média de acesso ao canal, esta variou de acordo com o AC do EDCA usado, bem como com a posição do transmissor. Por exemplo, áreas mais distantes possuem latência mais baixa devido à menor região de detecção da portadora. Para melhorar o desempenho em áreas distantes, os autores propõem o uso de RSUs como retransmissores. Segundo os autores, o desempenho melhorou de forma moderada ao inserir uma RSU, equipada com uma antena omnidirecional, no centro da interseção para retransmissão das mensagens de segurança. Já ao usar antenas bidirecionais na RSU, o desempenho melhorou de forma significativa. Por exemplo, usando antenas omnidirecionais, a PRR é muito baixa quando

o transmissor se encontra distante do centro da interseção. Com antenas bidirecionais, a PRP é $> 0{,}9$ independente da posição do transmissor. A análise também indica que o estudo analítico demonstrou uma grande concordância (95%) com as simulações.

Em [117], Cao *et al.* propõem um modelo analítico para o EDCA do IEEE 802.11p, validado no NS-2. O modelo é baseado nos modelos de cadeias de Markov 2-D, responsável por modelar o *backoff* de cada AC, e 1-D, que modela o período de contenção com base nos valores de AIFS e CW. Em ambos os casos, as probabilidades de transmissão e colisão são derivadas para cada AC. Baseado nestas possibilidades, modelos de desempenho também são derivados visando analisar a vazão normalizada, latência de acesso ao canal e latência de enfileiramento. O cenário de avaliação consistiu em um trecho de 1000 m de uma via unidirecional, com uma RSU na posição central do trecho, e veículos se locomovendo com média de 112,6 km/h. O modelo proposto foi comparado com um modelo do estado da arte [118], que analisa o desempenho do EDCA do IEEE 802.11p e, segundo os autores, é adequado para condições saturadas e não saturadas, porém não faz o procedimento de detecção de portadora inicial. Com relação à avaliação em função do número de veículos, taxa de chegada de pacotes de 0,45 Mbps, e pacotes de 512 bytes, a análise dos resultados feita pelos autores indica que a maior vazão foi obtida na AC0, e que a vazão de cada AC cresce até um dado ponto, após o qual começa a diminuir devido ao aumento das colisões pelo aumento do número de veículos. Quanto à latência de acesso ao canal, esta permaneceu baixa para as duas ACs de maior prioridade, enquanto aumentou de forma rápida para as ACs de menor prioridade. Em relação à latência de enfileiramento, esta permaneceu baixa para a AC de prioridade mais alta (AC0), enquanto nas demais ACs esta métrica aumentou rapidamente conforme o número de veículos aumentou. Já com relação à avaliação em função de um número fixo de veículos (cinco), taxa de chegada de pacotes, e pacotes de 512 bytes, a análise da vazão feita pelos autores indica que, em condições de saturação do canal (taxa de chegada de pacotes curta), os recursos são quase monopolizados pela AC de maior prioridade (AC0). Segundo os autores, novamente a latência de acesso ao canal se manteve baixa para ACs de maior prioridade (AC0 e AC1), enquanto nas demais ACs a latência foi alta em condições de saturação do canal. Além disso, mais uma vez a latência de enfileiramento se mostrou baixa para a AC de maior prioridade, enquanto nas demais ACs esta latência foi alta em condições de saturação do canal. Conforme os autores, as simulações demonstram a acurácia do modelo proposto. Além disso, pelos resultados das simulações, o modelo se mostrou superior na comparação ao modelo do estado da arte. De acordo com os autores, isto se deve à inclusão do procedimento de detecção de portadora inicial no modelo proposto.

Em [93], Heinovski *et al.* comparam o desempenho do IEEE 802.11p e do ARIB T109 por meio de simulações validadas por um estudo analítico. Para as simulações, os autores desenvolveram um modelo baseado nas camadas PHY e MAC do ARIB T109 para o Veins. No modelo, a operação dos protocolos TDMA (*Time-Division Multiple Access*)

e CSMA/CA, entre outros usados no ARIB T109, foram considerados. Os autores também consideram um modelo de desvanecimento causado por prédios em um ambiente urbano. Tal modelo está disponível no Veins para IEEE 802.11p. Neste sentido, experimentos reais também foram realizados como forma de ajustar o modelo para operação em 700 MHz. Para isso, dois veículos portando dois SDRs, receptores GPS (*Global Positioning System*) e antenas omnidirecionais atuaram como transmissor e receptor em um ambiente urbano. Cada um dos dois SDRs foi configurado em 5,9 GHz (IEEE 802.11p) e 868 MHz (ARIB T109), como forma de gerar os dados para parametrização do modelo. O cenário de simulação consistiu de uma área de 156 km^2, mais de 13 mil prédios, e entre 200.000 e 300.000 veículos, sendo 6.000 simultaneamente no horário de pico. Com exceção de uma região de 1 km x 1 km, os dados coletados para avaliação correspondem a uma região de 2 km x 2 km. Apesar de conter três RSUs, cenários com RSUs desativadas também são considerados. Para ambas as tecnologias, foram transmitidos *beacons* de 100 bytes à 6 Mbps, à taxa de 1 Hz. Foi definida uma potência de transmissão 20 dBm e 10 dBm, para o IEEE 802.11p e ARIB T109, respectivamente. A avaliação foi realizada com base na análise da distância de comunicação, taxa de detecção de quadros, utilização do canal, taxa de colisão de quadros e latência fim-a-fim. Em resumo, segundo a análise dos resultados feita pelos autores, por ser menos impactado pelo desvanecimento causado por prédios, o alcance da comunicação obtido no ARIB T109 é muito superior ao obtido pelo IEEE 802.11p, sendo compatível com os valores do estudo analítico. Por outro lado, isto também leva a uma maior interferência no canal, como pôde ser observado na taxa de detecção de quadros, utilização do canal e taxa de colisão de quadros. Por fim, a latência fim-a-fim no IEEE 802.11p se mostrou inferior à obtida no ARIB T109.

Em [72], Mannoni *et al.* avaliam o desempenho do ITS-G5 (IEEE 802.11p) e C-V2X (*Release* 14) Modo 4 por simulações. A avaliação consiste de pacotes com tamanho fixo e variado, e, especificamente para o C-V2X, da variação de parâmetros como o número de RBs (*Resource Blocks*) usados, o tipo de MCS (*Modulation and Coding Schemes*), e se a retransmissão HARQ (*Hybrid Automatic Repeat Request*) é usada – melhora o alcance com base na redundância incremental. Inicialmente, os autores avaliaram a camada PHY em um enlace P2P, cujos resultados indicam, em resumo, que o C-V2X obtém um maior alcance em comparação ao IEEE 802.11p, especialmente se a retransmissão HARQ é usada. Os autores também avaliaram a camada MAC em um enlace compartilhado entre múltiplos usuários. Segundo a análise feita pelos autores, em condições de baixa densidade ($<$150 usuários/km^2), o alcance é maior no C-V2X. Segundo os autores, isto é devido ao emprego de taxas de dados mais baixas no C-V2X (2,4 Mbps) em comparação ao IEEE 802.11p (4,76 Mbps). Por outro lado, em condições de alta densidade ($>$150 usuários/km^2), o IEEE 802.11p supera o C-V2X. Conforme os autores, a avaliação do C-V2X não levou em conta as retransmissões HARQ. Segundo os mesmos, a retransmissão é aceitável em baixa densidade ($<$150 usuários/km^2), o que potencialmente me-

lhoraria o alcance no C-V2X. Já com relação ao tempo médio necessário para acessar o recurso, a análise indica que no IEEE 802.11p ele depende da carga da rede. Em condições de baixa densidade, a latência foi 207 μs, e 10 ms em condições de alta densidade (3000 usuários/km^2). Tal resultado é superior ao obtido pelo C-V2X. Nesta mesma direção, para uma densidade de 100 usuários/km^2, pacotes de 300 bytes, e curto alcance de comunicação, a latência obtida no IEEE 802.11p foi muito inferior à obtida no C-V2X. Entretanto, a latência obtida no C-V2X se torna inferior à obtida no IEEE 802.11p com o aumento do alcance. Especificamente, o C-V2X supera o IEEE 802.11p a partir de 305 m, para uma janela de seleção de 20 ms, e 375 m, para uma janela de 100 ms.

Em [70], assim como Mannoni *et al.* em [72], Shimizu *et al.* comparam o desempenho do IEEE 802.11p e C-V2X (*Release* 14) por meio de simulações em cenários de baixa e alta densidade de veículos. O cenário consistiu de uma via expressa de 5 km de extensão e bidirecional, onde os veículos se locomovem à 100 km/h. Apesar dos 5 km, apenas um trecho central de 1 km foi considerado como forma de evitar o efeito de borda. Duas densidades de veículos são consideradas: (1) alta, com 432 veículos/km; e (2) baixa, com 108 veículos/km. Entre outros parâmetros de simulação, tanto o IEEE 802.11p quanto o C-V2X operam em uma frequência de 5,9 GHz, com canais de 10 MHz, potência de transmissão de 20 dBm, e 0 dBi de ganho de antena. CAMs de 317 bytes (IEEE 802.11p) ou 300 bytes (C-V2X) são geradas a cada 150 ms, se os canais não estiverem congestionados. Para as duas tecnologias, são usados mecanismos para controle do congestionamento do canal. A avaliação foi baseada na PRR (que é similar à PDR), PIR, idade da informação, e latência fim-a-fim. Segundo a análise dos resultados feita pelos autores, a PRR obtida em condições de baixa densidade indica que ambas as tecnologias obtém um desempenho similar até 300 m. Entretanto, acima deste limiar, o desempenho do C-V2X é melhor. Já em condições de alta densidade, o desempenho do IEEE 802.11p supera o do C-V2X em distâncias $<$400 m. Os autores atribuem esse resultado ao controle de congestionamento usado no IEEE 802.11p. Com relação ao PIR obtido em condições de baixa densidade, o desempenho de ambas as tecnologias são comparáveis em distâncias $<$450 m. Assim como ocorreu na PRR, em condições de alta densidade o desempenho do IEEE 802.11p é melhor. A análise também indica que os resultados da idade da informação apresentam o mesmo comportamento do PIR. Além disso, independente da densidade de veículos, a latência fim-a-fim no IEEE 802.11p é muito inferior ($<$2 ms em 90% dos casos) à obtida no C-V2X. Os autores creditam isso ao mecanismo de acesso ao meio de ambas as tecnologias. Enquanto no IEEE 802.11p é usado o CSMA/CA, no C-V2X é usado o SB-SPS (*Sensing-Based Semi-Persistent Scheduling*).

Em [28], Anwar *et al.* avaliam o desempenho da camada PHY do 5G NR-V2X, LTE-V2X, IEEE 802.11bd, IEEE 802.11bd$^{\text{DC}}$ (com DCM e modo de extensão de alcance para MCS0, MCS1 e MCS3) e IEEE 802.11p, por meio de análise teórica e simulações no MATLAB. A análise consistiu em avaliar a taxa de dados máxima e a latência de transmissão,

em função do tamanho do pacote (100/1500 bytes). Já as simulações analisam a PER, PRR, taxa de dados e PIR. Segundo a análise teórica dos autores, o 11bd obtém a menor latência de transmissão, para qualquer tamanho de pacote. Comparado ao IEEE 802.11p, o 11bd possui menor latência pelo uso de MCS de mais alta ordem, além de ter quatro portadoras de dados a mais. Porém, os autores ponderam que o 5G NR-V2X tende a superar o 11bd (ao menos com base no estudo realizado). Quanto à taxa de dados, o 11bd supera a taxa de pico do IEEE 802.11p com pacotes de 100 bytes e 1500 bytes. Novamente, porém, o 5G NR-V2X se mostrou superior. Para as simulações da PER com pacotes de 100 bytes, e modulação QPSK ½ e 64QAM ⅔, a análise dos resultados feita pelos autores indica que o melhor desempenho foi obtido, respectivamente, por 11bd^{DC} e 11bd. Já o IEEE 802.11p e LTE-V2X possuem a pior PER. Com pacotes de 1500 bytes e modulação QPSK ½, apesar da pequena diferença, novamente o 11bd^{DC} apresenta o melhor desempenho, e o IEEE 802.11p o pior. Para 64QAM ⅔, LTE-V2X e 5G NR-V2X possuem a melhor PER. Quanto à PRR com pacotes de 100 bytes, LTE-V2X e 5G NR-V2X superam as variantes do IEEE 802.11, independente da modulação (MCS0 ou 64QAM ⅔), obtendo o dobro do alcance do IEEE 802.11p e 11bd. Segundo os autores, os resultados ainda não indicam que o 11bd^{DC} ofereça o dobro do alcance do IEEE 802.11p. Com pacotes de 1500 bytes, o alcance do IEEE 802.11p foi fortemente impactado. Quanto à taxa de dados com pacotes de 100 bytes, a análise indica que o 5G NR-V2X supera todas as tecnologias, enquanto o IEEE 802.11p é superado pelo 11bd e 11bd^{DC}. Com pacotes de 1500 bytes, a até 10 m, o 11bd^{DC} obtém o melhor desempenho. Porém, a taxa de dados degrada rapidamente com a distância. Novamente LTE-V2X e 5G NR-V2X superam as variantes IEEE 802.11. Quanto ao PIR com pacotes de 100 bytes, 5G NR-V2X, LTE-V2X e 11bd^{DC} obtém o melhor desempenho. Já para 1500 bytes, o 5G NR-V2X supera os demais. Conforme os autores, é esperado que o 5G NR-V2X supere as demais tecnologias, e que o 11bd ofereça maior alcance e taxa de dados em comparação ao IEEE 802.11p.

Em [119], Teixeira *et al.* avaliam o desempenho do IEEE 802.11p por meio de experimentos reais com interfaces DCMA86-P2, baseadas no *chipset* Atheros AR5414A-B2B. Por meio de dois *laptops* equipados com as interfaces citadas e um módulo de GPS, foram analisados (1) o tempo de associação, cuja análise foi feita em laboratório com ambos os *laptops* um ao lado do outro; e (2) vazão, latência, *jitter* e PDR, baseadas na comunicação entre dois veículos portando um *laptop*, onde cada interface foi conectada à uma antena de 5 dBi fixada no teto dos veículos, junto à antena do GPS. Os experimentos foram realizados em um trecho com cerca de 650 m. Um veículo (servidor) foi mantido fixo em um ponto da via, enquanto o outro (cliente) se locomovia à 20 km/h, 40 km/h e 60 km/h. A avaliação consistiu no envio, pelo cliente, de pacotes UDP numerados e com tamanho variando entre 150 bytes, 500 bytes e 1460 bytes. O servidor responde ao cliente com o número do pacotes recebidos e calcula as métricas. Segundo a análise dos resultados feita pelos autores, em um ambiente controlado, o tempo de associação foi

$1{,}035 \pm 0{,}0024$ s. Quando a distância entre os veículos foi $<$100 m, foi obtida uma vazão média de 1 Mbps, 3 Mbps e 8 Mbps, com pacotes de 150 bytes, 500 bytes e 1460 bytes, respectivamente. Para distâncias $>$300 m, foi nítida a redução da vazão, especialmente com pacotes de 1460 bytes. Quanto à variação da latência em relação à distância, um aumento gradual com base na distância pôde ser observado para todos os tamanhos de pacotes. A latência média foi de cerca de 10 ms para pacotes de 150 bytes, e entre 20 ms e 500 ms para pacotes de 1460 bytes. Quanto ao *jitter*, este cresceu gradualmente com a distância, especialmente para pacotes de 500 bytes. Como esperado, o *jitter* para pacotes de 1460 bytes foi o maior obtido. Já com relação à taxa de perda em diferentes distâncias e velocidades, exceto em distâncias $>$300 m (onde a perda foi $>$10%), nos demais casos esta métrica ficou próxima de 1%. Pelos resultados, os autores consideram o uso de pacotes de 500 bytes mais indicado para aplicações de segurança, enquanto pacotes maiores podem ser usados em aplicações de entretenimento. Os autores também destacam o impacto da velocidade na vazão (mais observável em pacotes de 1460 bytes), latência e na taxa de perda.

Em [53], Barcelos *et al.* propõem um sistema de monitoramento de veículos que usa um dispositivo de comunicação de baixo custo compatível com o IEEE 802.11p. No sistema, via Bluetooth, uma aplicação Android executando em um *smartphone* coleta dados do motor (temperatura, RPM, velocidade) através de um dispositivo conectado à interface OBD-II do veículo. Ao mesmo tempo, é feita a coleta de dados (*timestamp*, latitude, longitude) obtidos via GPS no *smartphone*. Via IEEE 802.11g, a aplicação Android transmite os dados para um dispositivo atuando como uma OBU, composto por uma placa RouterBoard RB433AH, da MikroTik. Via IEEE 802.11p, a OBU pode se comunicar com outras OBUs e RSUs de forma a encaminhar os dados coletados para um servidor remoto, onde estes serão armazenados para posteriores consultas (histórico, localização do veículo em tempo real) via interface Web. Os dispositivos foram avaliados em dois cenários reais: (1) V2V, baseado na comunicação entre dois veículos localizados nos extremos da via, distantes 792 m, e que se locomovem em direção um do outro; e (2) híbrido, onde um veículo fixo em uma posição intermediária da via (465 m) serve de intermediador da comunicação entre um veículo móvel, que inicia sua rota à partir de um extremo da via (0 m), e a RSU, bloqueada por um prédio. Em ambos os cenários, os veículos se locomovem à 20 km/h, 40 km/h e 60 km/h. Visando otimizar o tempo de contato, a transmissão de *beacons* foi desativada. Os dispositivos operam a uma taxa fixa de 6 Mbps, frequência de 5,890 GHz e banda de 10 MHz. A avaliação consistiu da análise da taxa de perda, atraso de entrega, e taxa de transmissão, com base na transmissão de pacotes UDP de 512 bytes. Segundo a análise dos resultados feita pelos autores, a comunicação foi possível em um diâmetro de 700 m. Em termos da taxa de perda, a até 200 m, a mesma foi $<$10% para as comunicações V2V, e $<$20% para as comunicações V2I. Além disso, um compromisso entre o aumento da velocidade e o aumento da perda foi identificado. O atraso, cuja média foi $<$100 ms, não variou de forma significativa com a distância. Já o aumento da velocidade levou ao

aumento do atraso, especialmente nas comunicações V2V à 60 km/h. Quanto à taxa de transmissão, esta se manteve constante independente da distância, com maior variação nas comunicações V2V.

Em [120], Vivek *et al.* avaliam o desempenho do IEEE 802.11p por meio de experimentos reais com dispositivos de comunicação comerciais. Os experimentos foram realizados usando duas OBUs e uma RSU, modelo ARADA LocoMate, dotadas de *hardware* dedicado. A avaliação consistiu da análise do RTT, *jitter*, e taxa de perda de pacotes. O cenário consistiu em um trecho de via de 600 m, que devido a um declive de cerca de 1,5 m, causa condições NLoS na comunicação entre RSU e OBU entre os pontos 180 m e 450 m. A RSU foi instalada em um extremo da via, à uma altura de 6 m. Uma das duas OBUs foi instalada próxima à RSU como forma de gerar tráfego no canal de comunicação e interferência no canal adjacente. As comunicações foram realizadas à taxa de 6 Mbps no CCH e no SCH 172, variando a distância entre a OBU móvel (veículo) e a RSU. Segundo a análise dos resultados feita pelos autores, em ambos os canais, a taxa de perda aumenta com a distância entre a OBU e a RSU. Um aumento da taxa de perda ocorreu próximo ao ponto 200 m da via de testes, o que os autores acreditam ser devido às condições NLoS provocadas pelo declive próximo à este ponto da via. Já com relação ao *jitter* e RTT, nenhum compromisso com o aumento da distância foi observado. Para ambos os canais, o RTT médio obtido ficou entre 2 ms e 3 ms, enquanto o *jitter* variou entre 0,4 ms e 1,3 ms.

Em [55], Wang *et al.* avaliam a confiabilidade das comunicações V2V por meio de experimentos reais realizados em condições de tráfego real. A avaliação consistiu em (1) pré-processar os dados; (2) classificar as condições de LoS; e (3) analisar métricas de desempenho. Em (1), é feito um pré-processamento seguindo um critério prévio, como a remoção de dados coletados enquanto os veículos executavam uma conversão. Em (2), os autores propõem um método de classificação *fuzzy* das condições de LoS encontradas nos experimentos. Por exemplo, em um dos casos, os autores usam a densidade de tráfego, estimado com base na velocidade dos veículos, para definir a probabilidade do sinal ser bloqueado por veículos intermediários. Já em (3), a confiabilidade das comunicações é medida com base na análise do RSSI (*Received Signal Strength Indication*), PDR e latência. O cenário de avaliação consistiu de dois veículos se locomovendo em uma via expressa real com cerca de 65 km de extensão e limite de velocidade de 80 km/h. Os experimentos foram realizados em condições de tráfego real, inclusive em horários de pico. Cada veículo portou um *laptop* e uma WSU (*Wireless Safety Unit*) Denso, compatível com o IEEE 802.11p. Uma aplicação em cada *laptop* era responsável por criar, à taxa de 5 Hz, um pacote de 64 bytes e enviar, via *socket* UDP e por meio de um cabo RJ45, para a WSU do veículo. Via IEEE 802.11p, a WSU atuando como transmissor propagava o pacote na rede. Ao receber o pacote, a WSU do veículo atuando como receptor encaminhava o pacote recebido para o *laptop* local, já contendo o RSSI sensoreado. As comunicações foram realizadas no CCH, à 6 Mbps. Segundo a análise dos resultados feita pelos autores,

as condições de LoS são principalmente determinadas pelo declive da via e pela presença de veículos intermediários entre os veículos atuando como transceptores. Além disso, o desempenho em condições reais se mostrou distante do ideal: a PDR foi $< 100\%$ mesmo quando ambos os veículos estavam próximos e o alcance de comunicação foi muito inferior ao alcance teórico atribuído ao IEEE 802.11p. A análise também indica que fatores ambientais têm pouco impacto na latência, que permaneceu <5 ms em 96,5% dos dados.

Em [121], Rajput *et al.* analisam o desempenho do IEEE 802.11p por meio de experimentos reais. O cenário consistiu de um trecho de 110 m, onde um veículo fixo transmitia BSMs de 45 bytes à 6 Mbps a um outro veículo, que se locomovia em direção ao primeiro. As transmissões foram feitas no SCH 172 usando uma OBU ARADA LocoMate, com potência de 14 dBm. A avaliação baseou-se na latência e no RSSI. Segundo a análise dos resultados feita pelos autores, apesar da variação com o aumento da distância, um compromisso entre o aumento da latência e o aumento da distância não foi identificado. A latência variou entre 0,9 ms e 541,63 ms, com média de 94 ms. Quanto ao RSSI, este permaneceu alto para distâncias <20 m. Como ocorreu na análise da latência, nenhum compromisso com a distância foi identificado, apesar da média do RSSI variar em mudanças drásticas na distância. Os registros dos experimentos foram disponibilizados em um *dataset* para uso público.

Em [122], Bloessl *et al.* apresentam um *framework* baseado em SDR para simulação e experimentação com IEEE 802.11p. Como transceptor SDR IEEE 802.11p, foi usada uma plataforma GNU Radio. Segundo os autores, baseadas em GPP (*General Purpose Processor*), tais plataformas processam o sinal em tempo real a partir dos dados do SDR. Além disso, podem ser usadas em simulações, aplicando modelos de propagação, entre outros efeitos. A implementação da camada PHY é feita em um PC normal. Conforme os autores, isto permite fácil modificação e uso. A avaliação consistiu de simulações, testes de interoperabilidade e experimentos em campo. Nas simulações, os resultados da taxa de entrega de quadros concordaram com a literatura, no que se refere às modulações mais altas requererem um SNR maior. A interoperabilidade foi testada com três tipos de dispositivos: (1) interfaces WLAN operando nos modos IEEE 802.11a/g; (2) interfaces DCMA-86P2, adaptadas para o IEEE 802.11p, e uma interface ath9k baseada no *chipset* Atheros, compatível com IEEE 802.11p; e (3) OBUs MK5 da Cohda Wireless. A capacidade de processamento do sinal em tempo real também foi avaliada em diferentes plataformas (PC, MacBook, laptop) e condições de saturação do canal (envio de quadros de 435 bytes e 1500 bytes à 10 Hz em modulações QPSK ½ e 64-QAM ¾). Segundo a análise dos resultados feita pelos autores, o receptor foi capaz de decodificar todos os quadros, sem perdas. Experimentos também mostraram que é possível implementar, com pequenas modificações, funções de AGC (*Automatic Gain Control*) e acesso ao canal (EDCA) para transmissões em *broadcast*, com o objetivo de melhorar o atraso e o *jitter*, inerentes ao SDR. Os experimentos de campo consistiram de dois veículos se locomovendo entre

40 km/h e 70 km/h, em diferentes ambientes. No transmissor, quadros de 435 bytes foram transmitidos na modulação QPSK ½, usando a OBU MK5 e o SDR. Já no receptor, além da OBU MK5 e do SDR, também foi usada uma interface DCMA-86P2. Quanto aos resultados da transmissão, a análise da PDR obtida pela OBU MK5 indica que o SDR é capaz de gerar quadros compatíveis com o IEEE 802.11p. Além disso, o desempenho dos transmissores se mostrou semelhante. Quanto aos resultados da recepção, usando a OBU MK5 como transmissor, a análise da PDR indica que os receptores apresentam desempenho comparável, com ligeira vantagem para a OBU MK5. Enquanto o SDR perdeu 20% dos quadros, a OBU MK5 e a DCMA-86P2 perderam 10%.

Em [123], Huang *et al.* avaliam o desempenho do IEEE 802.11p por meio da análise dos dados do projeto SPMD (*Safety Pilot Model Deployment*), da Universidade de Michigan. O projeto possui 2800 veículos, além de 25 RSEs (*Road Side Equipment*), que é similar às RSUs. Todos possuem algum dispositivo para comunicação veicular, de três fornecedores. Os dados foram coletados durante mais de 1000 dias, em condições de tráfego real, abrangendo as cidades de Ann Arbor, Michigan, e Ohio. Cerca de 5,6 TB de dados foram coletados. Na análise dos autores, foram considerados dados de 1050 veículos, coletados por RSEs durante 933 dias. A antena é montada sob a janela traseira dos veículos. Os dados coletados cobrem trechos com interseções, elevação viária, folhagem de árvores (no inverno/verão), condições NLoS (geradas por prédios/veículos) e condições LoS. O impacto das condições climáticas (céu limpo/chuva/neve), direção do veículo e de diferentes rádios DSRC também foi analisado. A análise mediu o alcance máximo e a PDR a partir da comunicação entre veículos se locomovendo à 18 km/h, 36 km/h e 54 km/h, e RSEs fixas em interseções. Segundo a análise dos resultados feita pelos autores, a elevação da via afeta a comunicação, já que os picos mais altos da distância em que o RSE recebe a primeira BSM do veículo se alinham com as condições de LoS e com a elevação da via. A análise também demonstra que as condições NLoS geradas por prédios e veículos são a principal causa de impacto no alcance máximo e na PDR, constatado ao comparar com os resultados da avaliação da elevação da via e tráfego noturno. Durante o inverno, o impacto das condições NLoS causadas pela folhagem de árvores é menor, já que a distância na qual o RSE recebe a primeira BSM do veículo é um pouco maior em comparação aos meses de verão. Não foi possível observar diferenças entre as diferentes condições climáticas. Por outro lado, foi possível observar uma influência da direção do veículo. Nos casos onde o veículo se afastou do RSE, o alcance máximo e a PDR foi maior. Conforme os autores, isto se deve à posição da antena no veículo. A análise indica pouca influência do número de transmissores, se $\leq$6. Por fim, a análise dos diferentes rádios DSRC indica que, em termos de alcance, os resultados são semelhantes, enquanto a PDR mostra algumas diferenças.

Em [23], Renda *et al.* apresentam uma extensa análise do padrão de recepção de *beacons* por experimentos reais. A meta é avaliar a importância do PIR em estimar o nível de consciência situacional, já que esta métrica se mostrou, pelo Coeficiente de Pearson,

fracamente correlacionada com a PDR. Os experimentos foram feitos em condições reais de tráfego, com densidade variando entre média/densa, e velocidade entre 90 km/h a 130 km/h. A avaliação contou com dois cenários: (1) dois veículos em um trajeto de ida-e-volta com 906 km, e dois veículos em dois trajetos de ida-e-volta, com 176 km cada; e (2) três veículos, em três trajetos de ida-e-volta com 176 km cada. Na análise em (1), os autores definiram dois tipos de alcance: até 80 m, e até 160 m. Com isso, o efeito de borda é evitado. Em (2), os veículos, em uma configuração *car-following*, são identificados como V0 (dianteiro), V1 (intermediário), e V2 (traseiro). Baseado nesta configuração, três tipos de enlaces diretos são considerados pelos autores: V0/V1, V1/V2, e V0/V2. Além disso, um enlace por múltiplos saltos V0/V2, passando por V1, também é considerado. Em cada um dos três trajetos de (2), foram usados um veículo alto (cerca de 1,7 m) e dois veículos curtos (1,45 m). A posição do veículo alto foi alternada (dianteiro/intermediária/traseiro) ao longo dos trajetos. A avaliação foi baseada na análise da PDR, PIR, número e distribuição de *blackouts* (PIR $\geq$1 s, com base no tempo de reação do motorista), e frequência média de *blackouts*. Cada veículo foi equipado com um dispositivo LinkBird-MX v3, da NEC, compatível com o IEEE 802.11p, receptor GPS, *laptop* e antena omnidirecional com 5 dBi de ganho, no teto do veículo. Os *beacons* foram transmitidos no canal 180, à 10 Hz. Pela distribuição do PIR, os autores concluem que *blackouts* de consciência situacional são frequentes e tendem a ocorrer em lote já que possuem forte correlação positiva no tempo. Segundo os autores, o desempenho do *beaconing* é fortemente impactado pela configuração dos veículos (alto/baixo) e pelas condições LoS/NLoS. Isto pode ser observado pela ocorrência de *blackouts* e pelo aumento da média do PIR. Como forma de melhorar o PIR em condições NLoS, um método de transmissão por múltiplos saltos foi proposto, onde dados situacionais de veículos vizinhos são inseridos nos *beacons* via *piggybacking*. Segundo a análise dos autores com base nos dados dos experimentos, o método é capaz de reduzir a média do PIR, e a probabilidade/frequência de *blackouts* nas comunicações de até dois saltos. Nas simulações, a análise demonstra que o benefício do método se estende além do segundo salto. Os autores também propõem o modelo Gilbert–Elliot, de forma a modelar o padrão de recepções de *beacons* observado nos experimentos reais.

Em [52], Sassi *et al.* avaliam o desempenho do IEEE 802.11p por experimentos reais e simulações no MATLAB, e investigam a correspondência dos resultados. Os experimentos reais foram realizados em uma pista de 1500 m, de um aeródromo não utilizado. Com dois veículos equipados com OBUs ARADA LocoMate, três cenários foram avaliados: (1) alcance da comunicação no IEEE 802.11p; (2) efeito da velocidade moderada; e (3) efeito da alta velocidade na comunicação. Em (1), a análise é realizada com ambos os veículos estáticos, sendo um transmissor, e o outro receptor. O objetivo é analisar o efeito da SNR na PLR (*Packet Loss Ratio*) à medida que aumenta a distância entre os veículos, variando entre 100 m e 1000 m, em passos de 100 m. Em (2), um dos veículos, atuando como uma RSU fixa na via, transmitia pacotes em direção ao outro veículo, que se locomovia em

direção ao primeiro entre 10 km/h e 110 km/h. O objetivo é avaliar a comunicação V2I, e analisar o impacto da mobilidade moderada na PLR. Já em (3), a comunicação V2V é avaliada, onde um veículo transmitia pacotes ao outro veículo, e ambos se locomoviam em direção um do outro entre 10 km/h e 110 km/h. Com velocidades relativas de até 220 km/h, o objetivo de (3) é analisar o impacto da alta mobilidade na PLR. Os mesmos cenários são considerados nas simulações, e a análise é feita em cima da BER. Nas simulações, os autores implementaram a camada PHY do IEEE 802.11p, e um modelo de canal Rice é considerado. Nos dois ambientes, são consideradas transmissões em todas as modulações do IEEE 802.11p. Segundo a análise dos resultados feita pelos autores, o alcance máximo teórico de 1000 m do IEEE 802.11p só pode ser obtido à 3 Mbps e 4,5 Mbps. Em todas as modulações, a PLR/BER aumenta com a distância. Apesar disso, os autores mencionam que taxas mais altas (18 Mbps, 24 Mbps, e 27 Mbps) podem ser usadas se os veículos estiverem próximos (até 200 m). Segundo os autores, isto se deve ao fato de que, se a potência de transmissão é fixa, a qualidade do sinal melhora ao reduzir a distância. Os autores concluem que taxas mais baixas são adequadas para comunicações em longa distância. Com relação ao efeito da mobilidade, a análise indica que a velocidade – moderada e especialmente a alta – afeta a comunicação dado o efeito Doppler. Quanto maior foi a velocidade do veículo, pior foi a qualidade das transmissões em termos da PLR/BER. No geral, quanto maior foi a taxa de dados, maior foi a PLR/BER. Os autores concluem que o modelo do MATLAB foi capaz de refletir os resultados dos experimentos reais.

Em alguns casos, o uso de modelos muito abstratos, visando um melhor desempenho computacional, pode fazer com que os resultados das simulações não sejam condizentes com a realidade. Igualmente, apesar de testes práticos serem altamente relevantes por permitirem avaliar a operação real de um sistema [122], o custo e a complexidade tornam a avaliação em larga-escala proibitiva. Inspirados pelo trabalho de Sassi *et al.* [52], nesta tese também investiga-se se os resultados obtidos por simuladores são equivalentes aos de experimentos reais, no que tange à transmissão periódica de BSMs sobre o IEEE 802.11p. Como Sassi *et al.*, os experimentos foram feitos em uma pista de 1200 m, de um aeroporto desativado, onde cenários com velocidades relativas de até 160 km/h foram considerados visando avaliar o efeito da mobilidade na comunicação. O efeito da variação das modulações/taxas de dados do IEEE 802.11p também é investigado. Como as OBUs ARADA LocoMate usadas por Sassi *et al.*, as OBUs e RSU MK5 da Cohda Wireless, utilizadas nesta tese, são dispositivos comerciais com *hardware* dedicado. Segundo Bloessl *et al.* [122], tais dispositivos são baseados em *hardware* e *software* avançados, e fornecem pilhas de comunicação completas para o DSRC/WAVE. Dispositivos Cohda respondem por mais de 60% dos experimentos de comunicação com veículos, com cerca de 18 mil km de testes de campo [124]. Assim, é possível considerar que a implementação das pilhas WAVE/IEEE 802.11p em tais dispositivos é bastante testada. Diferente de Sassi *et al.*, a avaliação da comunicação V2I se deu pela troca de dados entre uma OBU

e uma RSU, e não entre OBUs. Cabe ressaltar que, em tal cenário, o veículo que se locomove em direção à RSU atua como transmissor. Em Sassi *et al.*, o MATLAB é usado como simulador. Nesta tese, os resultados dos experimentos reais são confrontados com os obtidos pelo NS-3/PhySim e Veins/MiXiM. Além disso, além da PLR – aqui tratada como PDR – analisada por Sassi *et al.*, investiga-se também o PIR, dada a sua importância para aplicações de segurança que requerem atualizações em um intervalo regular [28]. Esta análise teve como inspiração o trabalho de Renda *et al.* [23], especialmente quanto à análise de correlação entre PIR e PDR. Diferente de Renda *et al.*, nesta tese o efeito de borda é considerado.

3.2 Análise de Viabilidade do Wi-Fi Direct

Segundo Khan *et al.* [77], trabalhos com Wi-Fi Direct podem ser divididos entre aqueles que se dedicam a avaliar seus recursos e aqueles que visam estendê-los. Neste sentido, Khan *et al.* enumeram trabalhos que visam, por exemplo, a redução do atraso nas etapas de *Discovery*, *Service Discovery* e estabelecimento do grupo P2P. Critérios objetivos para eleição do GO também são um tema explorado. Nestes, algoritmos visam estabelecer parâmetros para definição do *Intent Value*, baseados na bateria restante do dispositivo, capacidade de processamento, entre outros. Dado que a transmissão por múltiplos saltos não é especificada no Wi-Fi Direct, propostas nesta área também existem na literatura, especialmente usando a entidade P2P *Concurrent Device* como retransmissor. A economia de energia no GO é um tema recorrente, com trabalhos visando a definição de parâmetros para o OppPS e NoA, bem como novos protocolos. Por fim, o aumento da persistência do grupo P2P também é um tema pautado, onde mecanismos visam a definição de uma entidade GO de *backup* como forma de evitar que um novo processo de conexão seja realizado após o GO deixar o grupo [39]. O foco, porém, será nas análises de viabilidade do Wi-Fi Direct no contexto veicular. Também são mostrados os trabalhos relacionados à aplicação do *beacon-stuffing*, para transmissão de dados sem conexão usando o Wi-Fi Direct.

Em [3], Camps-Mur *et al.* apresentam o que parece ser a primeira análise de desempenho do Wi-Fi Direct. Por meio de experimentos reais e simulações, o atraso na formação dos grupos *Standard*, *Autonomous* e *Persistent* foi avaliado. Além disso, os autores também implementaram e avaliaram o protocolo NoA, para economia de energia no Wi-Fi Direct. Em ambos os casos, a avaliação prática foi baseada em uma implementação de código-aberto do Wi-Fi Direct baseada no *wpa_supplicant*. Não está claro se o simulador usado foi desenvolvido pelos autores ou se foi usado um simulador da literatura. A avaliação do atraso na formação dos grupos foi realizada usando dois *laptops* em um ambiente com interferência. Segundo a análise dos resultados feita pelos autores, o *Scan* inicial é de no mínimo 3 s para todos os casos, e os atrasos para descoberta nos modos *Standard* e *Persistent* são similares (1 s a 7 s). Já o modo *Autonomous* obtém um atraso constante

(3 s). Quanto ao atraso para formação do grupo, os três modos mostram um comportamento similar, apesar do modo *Persistent* reduzir o atraso em 500 ms. Já a similaridades dos modos *Standard* e *Autonomous* se deve ao fato de, neste último, a simplicidade do processo estar associada apenas à etapa de negociação do GO, que infere um atraso muito pequeno em comparação ao provisionamento WPS. Visando uma execução automatizada, os autores pré-provisionaram os dispositivos com um PIN WPS. Em 80% dos casos, o atraso total do modo *Autonomous* é $<$5 s, enquanto que nos modos *Standard* e *Persistent* pode chegar a 8 s e 9 s, respectivamente. Por não considerar interferência, no geral as simulações mostraram algumas diferenças em relação aos experimentos reais. Já a avaliação do NoA consistiu em analisar o compromisso entre o tamanho dos períodos de ausência e a economia de energia/vazão do grupo P2P. Segundo os autores, uma política dinâmica de ajuste dos períodos, baseada no algoritmo ASPP (*Adaptive Single Presence Period*), é mais efetiva em obter boa vazão e baixo consumo de energia.

Em [2], Jeong *et al.* propõem o que parece ser a primeira abordagem do Wi-Fi Direct em VANETs para aplicações de segurança. O método, um esquema híbrido de comunicação baseado no Wi-Fi Direct e 4G, é composto por três componentes: (1) servidor; (2) WDMS (*Wi-Fi Direct Management System*); e (3) WDE (*Wi-Fi Direct Extension*). Os dois últimos rodam nos *smartphones*. Por meio do WDMS, cada dispositivo envia ao servidor, via rede 4G, seu endereço MAC (*Medium Access Control*), posição e velocidade. Essa informação é atualizada no servidor sempre que o dispositivo muda de posição ou estado de conexão com a rede. Sempre que a distância entre dois dispositivos for $<$200 m, o servidor envia uma mensagem de formação de grupo aos dispositivos com a rede apropriada e o GO. O WDMS também armazena os dados de dispositivos adjacentes enviados pelo servidor. Segundo os autores, ele também decide se avisa sobre colisões usando uma BSM recebida do WDE, um sistema que regula o fluxo de funções sequenciais do Wi-Fi Direct. Aliás, decisões do WDE, como pular o *Discovery* do Wi-Fi Direct ou iniciar um grupo P2P com um vizinho, depende de uma mensagem de controle do WDMS. A avaliação do método se deu usando veículos reais equipados com *smartphones*. Os cenários se diferenciam pelo número de veículos (2 ou 3), pelas velocidades (20 km/h ou 30 km/h) e pela forma como os veículos se locomovem (em direções opostas, na mesma direção) na formação/desativação do grupo P2P. Neste caso, um dos objetivos é avaliar se o método permite a reconexão rápida nos casos onde o GO deixa o grupo P2P. Segundo a análise dos resultados feita pelos autores, o atraso de descoberta caiu de 1,5 s para 100 ms com o método proposto. No cenário que demonstra a desconexão do GO, o atraso caiu de 3 s para 200 ms. Além disso, segundo os autores, o método proposto também não consome uma grande quantidade de dados a ponto de onerar a solução pelo uso da rede 4G.

Em [39], Manamperi *et al.* avaliam um método de transmissão *broadcast* entre GO e clientes do grupo, baseado no método proposto por Satish *et al.* [125]. O método, denominado GOB (*Group Owner Broadcast*), visa substituir o modelo de transmissão P2P

original do Wi-Fi Direct. Os autores avaliam sua aplicação em VANETs. No método P2P original, a troca de dados entre GO e clientes (e vice-versa) ocorre após a transmissão de quadros RTS (*Request to Send*) e CTS (*Clear to Send*). Além disso, quadros ACK (*ACKnowledgment*) são enviados após cada recepção bem-sucedida. Segundo os autores, no método P2P original, para um grupo de tamanho n, podem ser feitas $n-1$ transmissões de clientes para o GO, além de $(n-1)^2$ transmissões do GO para os clientes. No GOB, o GO recebe os quadros dos clientes e, junto ao seu próprio quadro, agrega tudo em um quadro único, enviando-o aos clientes do grupo. Por ser *broadcast*, ACKs não são usados. Por meio de uma análise teórica dos métodos P2P e GOB, o atraso total e o consumo de energia médio do GO foi avaliado. A análise dos resultados feita pelos autores indica, para ambas as métricas, uma relação quadrática com n no método P2P e uma relação linear no GOB. Simulações no INET também foram realizadas, tendo como base a comunicação entre veículos. Segundo a análise dos resultados feita pelos autores, o atraso e consumo de energia é maior no método P2P em comparação ao GOB. Devido à ausência de ACKs e retransmissões, as simulações também indicam um aumento da perda de quadros conforme aumenta o número de veículos no grupo. Apesar disso, para grupos de tamanho moderado, as perdas tendem a ser aceitáveis.

Em [40], Balasundram *et al.* comparam o desempenho do Wi-Fi Direct com o obtido pelo IEEE 802.11p. Via simulações no NS-3, métricas como vazão, atraso e taxa de perda foram avaliadas. Dois cenários, com base no modo de comunicação, são considerados: (1) um salto, realizada por dois veículos que transmitem dados com destino a uma RSU; (2) múltiplos saltos, baseada na transmissão de dados entre veículos de diferentes *clusters*. Cabe ressaltar que, nas simulações do NS-3, os autores consideraram que os grupos P2P compostos por veículos já estavam formados quando a comunicação era feita, desconsiderando o atraso para formação destes grupos. Aliás, segundo Khan *et al.* [77], o NS-3 não possui suporte ao Wi-Fi Direct, já que o *Discovery* e *Service Discovery* não são implementados neste simulador. A análise dos resultados feita pelos autores indica, para ambas as tecnologias, um aumento da perda de quadros conforme aumenta a distância entre transmissor e receptor. Entretanto, esta perda aumenta mais rapidamente no Wi-Fi Direct em comparação ao IEEE 802.11p. Segundo os autores, isto pode estar relacionado com a menor potência de transmissão do Wi-Fi Direct. O mesmo comportamento foi observado em relação à vazão, mesmo considerando o emprego de mobilidade. Na transmissão por múltiplos saltos, o atraso fim-a-fim médio no Wi-Fi Direct foi superior em comparação ao obtido no IEEE 802.11p, ao passo que a taxa de recepção de quadros média foi inferior.

Em [95], Shahin *et al.* propõem o protocolo ADS (*Alert Dissemination using Service discovery*) para disseminação de alertas baseado no modelo *Publish/Subscribe* do *Service Discovery* do Wi-Fi Direct. O objetivo é permitir a disseminação de alertas usando o mecanismo de requisições e anúncios, sem que seja necessário estabelecer um grupo P2P. No protocolo, ao detectar um alerta, um dispositivo cria um registro de anúncio de ser-

viço e substitui seu campo de descrição pelos dados do alerta. Ao receber uma requisição de outro dispositivo para listar seus serviços suportados, o detentor do alerta responde anunciando o serviço/alerta armazenado. O ADS é composto de duas partes: (1) gerenciamento de alertas locais; e (2) gerenciamento de alertas remotos. Enquanto o primeiro é responsável pela disseminação de alertas detectados pelo próprio dispositivo, o segundo trata de alertas recebidos de outros dispositivos. Por meio do gerenciamento de alertas remotos, é possível reencaminhar alertas usando o mesmo mecanismo do *Service Discovery*. Alertas são compostos pelo ID do dispositivo que o gerou, por um número de sequência, por uma descrição e por um campo que atesta se ele ainda é válido. Além disso, para cada alerta também é mantido um TTL (*Time-To-Live*), que permite descartar alertas inativos (que já não são mais válidos) após um dado tempo. O protocolo foi implementado em *smartphones* com Android, com os alertas sendo baseados na posição geográfica obtida a partir da interação de um usuário com um mapa. Apesar da realização bem-sucedida de testes de validação, a operação do protocolo em condições reais não foi descrita pelos autores. Apenas uma análise teórica do desempenho foi realizada.

Em [68], Won *et al.* propõem um completo sistema para monitoramento do risco de colisões entre veículos e pedestres. No WiSafeCross, se um pedestre caminha próximo à faixa de travessia, denominada zona de alerta, enquanto visualiza a tela do *smartphone*, mensagens são trocadas via Wi-Fi Direct com os veículos que se aproximam. Tais mensagens carregam o tempo para que pedestre e veículo alcancem a faixa, permitindo calcular o risco de colisão e enviar alertas ao pedestre e/ou ao motorista. O sistema é composto por cinco módulos, responsáveis por: (1) aumentar a precisão do GPS, identificando a posição mais provável do pedestre; (2) desativar o módulo GPS enquanto o pedestre não estiver na zona de alerta, reduzindo o consumo de energia; (3) detectar sinais de distração baseados na visualização da tela do *smartphone*; (4) definir quando e para quem enviar o alerta se houver risco de colisão; e (5) definir a comunicação entre pedestres e veículos usando o modo *Autonomous* do Wi-Fi Direct, com o pedestre atuando como GO. Para permitir a comunicação NxN no Wi-Fi Direct, foi proposta uma estratégia baseada na inclusão de um novo pedestre ao grupo já criado, com sua comunicação intermediada pelo GO. Inicialmente, a viabilidade do Wi-Fi Direct para o cenário proposto foi avaliada. Usando um veículo e *smartphones* reais, foram analisados, via comunicação V2P, o alcance da comunicação e o atraso fim-a-fim. Segundo a análise dos resultados feita pelos autores, a PDR é $> 80\%$ em distâncias < 70 m e o RTT (*Round-Trip-Time*) ficou entre 100 ms e 200 ms. Quanto à avaliação geral, o sistema foi capaz de reduzir o erro do GPS em área urbana em 72%. A ativação do GPS ocorreu a cerca de 1 m da zona de alerta, quando considerada a velocidade média do pedestre. Em 92% dos casos, a visualização da tela do *smartphone* foi detectada corretamente. Quanto menor é a velocidade do veículo, maior é a chance de evitar colisões. Por fim, a PDR foi relativamente alta no cenário com mobilidade, apesar da ligeira queda ao aumentar a velocidade até 32 km/h.

É importante fazer algumas observações com relação aos trabalhos relacionados. Trabalhos propostos com o objetivo de estender o Wi-Fi Direct como forma de melhorar a tecnologia, quando aplicados em *smartphones* Android, podem requerer que privilégios de administrador (*root*) sejam empregados no dispositivo. Por exemplo, a comunicação por múltiplos saltos, realizada entre GOs, não é suportada no Android [95]. Portanto, usá-la requer a modificação do código-fonte. Por conta disso, muitos destes trabalhos não são avaliados em testes práticos usando *smartphones* reais com Android, ou quando são, requerem *root*. Nesta tese, o objetivo é analisar a viabilidade do Wi-Fi Direct no ambiente veicular por meio de testes práticos usando *smartphones* reais, sem que seja necessário modificar o padrão. O objetivo é explorar o caráter ubíquo dos *smartphones*. Exigir *root* poderia tornar o uso do Wi-Fi Direct pouco prático para aplicações em redes veiculares. Além disso, alguns trabalhos analisam o Wi-Fi Direct por meio de simuladores. Nestes casos, existe a chance dos parâmetros e modelos de simulação não refletirem as especificações do padrão e/ou as condições físicas do mundo real. Em alguns casos, o próprio simulador pode não possuir módulos compatíveis com o Wi-Fi Direct, como o NS-3 [77]. Neste sentido, a comparação dos resultados entre experimentação prática e simulações pode ajudar a oferecer alguma confiabilidade. Com base nessa premissa, nesta tese foi investigado se os resultados dos testes práticos que analisam o Wi-Fi Direct para uso em redes veiculares são equivalentes aos obtidos pelo módulo de simulação para Wi-Fi Direct do INET [63].

Particularmente, a análise de viabilidade do Wi-Fi Direct feita nesta tese teve como inspiração a análise preliminar de Won *et al.* [68]. Antes de avaliarem o WiSafeCross de uma forma geral, os autores analisaram a viabilidade do Wi-Fi Direct para o cenário proposto com base na PDR, atraso fim-a-fim e alcance da comunicação, variando a distância de comunicação entre um pedestre e um veículo até alcançar 70 m. Nesta tese, além da PDR e do alcance, o PIR também foi avaliado. A avaliação do alcance via Wi-Fi Direct foi feita de 50 m à 150 m, além de uma medição em 200 m. As medições foram feitas com base na comunicação entre dois pedestres. Em [68], a avaliação geral do sistema também foi realizada em um ambiente de mobilidade, onde um veículo se locomovendo a até 32 km/h se comunicava com um pedestre via Wi-Fi Direct. Nesta tese, o impacto do CET foi analisado em um cenário similar, porém com o veículo se locomovendo a até 100 km/h. Além disso, em [68], uma pista com apenas 75 m e sem obstáculos fora usada. Dado o alcance teórico de 200 m do Wi-Fi Direct [77], possivelmente veículo e pedestre já faziam parte de um grupo P2P mesmo antes do veículo ser colocado em movimento. Nesta tese, a pista de 1200 m usada nos experimentos permitiu avaliar o impacto do CET enquanto o veículo se locomovia em direção ao pedestre, em cenários com LoS e NLoS. Isto é importante para alguns cenários reais. Por exemplo, em uma via sinalizada (Figura 3.1), pedestres podem realizar a travessia na faixa mesmo quando não há autorização semafórica. Tal situação coloca em risco pedestres e motoristas, já que obstáculos, como um ônibus co-

letando passageiros, podem inibir a propagação do sinal e impedir o estabelecimento da conexão antes que o pedestre inicie a travessia. Isso é agravado pelo bloqueio do campo visual do pedestre, que não visualiza os veículos ao iniciar a travessia.

Figura 3.1: Exemplo de via sinalizada (Campus UFRJ). Fonte: Google Maps.

3.2.1 *Beacon-stuffing* para Comunicação Sem Conexão

Os experimentos de Camps-Mur *et al.* mostraram que, em alguns casos, o tempo para estabelecimento da conexão (CET) no Wi-Fi Direct pode chegar a 15 s [2, 3]. O CET, inclusive, pode ser considerado uma das principais desvantagens do Wi-Fi Direct se considerado seu uso no ambiente veicular [2]. Dependendo da velocidade empregada, o tempo de contato entre os nós pode ser curto, e o uso desta tecnologia como uma opção, em alguns cenários, ao IEEE 802.11p pode ser proibitivo. Deste modo, após investigar a equivalência dos resultados dos testes práticos feito com Wi-Fi Direct com as simulações no INET, um método simples de transmissão oportunística de mensagens de segurança baseado no *beacon-stuffing* foi avaliado. Por meio desta técnica, é possível transmitir dados de forma oportunística, sem estabelecer uma conexão no Wi-Fi Direct, minimizando o impacto do CET. Inclusive, nenhuma interação por parte do usuário é necessária. A aplicação do *beacon-stuffing* consiste em inserir, no nome do dispositivo Wi-Fi Direct, dados que compõem a mensagem de segurança, como posição e velocidade. Como o SSID de uma rede Wi-Fi, propagado pelo ponto de acesso via disseminação de *beacons*, o nome do

dispositivo Wi-Fi Direct é propagado de forma semelhante. Cabe ressaltar que, diferente da transmissão *ad-hoc* que também permite a transmissão de mensagens em *broadcast* sem conexão, o uso do *beacon-stuffing* no Android não requer privilégios de *root* [38]. A seguir, será apresentada uma descrição dos trabalhos que serviram de inspiração para a avaliação deste método.

Em [65], Chandra *et al.* propõem o que parece ser a ideia original do *beacon-stuffing*. Visando a comunicação imediata entre APs e clientes sem que seja necessário estar previamente associado à rede Wi-Fi, a técnica consiste em sobrescrever campos de quadros de controle (como *beacons* e *probe responses*) por dados de interesse de uma aplicação. Na proposta, os dados são embarcados como uma *string* de bytes, contendo: (1) o ID da mensagem; (2) o número do fragmento da mensagem; (3) uma *flag* que indica se há novos fragmentos; e (4) o *payload* da mensagem. Nos *beacons/probe responses*, os dados podem ser embarcados sobrescrevendo os seguintes campos: (1) SSID; (2) BSSID (BSS *IDentifier*); e (3) IE (*Information Element*). Segundo os autores, ao contrário da modificação dos 32 bytes do SSID, a modificação dos 6 bytes do BSSID – campo que identifica o AP usando seu endereço MAC – e dos 253 bytes do IE – campo para uso específico do fabricante do AP – requer acesso ao código-fonte do AP. Além disso, a embarcação de dados no IE requer, inclusive, a modificação do *driver* do dispositivo do cliente.

Em [66], Mao *et al.* propõem o PASA, que transmite dados sem conexão sobrescrevendo os nomes dos dispositivos Bluetooth e Wi-Fi Direct. Apesar de implementado em ambas as tecnologias, a descrição e os resultados em [66] se referem apenas ao Bluetooth. No PASA, dois estados são definidos para *smartphones*: (1) *Scanning*, referente ao período de *Discovery* – que, segundo os autores, no Bluetooth pode durar 12 s –, onde os dados são recebidos oportunisticamente; e (2) *Idle*, período em que o *Discovery* não é executado. Mensagens e *smartphones* possuem um ID único, baseados no endereço MAC. Por exemplo, enquanto aa:bb:cc:dd:ee:ff refere-se ao ID do *smartphone* x, aa:bb:cc:dd:ee:ff.12 refere-se à sua mensagem de ID 12. O índice de IDs de mensagens é cíclico, indo até 255 antes de voltar a 0. Mensagens inseridas nos 248 bytes do nome Bluetooth são compostas por cabeçalho e *payload*. O cabeçalho inclui (1) o intervalo (em s) entre os *scans*, (2) a faixa de índices das mensagens ativas e (3) o estado de recepção das mensagens em um dispositivo, definida como uma tabela *hash* cuja chave é o ID dos *smartphones* vizinhos e um *bitmap* associado. Já o *payload* carrega o conteúdo que será disseminado. O nome do dispositivo pode ser modificado periodicamente para transmitir várias mensagens, que podem ser fragmentadas. Um modelo analítico foi usado para definir um intervalo ótimo de atualização das mensagens no nome do dispositivo, visando minimizar o tempo para recepção das mensagens.

Em [69], Turkes *et al.* propõem o Cocoon, um *middleware* para redes móveis oportunísticas. O Cocoon consiste de dois componentes principais: (1) gerenciamento de conectividade, e (2) gerenciamento de aplicações. Pelo primeiro, Cocoon é capaz de trocar

dados usando ou (1) o modelo OBN (*Opportunistic Beacon Networking*), onde dados são trocados sem conexão por meio do nome do dispositivo Bluetooth, UUID (*Universally Unique Identifier*) do BLE ou do SSID do Wi-Fi Hotspot, ou (2) o modelo OAN (*Opportunistic Association Networking*), onde dados são trocados após conexão. No OBN, um dispositivo, ou OB (*Opportunistic Beacon*) no modo *beacon* anuncia dados de forma oportunística, enquanto outro dispositivo, BO (*Beacon Observer*), no modo *scan*, recebe tais dados ao executar um *scan* na rede. No OBN, via ativação/desativação da interface de rede, um dispositivo alterna entre os estados OB e BO, o que permite o envio e recepção de dados. No OBN e OAN, *beacons* são compostos por campos contendo dados de cabeçalho (p. ex. tipo da aplicação), roteamento (p. ex. TTL da mensagem), QoS (p. ex. valor que mostra o quão estáveis são os contatos ao longo do tempo), e *payload*. Dado que o espaço para uso no nome do dispositivo Bluetooth, UUID do BLE ou SSID do Wi-Fi é limitado, codificações como Base94 e bitwise são usadas para otimização do espaço.

Em [67], Dhondge *et al.* propõem o WiFiHonk, um sistema que usa *smartphones* para alertar veículos e pedestres sobre o risco de colisões. Por meio do *beacon-stuffing*, alertas são inseridos no SSID de *beacons* enviados a cada 100 ms pelo Wi-Fi Hotspot do Android, e recebidos durante o *scan*. Os autores mencionam que este mesmo mecanismo pode ser usado no Wi-Fi Direct. WiFiHonk consiste de quatro módulos: (1) *beacon-stuffing*; (2) estimativa de colisão; (3) tabela de colisão; e (4) alerta. Em resumo, estes módulos (1) coletam a posição, velocidade e direção de viagem de GPS, acelerômetro e giroscópio, respectivamente, e embarcam estes dados nos 32 bytes do SSID como um WHIP (*WiFiHonk Information Packet*); (2) calculam os vetores de direção dos veículos com base nos dados extraídos do SSID e comparam com o vetor de direção do pedestre, de forma a analisar se ambos irão convergir em um ponto em comum e ao mesmo tempo. Se sim, o tempo estimado para colisão é calculado; (3) armazenam o tempo estimado em uma tabela junto ao ID do veículo envolvido na possível colisão; e (4) alertam o pedestre sempre que o tempo estimado para colisão atinge um ponto crítico. Por meio de simulações, os autores avaliaram o WiFiHonk em comparação ao Wi-Fi Direct em diferentes velocidades, distâncias e configurações de mobilidade. Segundo a análise dos resultados feita pelos autores, enquanto o WiFiHonk conseguiu entregar ao menos um WHIP até 112 km/h, no Wi-Fi Direct isto só foi possível até 24 km/h devido ao CET. Quanto ao risco de colisão, o WiFiHonk foi capaz de diminuir a probabilidade de colisão, já que enviou alertas ao pedestre mesmo em altas velocidades. Por outro lado, este risco foi de quase 100% no Wi-Fi Direct em velocidades >16 km/h. Cabe ressaltar que os IDs dos veículos armazenados na tabela de colisões são baseados no endereço MAC extraído do IE do WHIP emitido pelo veículo em questão. Por manipular o IE, o método pode exigir privilégios de *root* em *smartphones* Android, o que tornaria a solução difícil de implantar no mundo real [68].

Apresentados os trabalhos que inspiraram o desenvolvimento desta tese, no próximo capítulo é feita uma descrição dos experimentos com o IEEE 802.11p.

Capítulo 4

Experimentos com o IEEE 802.11p

Este capítulo descreve a configuração dos experimentos de avaliação do IEEE 802.11p. Os experimentos reais foram realizados com OBUs e RSUs MK5, da fabricante australiana Cohda Wireless, além de simulações executadas no NS-3/PhySim e Veins/MiXiM. Nas seções a seguir, serão apresentados os cenários de avaliação, bem como os detalhes da configuração dos experimentos reais e a descrição dos parâmetros usados nas simulações.

4.1 Cenários de Avaliação

De forma a avaliar o desempenho do IEEE 802.11p por meio de experimentos reais e simulações, três cenários, envolvendo a transmissão periódica de BSMs, foram definidos com base nos cenários propostos por Sassi *et al.* [52]. A Figura 4.1 apresenta os três cenários de avaliação.

- **Cenário 1 – Impacto do Aumento da Distância:** permite avaliar o impacto do aumento da distância entre os nós (perda de percurso), devido ao desvanecimento em larga-escala (*large-scale fading*). Além disso, permite avaliar o alcance da comunicação (em função do raio) do IEEE 802.11p. Por exemplo, se os requisitos de alcance de aplicações de segurança baseadas em um salto são suportados. Também é útil para mensurar o custo de implementação de RSUs. Neste cenário, um veículo parado portando uma OBU se comunica com uma RSU instalada na extremidade de uma via com 1000 m de extensão. Com a via dividida em dez trechos de 100 m, o veículo inicia suas transmissões a 100 m de distância da RSU e, após a transmissão de 500 BSMs, o mesmo é reposicionando para cada um dos trechos de 100 m seguintes, repetindo o procedimento até concluir no trecho a 1.000 m da RSU (alcance máximo teórico do IEEE 802.11p). Como Huang *et al.* [123], neste cenário são avaliados o alcance máximo, a distância máxima na qual a RSU é capaz de receber BSMs da OBU, e o alcance efetivo da comunicação, a distância máxima na

qual a RSU pode receber, no mínimo, 80% das BSMs transmitidas pela OBU [126]. Ambos os alcances medidos são diferentes para cada modulação.

- **Cenário 2 – Impacto da Mobilidade Moderada:** permite avaliar o impacto da mobilidade moderada na comunicação, supostamente capaz de causar um desvanecimento de pequena-escala no canal sem-fio devido, por exemplo, ao Doppler *shift*. Neste cenário, um veículo portando uma OBU viaja a 20 km/h, 50 km/h e 80 km/h e se comunica com uma RSU instalada na extremidade da via. O veículo inicia sua trajetória a cerca de 1000 m da RSU, transmitindo continuamente BSMs para este dispositivo. Ao contrário da análise por trecho de 100 m feita no cenário anterior, neste cenário são contabilizadas todas as transmissões feitas pelo veículo durante seu percurso em direção à RSU, e os resultados são gerados a cada 25 m.

  Cenário 3 – Impacto da Mobilidade Intensa: similar ao cenário anterior, permite avaliar o impacto da mobilidade intensa na comunicação. Neste cenário, são utilizados dois veículos, ambos portando uma OBU, mas com apenas um deles atuando como transmissor. Iniciando suas trajetórias de cada extremidade da via (cerca de 1200 m) e ao mesmo tempo, os veículos seguem em direções opostas com a mesma velocidade, produzindo velocidades relativas de 40 km/h, 100 km/h e até 160 km/h. Novamente, a transmissão de BSMs é contínua, e a análise é feita a cada 25 m.

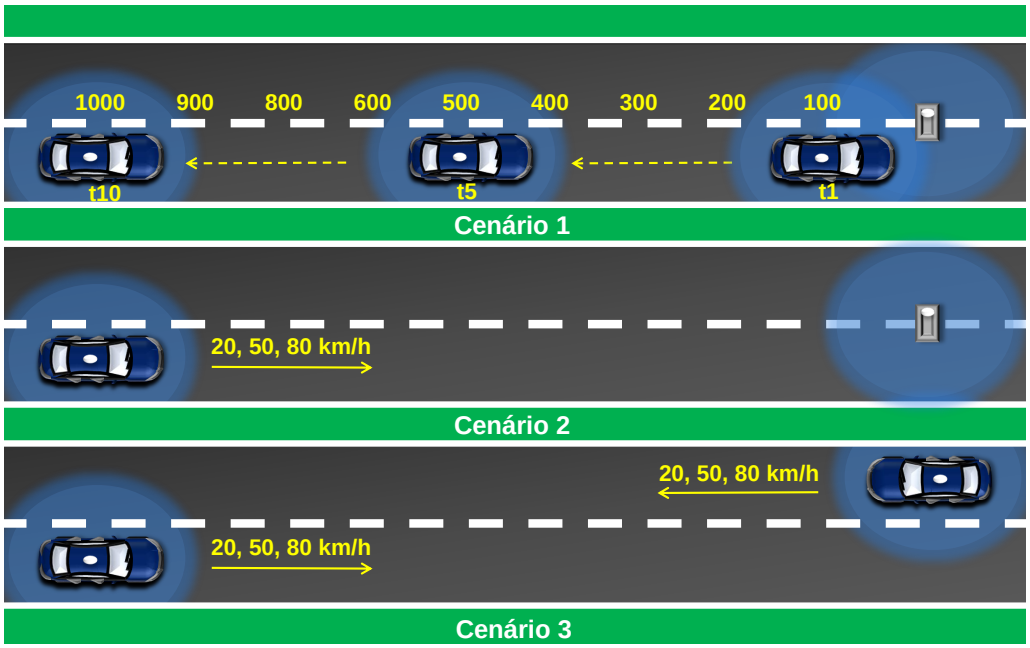

Figura 4.1: Cenários avaliados nos experimentos do IEEE 802.11p.

Nos três cenários, a análise da equivalência entre os experimentos reais e as simulações se apoia na análise da PDR e do PIR. Segundo Renda *et al.* [23], muitos dos trabalhos envolvendo a avaliação de desempenho de uma aplicação de *beaconing* periódico focam

apenas na análise da PDR, desconsiderando o PIR. Como Sassi *et al.* [52], para todos os cenários, o impacto de diferentes modulações/taxa de dados suportadas pelo IEEE 802.11p também foi avaliado. Das oito modulações suportadas, os experimentos foram realizados considerando apenas aquelas associadas às taxas de 3 Mbps (somente no Cenário 1), 6 Mbps, 12 Mbps, 18 Mbps e 24 Mbps. Duas razões justificam essa decisão:

- **Baixa variação entre modulações semelhantes:** como pode ser visto nos resultados obtidos por Sassi *et al.* [52], entre modulações associadas a taxas de dados com valores próximos, como 3 Mbps, 4.5 Mbps e 6 Mbps, os resultados da PDR tendem a ter pouca flutuação, o que justifica a escolha da experimentação com taxas de dados intermediárias.
- **Complexidade dos experimentos reais:** uma vez que o total de permutações dos cenários é equivalente ao produto cartesiano, no Cenário 1, das cinco modulações usadas nos dez trechos, e nos Cenários 2 e 3, das quatro modulações usadas nas três velocidades, um total de 74 permutações pode ser derivado. Se todas as modulações fossem analisadas, a realização dos experimentos reais seria ainda mais complexa e custosa.

Ainda com relação à complexidade dos experimentos reais, inicialmente, visando uma análise estatística dos dados, tentou-se executar dez rodadas para cada permutação. Entretanto, devido a alguns fatores, como ameaça de chuva e interrupção dos testes em trechos onde já não havia recepção de BSMs devido à longa distância entre os nós, o total de rodadas para cada permutação foi variável. No geral, tentou-se executar, pelo menos, cinco rodadas para cada permutação. Porém, em 13 das 74 permutações de cenário, o total de rodadas executado foi inferior a cinco. A Tabela 4.1 apresenta o total de rodadas de cada cenário, bem como outros números dos experimentos reais de avaliação do IEEE 802.11p. No Cenário 2, com algumas exceções, foram executadas dez rodadas para cada permutação de cenário. Por isso o total de rodadas deste cenário é muito superior ao do Cenário 3, onde no geral foram executadas cinco rodadas. Com base no total de rodadas, uma distância de cerca de 346 km foi percorrida pelos veículos, majoritariamente nos Cenários 2 e 3. No Cenário 2, durante uma rodada de experimentos, o veículo se locomove em direção à RSU e depois retorna à posição original para uma nova rodada (ida e volta na via de 1000 m). Enquanto isso, no Cenário 3 dois veículos são utilizados, percorrendo a via de 1200 m. Em ambos os casos, a distância percorrida pelos veículos é o resultado do total de rodadas vezes dois. Para as simulações, sempre foram executadas dez rodadas para cada permutação de cenário.

A Tabela 4.2 apresenta uma síntese dos cenários de avaliação. Em todos os cenários, há apenas um nó – sempre uma OBU – atuando como transmissor.

Tabela 4.1: Números dos experimentos da avaliação do IEEE 802.11p.

Variável	Cenário 1	Cenário 2	Cenário 3
Trechos (100 m)	10	-	-
Modulações	5	4	4
Velocidades	-	3	3
Total de Veículos	1	1	2
Extensão da via (km)	1	1	1,2
Total de permutações	50	12	12
Total de rodadas	259	103	58
Trajeto percorrido (km)	1	206 (ida e volta)	139,2 (pelos 2 veículos)

Tabela 4.2: Características dos cenários dos experimentos com IEEE 802.11p.

Cenário	Investigação	Transmissor	Receptor	Velocidade (km/h)	Taxa (Mbps)
1 (V2I)	Aumento da distância	OBU	RSU	Estático (0)	3-6-12-18-24
2 (V2I)	Mobilidade moderada	OBU	RSU	20-50-80	6-12-18-24
3 (V2V)	Mobilidade intensa	OBU[1]	OBU[2]	40-100-160	6-12-18-24

4.2 Configuração dos Experimentos Reais

Os experimentos reais foram feitos utilizando a 5ª geração de OBUs e RSUs da fabricante Cohda Wireless, modelo MK5. Segundo o documento de especificações dos dispositivos, fornecido pela Cohda Wireless, em resumo, ambos possuem a mesma interface de *hardware*, com dois rádios IEEE 802.11p, frequência de operação em 5,9 GHz, canais de 10 MHz e taxas que vão de 3 Mbps a 27 Mbps. Um receptor GNSS, modelo U-blox M8N, com precisão de até 2,5 m (nível de faixa) também é embarcado nos dispositivos, permitindo serviços de tempo e posicionamento. Os dispositivos contam com processador de 800 MHz, 1 GB de SDRAM, e 4 GB de memória *flash* eMMC, além de uma interface de saída de áudio que pode ser usada para integração com HMI. Ambos executam uma versão embarcada do sistema operacional Linux, *kernel* 3.10.17. Já o ganho de antena é diferente. Enquanto que a OBU usa antenas MobileMark SMW-303 com 5 dBi, na RSU são usadas antenas MobileMark ECO6-5500-WHT com 6 dBi. As antenas da RSU foram instaladas em uma base, com aproximadamente 1,8 m de altura. Já as antenas da OBU foram instaladas no teto do veículo, cuja altura mede em torno de 1,6 m. Os experimentos foram realizados com uma potência de transmissão de 32 dBm. As Figuras 4.2(a) e 4.2(b) apresentam os dispositivos utilizados nos experimentos.

A carga gerada na rede consiste na transmissão periódica e em *broadcast* de BSMs, feita pela OBU com destino (1) à RSU (Cenários 1 e 2), ou (2) a outra OBU (Cenário 3). O objetivo é avaliar o desempenho do IEEE 802.11p com base na operação de uma aplicação de *beaconing* periódico, denominada *bsm-shell*, fornecida pelo SDK (*Software Development Kit*) da Cohda Wireless. Cada BSM possui 51 bytes, e sua estrutura é mostrada na Figura 4.3. A identificação do significado dos campos hexadecimais que compõem a BSM

(a) OBU *Cohda Wireless*. (b) RSU *Cohda Wireless*.

Figura 4.2: Modelos de OBU e RSU utilizadas na avaliação do IEEE 802.11p.

foi feita por Pinto Neto *et al.*, em [4]. Entre outras informações, a BSM é composta por (1) um ID; (2) pelo *timestamp* da informação gerada; pelas coordenadas geográficas do nó, que nesta tese são a (3) latitude, (4) longitude e (5) altitude do veículo transmissor, obtidas do GNSS à taxa de 5 Hz; (6) a velocidade atual do veículo; (7) seu sentido de direção; e (8) sua dimensão. As BSMs são transmitidas através do CCH 178, a cada 50 ms. Para a coleta das métricas, o veículo transmissor (OBU) armazena o *timestamp* dos momentos em que as BSMs foram enviadas e suas próprias coordenadas geográficas. Já o receptor (RSU ou OBU) armazena suas próprias coordenadas geográficas e o *timestamp* associado, bem como o conteúdo das BSMs recebidas, contendo o *timestamp* da informação gerada e as coordenadas geográficas do veículo.

```
<DSRC_BasicSafetyMessage>
    <msgID><basicSafetyMessage/></msgID>
    <blob1>                (2)      (3)          (4)      (5)
     (1)7E 2E 7C 0E 21 FF FF 35 A4 E9 01 6B 49 D2 01 F0
        00 FF FF FF FF 45 DC 70 80 05 00 8C 00 1E 14 00
        AF 00 00 32 C1 A4 (6)  (7)
    </blob1>        (8)
    <safetyExt>
        <events>256</events>
    </safetyExt>
</DSRC_BasicSafetyMessage>
```

Figura 4.3: Estrutura de uma BSM coletada nos experimentos reais – Baseado em [4].

Os experimentos reais foram realizados em um aeroporto desativado, na cidade de Leopoldina – MG, Brasil. O local é composto por uma pista com cerca de 1200 m de extensão, e não possui interferências de redes celulares ou redes IEEE 802.11. Além disso, por se tratar de uma área predominantemente aberta, assume-se que o impacto das reflexões de sinal e propagação por múltiplos caminhos é mínimo. A Figura 4.4(a) apresenta

a visão aérea do local dos experimentos, enquanto as Figuras 4.4(b) e 4.4(c) mostram a OBU e RSU sendo utilizadas. Por fim, as Figuras 4.4(d), 4.4(e), 4.4(f), 4.4(g), e 4.4(h) apresentam a avaliação em progresso nos três cenários descritos anteriormente.

4.3 Configuração das Simulações no NS-3/PhySim

A versão do PhySim usada é a 1.2, construída com base no simulador NS-3 versão 13. A implementação e a configuração dos parâmetros das simulações foi feita usando o *framework* desenvolvido por Arbabi *et al.* [108] para o NS-3. Em [108], os autores implementaram um modelo de rodovia em linha reta bidirecional (classe `Highway`), que controla a mobilidade dos veículos (`Vehicle`) por meio dos modelos IDM e MOBIL (`Model` e `LaneChange`). Como mencionado na Seção 2.4, dada a simplicidade do cenário real desta tese, os recursos oferecidos pelos modelos não foram utilizados. Em [108], os veículos se comunicam via Wi-Fi. Esse modelo de transmissão foi substituído pela aplicação denominada `OnOffApplication`, retirada do arquivo `physim-1sender-only-rayleigh`, fornecido no diretório de exemplos do PhySim. Outros parâmetros de configuração também foram baseados na definição de `physim-1sender-only-rayleigh`, como aqueles relacionados à fragmentação de pacotes, uso de embaralhador (*scrambler*) fixo, níveis da potência de transmissão, estimador de canal, atraso de propagação, entre outros. Já o parâmetro que define o modelo de comunicação usado teve o seu valor modificado. No arquivo `physim-1sender-only-rayleigh`, este parâmetro vem configurado por padrão como IEEE 802.11a. Nas simulações, o mesmo teve seu valor modificado para IEEE 802.11p. Assume-se que esta modificação torna a simulação compatível com os parâmetros de camada física do IEEE 802.11p. Os parâmetros das simulações são configurados no arquivo `vanet-highway-test.cc`. Já a coleta das métricas, e definição de veículos e RSUs (`Obstacle`), são feitas em `controller.cc`. Por fim, a configuração dos modelos de propagação, entre outros, são feitas em `highway.cc`.

As características da via simulada, como largura e comprimento, foram baseadas no aeroporto utilizado nos experimentos reais. Do mesmo modo, foi configurada a altura dos dispositivos, com 1,5 m para o veículo, e 2,0 m para a RSU. Como nos experimentos reais, pacotes de 51 bytes são transmitidos a cada 50 ms, no CCH. Com base nos registros dos experimentos reais, foi definida uma potência de transmissão de 32 dBm. Já a configuração do ganho de antena depende do receptor. Se o receptor é uma RSU (Cenários 1 e 2), definiu-se um ganho de 6 dBi. Se o receptor é uma OBU (Cenário 3), o ganho é de 5 dBi. A posição do veículo na via é obtida por meio das coordenadas cartesianas x, y, z, fornecidas pelo modelo de mobilidade. Das oito modulações suportadas pelo IEEE 802.11p, apenas BPSK ½ (Cenário 1), QPSK ½, 16QAM ½, 16QAM ¾ e 64QAM ⅔ foram avaliadas. Para tais modulações, definiu-se um nível de sensibilidade do receptor de -98 dBm, -95 dBm, -90 dBm, -86 dBm e -82 dBm, respectivamente. Tais valores foram retirados das espe-

(a) Visão aérea do local. Fonte: Google Maps.

(b) OBU instalada no veículo.

(c) RSU instalada na via.

(d) Alcance máximo.

(e) Cenário V2I.

(f) Cenário V2I.

(g) Cenário V2V.

(h) Cenário V2V.

Figura 4.4: Cenário dos experimentos reais com o IEEE 802.11p.

cificações de desempenho do rádio da OBU/RSU, no documento fornecido pela Cohda Wireless, considerando um canal sem múltiplos caminhos, antenas de recepção simples, PSDU (*Packet Service Data Unit*) de 1000 octetos, PER $<10\%$ e temperatura de 25º. O nível do ruído de fundo é definido em -98 dBm, baseado no estudo de configuração de ruído para simulações de redes veiculares, realizado por Bloessl *et al.* [127].

Como forma de simular o desvanecimento em larga-escala, provocado pela atenuação do sinal de rádio gerada pelo aumento da distância entre os nós, o modelo de propagação `PhySimLogDistancePropagationLoss` foi configurado. Nas simulações, tal modelo foi capaz de reproduzir o comportamento da atenuação nos experimentos reais. No modelo, a perda de referência foi definida como 44.0 dB, baseado no RSSI dos experimentos reais do Cenário 1 à 0 m de distância, para todas as modulações. O parâmetro do expoente de perda, que define a taxa na qual a perda de percurso aumenta com a distância [128], foi definido empiricamente como 2.83. Segundo Rappaport *et al.* [128], este valor depende do ambiente de propagação específico. Por exemplo, no espaço-livre o expoente de perda é 2, enquanto que em um ambiente com obstruções o mesmo pode chegar a 6. A definição do valor do expoente de perda se deu na etapa de calibração das simulações, que consiste em aproximar o ambiente simulado do real com base nos resultados do alcance da comunicação, obtidos nos experimentos reais, usando a modulação BPSK ½ (3 Mbps) como referência. No NS-3/PhySim isto é feito ajustando, manualmente, o valor do expoente de perda do modelo `PhySimLogDistancePropagationLoss` até que seja possível obter, em todos os trechos de 100 m das simulações de avaliação do alcance à 3 Mbps (Cenário 1), uma PDR semelhante à obtida nos resultados de alcance, dos experimentos reais, também à 3 Mbps. A partir de então, avalia-se o quão próximos os resultados das simulações do NS-3/PhySim são dos experimentos reais, considerando também as demais taxas de dados suportadas pelo IEEE 802.11p. A mesma estratégia é usada para a etapa de calibração do Veins/MiXiM.

Para simular o desvanecimento em pequena-escala, que pode ser gerado devido à mobilidade dos nós, junto ao `PhySimLogDistance`, o modelo de propagação `PhySimRicianPropagationLoss` foi configurado. Tal modelo permite simular um desvanecimento Rician, onde ao menos uma réplica do sinal é recebida como resultado de uma propagação com LoS. Para definir o componente de LoS, o parâmetro `LineOfSightPower` do modelo foi definido como 7.0. Por padrão, este parâmetro possui valor 0, criando um desvanecimento Rayleigh. Já o parâmetro `MinimumRelativeSpeed` do modelo foi definido conforme o cenário de mobilidade. Se Cenário 2, a velocidade do veículo transmissor (20 km/h, 50 km/h, ou 80 km/h) é atribuída ao parâmetro. Se Cenário 3, esta velocidade é dobrada para obter a velocidade relativa. Isto foi usado para calcular o valor do parâmetro `LineOfSightDoppler`, que assume-se ser usado no cálculo do Doppler *shift*. O valor do parâmetro `LineOfSightPower`, além do cálculo do parâmetro `LineOfSightDoppler`, foram baseados nos valores configurados para o modelo `PhySimRicianPropagationLoss`,

usado junto a um modelo de propagação com LoS, em [129]. Cabe ressaltar, porém, que a forma de calcular o parâmetro `LineOfSightDoppler` foi modificada. Segundo Li *et al.* [91], o Doppler *shift* pode ser calculado como $v * f_c/c$, onde v é a velocidade relativa do objeto, f_c é a frequência central do sinal transmitido e c é a velocidade da onda eletromagnética. Assim, com base na equação de Li *et al.* [91] para cálculo do Doppler *shift*, nesta tese o parâmetro `LineOfSightDoppler` é calculado como $(nodeSpeed * 5.9e9)/(0.3e9)$. A Tabela 4.3 sintetiza os valores configurados nos parâmetros de simulação do NS-3/PhySim.

Tabela 4.3: Parâmetros das simulações do NS-3/PhySim.

Modelo	**Parâmetro**	**Valor**
PhySimWifiPhy	TxPowerEnd (dBm)	-32.0
	TxPowerStart (dBm)	-32.0
	TxGain (dBi)	5.0 (OBU)
	RxGain (dBi)	5.0 (OBU), 6.0 (RSU)
	CcaModelThreshold (dBm)	-65.0
	EnergyDetectionThreshold (dBm)	-98.0, -95.0, -90.0, -86.0, -82.0
PhySimInterferenceHelper	NoiseFloor (dBm)	-98.0
PhySimLogDistance	Exponent	2.83
	ReferenceDistance (m)	1
	ReferenceLoss (dB)	44.0
PhySimRician	MinimumRelativeSpeed (m/s)	5.55, 13.88, 22.22
	LineOfSightPower	7.0
	LineOfSightDoppler (Hz)	$(nodeSpeed * 5.9e9)/(0.3e9)$
WifiHelper	SetStandard	WIFI_PHY_STANDARD_80211p_CCH

4.4 Configuração das Simulações no Veins/MiXiM

Como mencionado na Seção 2.4.2, o Veins atua como um *gateway* entre o OMNeT++ e o SUMO. Foram usadas as versões do Veins 4.7.1, OMNeT 5.3, e SUMO 0.30.0. A geração da rota dos veículos se deu a partir da configuração de um *trace* de mobilidade no SUMO. Como mencionando na Seção 2.4, tal qual no NS-3/PhySim, muitos dos recursos de mobilidade fornecidos pelo SUMO não foram utilizados nas simulações do Veins/MiXiM, já que o objetivo era refletir as simples condições de mobilidade do cenário real. Novamente, a via simulada é baseada no aeroporto usado nos experimentos reais, e foi gerada usando as ferramentas NETEDIT e NETCONVERT, do SUMO. Como no NS-3/PhySim, no Veins/MiXiM a altura dos dispositivos é definida como 1,5 m para o veículo e 2,0 m para a RSU. Como nos experimentos reais, no Veins/MiXiM as BSMs de 51 bytes são transmitidas a cada 50 ms, no CCH. A implementação da transmissão e recepção de BSMs pela OBU foi baseada nas rotinas de transmissão/recepção definidas no arquivo `TraCIDemo11p`, disponível no diretório de aplicações do Veins. Também foram usados os arquivos `TraCIDemoRSU11p`, para tratar as recepções na RSU, e `BaseWaveAppLayer`, para coleta de métricas. A configuração dos parâmetros usados nas simulações foi baseada na configuração padrão do arquivo `omnetpp.ini`, disponível no diretório de exemplos do

Veins. Neste arquivo, parâmetros desnecessários, como um modelo de obstáculos, foram comentados ou tiveram seus valores modificados para representar os cenários de avaliação. A seguir serão descritos os parâmetros cujos valores foram modificados em algum nível.

Conforme feito no NS-3/PhySim, no Veins/MiXiM foram definidos os mesmos valores para a potência de transmissão, sensibilidade no receptor e ruído de fundo. De igual modo, a posição do veículo é obtida via coordenadas x, y, z do modelo de mobilidade, e o ganho de antena é definido conforme o receptor. Se RSU (Cenários 1 e 2), o ganho de antena é de 6 dBi. Se OBU (Cenário 3), 5 dBi. Entretanto, no Veins/MiXiM a antena configurada para os nós é baseada no tipo `SampledAntenna1D`, ID `monopole`, que define amostras de ganho de acordo com o ângulo da antena. Segundo o *website* do Veins, este é o único tipo implementado até o momento[1]. Baseado no exemplo de configuração disponível no *website* do Veins, foram definidas amostras de ganhos de 5 dBi e 6 dBi, para a frente, lado direito, traseira, e lado esquerdo de veículo (OBU) e RSU, respectivamente. Porém, sem considerar ganho ou rotação (em graus) aleatórios da antena. Por fim, a distância máxima de interferência é proporcional ao comprimento da via simulada. Demais parâmetros seguem os valores definidos por padrão no arquivo `omnetpp.ini`.

O desvanecimento em larga-escala foi gerado pelo modelo `SimplePathLossModel`. Como o `PhySimLogDistancePropagationLoss`, este modelo foi capaz de reproduzir o comportamento da atenuação do sinal de rádio conforme a distância entre os nós crescia, repetindo o padrão dos experimentos reais. Como no NS-3/PhySim, o coeficiente de perda foi definido empiricamente como 3,005. Novamente, a definição deste valor ocorreu na etapa de calibração das simulações, baseado nos resultados do alcance da comunicação, obtidos nos experimentos reais, usando a modulação BPSK ½. Já o valor do parâmetro que define a frequência da portadora foi mantido como 5,890e9, valor já definido no arquivo de configuração `config.xml`, disponível no diretório de exemplos do Veins. De acordo com nosso conhecimento, ao menos com relação aos modelos de propagação disponíveis no Veins/MiXiM 4.7.1, nenhum parecia ser adequado para aplicar o desvanecimento em pequena-escala que pode ser gerado devido à mobilidade dos nós em ambientes de propagação com LoS predominante. Neste sentido, por considerar o Doppler *shift*, para simular o desvanecimento em pequena-escala, o modelo de propagação `JakesFading`, do MiXiM, foi configurado junto ao `SimplePathLossModel`. Entretanto, por simular um desvanecimento Rayleigh, este modelo é mais adequado para ambientes onde não há propagação com LoS predominante. Desta forma, visando aproximar o modelo de simulação do ambiente onde foram realizados os experimentos reais (predominantemente aberto e com LoS), o valor do parâmetro `fadingPaths` do modelo, que nesta tese é assumido como o número de caminhos percorridos pelas diferentes réplicas do sinal transmitido, foi al-

[1] https://veins.car2x.org/documentation/modules/#antennas

terado de 3, que é o valor definido no exemplo de configuração do modelo[2], para 1. Os demais parâmetros do modelo tiveram seus valores padrão mantidos. A Tabela 4.4 resume os valores configurados nos parâmetros de simulação do Veins/MiXiM.

Tabela 4.4: Parâmetros das simulações do Veins/MiXiM.

Modelo	**Parâmetro**	**Valor**
Mac1609_4	txPower (mW)	1584mW (32 dBm)
ConnectionManager	maxInterfDist (m)	1260
Phy80211p	sensitivity (dBm)	-98.0, -95.0, -90.0, -86.0, -82.0
	thermalNoise (dBm)	-98.0
SampledAntenna1D	ID	Monopole
	samples (dBi)	5.0, 5.0, 5.0, 5.0 (OBU)
	samples (dBi)	6.0, 6.0, 6.0, 6.0 (RSU)
SimplePathlossModel	alpha	3.005
	carrierFrequency (Hz)	5.890e9
JakesFading	carrierFrequency (Hz)	5.890e9
	fadingPaths	1
	delayRMS (s)	0.0001
	interval (s)	0.001

No capítulo atual, foram mostrados os detalhes dos experimentos envolvendo o padrão IEEE 802.11p. No capítulo seguinte, serão apresentados os resultados obtidos na avaliação do referido padrão.

[2]http://mixim.sourceforge.net/doc-2.1/MiXiM/doc/doxy/a00109.html#_details

Capítulo 5

Resultados dos Experimentos com o IEEE 802.11p

Este capítulo apresenta os resultados da avaliação do IEEE 802.11p, por meio de testes práticos com OBUs e RSUs comerciais e simulações no NS3/PhySim e Veins/MiXiM. Através da comparação dos resultados de ambos os ambientes, é possível avaliar a capacidade dos simuladores em reproduzir o comportamento obtido por uma aplicação baseada na transmissão de BSMs. A mediana dos resultados é exposta em gráficos com barras de erro verticais que mostram o desvio absoluto da mediana. Optou-se por usar a mediana, e não a média, por esta ser menos sensível a *outliers*. Uma exceção ocorre nos experimentos reais que analisam o PIR no Cenário 1: as amostras passaram por um processo de remoção de *outliers*, onde quaisquer valores cujas diferenças em relação à média foram maiores que dois desvios-padrões foram removidos. Como descrito na Seção 4.1, nos testes práticos, o total de rodadas para cada permutação foi variável. Tentou-se executar, pelo menos, cinco rodadas para cada permutação. Para o cálculo da mediana da PDR e do PIR, foram considerados os casos onde foi possível receber BSMs em pelo menos metade das rodadas, se o total de rodadas é par, e metade mais um, se o total é ímpar. Por exemplo, nos casos onde o total de rodadas foi quatro, as métricas foram calculadas se houve recepção em pelo menos duas rodadas. Nos casos onde o total foi nove, as métricas são calculadas se houve recepção em pelo menos cinco rodadas. As simulações foram executadas em um *laptop* Intel Core i7-7500U, de 2,7 GHz, e 16 GB de RAM. Como nas simulações sempre foram executadas dez rodadas, para cálculo das métricas são considerados os casos onde foi possível receber BSMs em pelo menos cinco das dez rodadas. Isto foi definido para associar o cálculo do PIR à PDR. No cálculo da mediana do PIR, é inviável calcular o PIR obtido em rodadas onde a PDR foi zero.

5.1 Impacto do Aumento da Distância

Esta seção tem como objetivo avaliar o impacto do aumento da distância entre os nós, além de investigar o alcance da comunicação do IEEE 802.11p em diferentes modulações. Como em Huang *et al.* [123], são avaliados o alcance máximo, distância máxima na qual a RSU é capaz de receber BSMs da OBU, e o alcance efetivo, distância na qual a RSU é capaz de receber, no mínimo, 80% das BSMs enviadas pela OBU [126]. Para este propósito, também é considerada a transmissão de BSMs à 3 Mbps, menor taxa de dados suportada no IEEE 802.11p, por supostamente permitir que as BSMs se propaguem por uma distância maior. Como mencionado nas Seções 4.3 e 4.4, os resultados dos experimentos reais que têm como objetivo avaliar o alcance obtido à 3 Mbps são usados na etapa de calibração das simulações.

A Figura 5.1 mostra a PDR e o PIR obtidos, nos experimentos reais e simulações, conforme a distância entre OBU e RSU aumenta. Como apontado por Sassi *et al.* [52], dado que a potência de transmissão é fixa, à medida que aumenta a distância entre os nós piora a qualidade do sinal recebido. Como observado por Sassi *et al.*, é notável a degradação da PDR à medida que a distância aumenta. Nos experimentos reais, o alcance máximo teórico de 1000 m do IEEE 802.11p é obtido apenas à 3 Mbps. Inclusive, a esta distância e usando esta taxa de dados, a RSU conseguiu receber mais de 80% das BSMs enviadas pela OBU. Este resultado demonstra que, apesar do aumento da taxa de perda conforme a distância entre os nós aumenta, ainda é possível obter um alcance efetivo à 1000 m de distância usando a menor taxa suportada pelo IEEE 802.11p. Tal resultado também foi observado por Sassi *et al.* [52], onde o alcance máximo também foi obtido à 4,5 Mbps. Como em [52], quanto menor é a taxa de dados, maior é o alcance. Conforme Sassi *et al.*, este resultado sugere o uso de baixas taxas ao visar comunicações de longo alcance. Por outro lado, o uso de taxas mais altas leva a uma piora da qualidade da comunicação. Como em [52], quanto maior é a taxa de dados, menor é a PDR. Segundo Sassi *et al.* [52], o impacto de altas taxas na PDR, como 18 Mbps e 24 Mbps, sugere que estas devem ser usadas, principalmente, se os nós estiverem geograficamente próximos. Por exemplo, em tais situações, um algoritmo de adaptação da taxa poderia escolher uma taxa mais alta, maximizando a vazão. Segundo Anwar *et al.* [28], usando modulações de mais alta ordem, menos símbolos OFDM são necessários para transmitir os dados, levando a uma menor latência fim-a-fim, o que poderia ser de grande importância para aplicações de segurança. Nesta tese, é possível obter um alcance efetivo, com PDR $\geq$80%, até 600 m, considerando as transmissões à 18 Mbps e 24 Mbps. Entretanto, é importante ressaltar que, à 18 Mbps, foi possível obter uma PDR $>$70% em 700 m e 800 m. Considerando a taxa de 12 Mbps, o alcance efetivo foi de 800 m. Já com relação às transmissões à 6 Mbps, é possível obter uma PDR $\geq$80% até 900 m. Apesar de ainda ser possível obter um alcance máximo de 1000 m à 6 Mbps, a PDR de $\approx$20% pode não permitir o pleno funcionamento de aplicações de

segurança a esta distância e usando esta taxa de dados. No geral, o comportamento obtido nos experimentos reais desta tese também foi observado nos resultados de Sassi *et al.* [52].

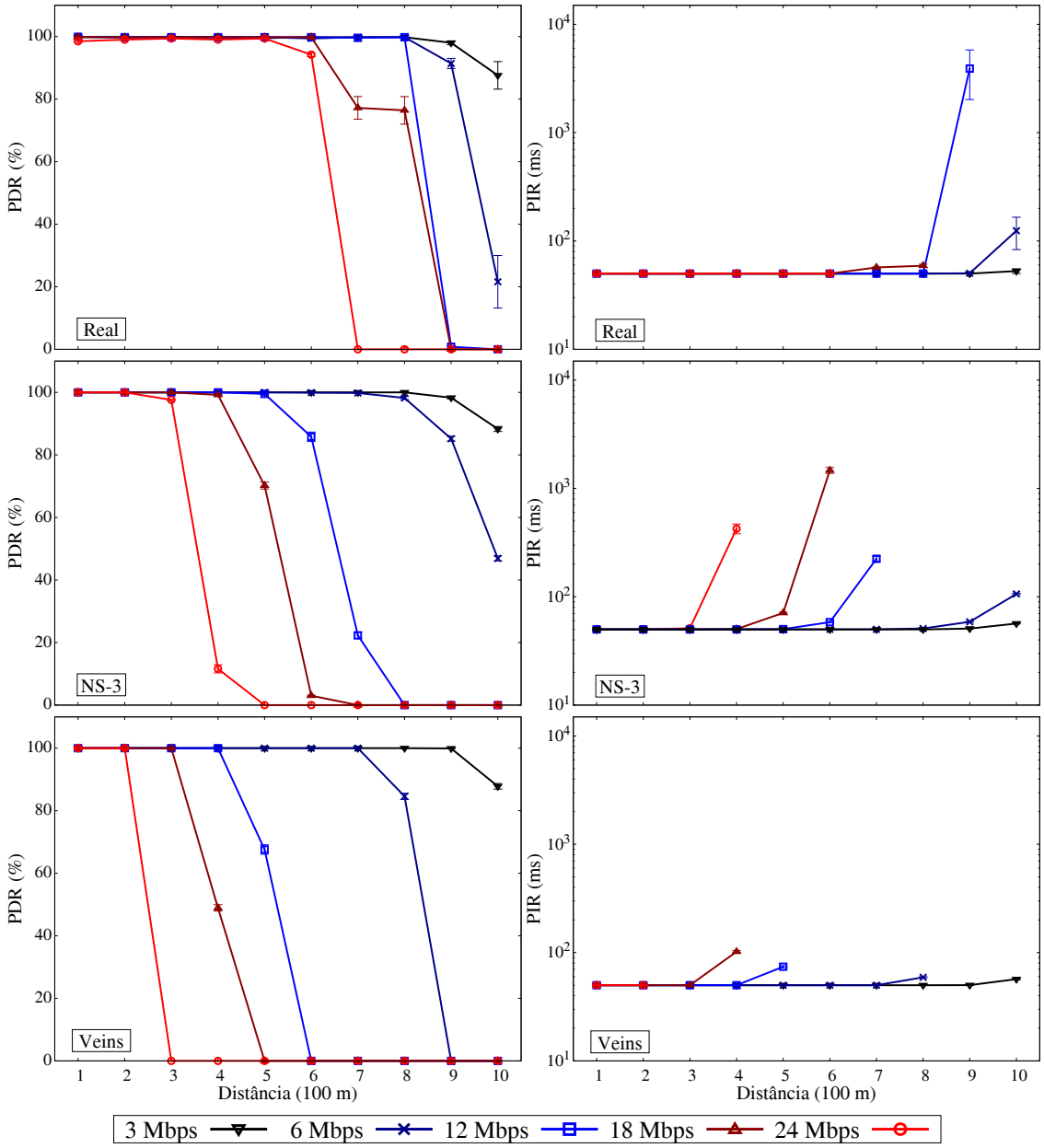

Figura 5.1: Alcance da comunicação com relação à PDR e ao PIR.

Antes de executar as simulações, foi necessário calibrar o ambiente de simulação de forma a aproximá-lo do ambiente real. Para os simuladores NS-3/PhySim e Veins/MiXiM, a etapa de calibração consistiu em ajustar o expoente/coeficiente de perda dos modelos de propagação `PhySimLogDistancePropagationLoss` e `SimplePathLossModel` baseado nos resultados reais de alcance, obtidos à 3 Mbps. Como é possível observar, nas simulações do NS-3/PhySim e Veins/MiXiM, foi possível obter uma PDR muito próxima à obtida nos experimentos reais à 3 Mbps, com 100% até 800 m, ≈100% em 900 m, e ≈87% em 1000 m. No geral, os simuladores são capazes de reproduzir o comportamento obtido nos

experimentos reais. Por exemplo, com relação à redução da PDR com o aumento da distância entre OBU e RSU e ao impacto na comunicação causado pelo uso de taxas de dados mais altas. Entretanto, em termos de valores absolutos, os resultados do NS-3/PhySim são ligeiramente mais próximos aos obtidos nos experimentos reais. Por exemplo, à 6 Mbps, o alcance efetivo é ≈900 m, conforme fora obtido nos experimentos reais. Esta é a única equivalência absoluta entre os ambientes real e simulado no Cenário 1. Enquanto isso, no Veins/MiXiM, o alcance efetivo à 6 Mbps se dá em 800 m. Já com relação aos resultados obtidos ao usar taxas de dados mais altas (18 Mbps e 24 Mbps), ambos os simuladores produzem valores subestimados. O alcance obtido nos experimentos reais é superior àquele obtido nas simulações. Apesar disso, os resultados do NS-3/PhySim são mais próximos aos experimentos reais em termos de valor, com alcance efetivo de 300 m, à 24 Mbps, e 400 m, à 18 Mbps. Já no Veins/MiXiM, o alcance é menor: 200 m e 300 m para as mesmas taxas de dados.

Com relação ao PIR, é possível perceber, nos experimentos reais, um relacionamento entre o aumento da distância entre os nós e o aumento desta métrica. Isto acontece devido ao efeito de borda, que considera transmissões feitas no limite do alcance da comunicação. Nestas regiões, a PDR é muito baixa. Assim, quanto maior é o alcance da comunicação, pior tende a ser a qualidade do enlace na região correspondente ao limite do alcance, o que prejudica a PDR e, consequentemente, o PIR. Nestes casos, quanto menor é a taxa de entrega de pacotes, maior tende a ser o intervalo de tempo entre as recepções. Conforme cenário vislumbrado por Renda *et al.* [23], exceções podem ocorrer quando as recepções ocorrem em lote. Por isso a análise de correlação entre as métricas é importante, já que dependendo do padrão de recepção de pacotes, pode não ser possível estimar o PIR a partir da PDR. Por exemplo, como mencionado na Seção 3.1, a análise feita por Renda *et al.* [23] demonstrou que as métricas PDR e PIR são fracamente correlacionadas. Entretanto, em [23], Renda *et al.* consideraram apenas as transmissões de BSMs realizadas enquanto os veículos se encontravam relativamente próximos um do outro, com alcance variando entre 80 m e 160 m. Nesta tese, devido ao efeito de borda, em todos os cenários de avaliação PDR e PIR demonstraram estar, no geral, correlacionadas. Por exemplo, no presente cenário, com exceção das transmissões feitas à 24 Mbps nos experimentos reais e Veins/MiXiM, foi possível observar uma correlação negativa que variou de forte a muito forte com o aumento da distância. Os graus de correlação podem ser vistos na Tabela 5.1. Como em Renda *et al.* [23], o cálculo da correlação foi baseado no Coeficiente de Pearson. A correlação entre PDR e PIR gerada pelo efeito de borda foi corretamente reproduzida nas simulações do NS-3/PhySim e no Veins/MiXiM (Tabela 5.1), apesar das diferenças em termos de valores absolutos com os experimentos reais. Um comportamento comum pode ser observado nos experimentos reais e nas simulações do NS-3/PhySim. Em pelo menos um trecho de 100 m, a mediana do PIR foi $\geq$1 s: no NS-3/PhySim, no trecho de 600 m, nas transmissões feitas à 18 Mbps; e nos experimentos reais, em 900 m/12 Mbps.

Em [23], Renda *et al.* definem um PIR $\geq$1 s como um *blackout* de consciência situacional. Como destacado pelos autores, *blackouts* registrados em sequência oferecem riscos à segurança, uma vez que a falta de percepção por longos períodos pode levar à não-detecção de situações perigosas.

Tabela 5.1: Coeficiente de correlação (Cenário 1).

	3 Mbps	**6 Mbps**	**12 Mbps**	**18 Mbps**	**24 Mbps**
Testes Reais	-0,99044	-0,99475	-1	-0,99133	0,11449
NS-3/PhySim	-0,99990	-0,99249	-0,99080	-0,95693	-0,99974
Veins/MiXiM	-1	-1	-1	-1	NA

5.2 Impacto da Mobilidade Moderada

Esta seção tem como objetivo avaliar o impacto do emprego, pelo veículo, de velocidades moderadas na comunicação. Por exemplo, apesar de ser aceito na literatura que as modificações feitas na camada PHY do IEEE 802.11p em relação ao IEEE 802.11a tenham tornado o primeiro, entre outros, tolerante ao Doppler *shift* [91], entende-se que a avaliação de tal cenário ainda é importante devido ao senso comum de que a comunicação realizada em altas velocidades pode levar à perda de pacotes. Novamente, também são consideradas diferentes modulações/taxas de dados nos experimentos. Ao contrário da análise por trechos de 100 m, nesta análise o cálculo da PDR e do PIR é feito a cada 25 m, com base na transmissão contínua de BSMs realizada pelo veículo enquanto se locomove em direção à RSU. É importante ressaltar que, nos experimentos reais, a transmissão de BSMs só foi iniciada a partir do momento que o veículo atingiu a velocidade desejada (20 km/h, 50 km/h, ou 80 km/h). Isto sempre aconteceu antes do veículo estar à 1000 m da RSU. A Figura 5.2 apresenta a PDR e o PIR obtidos, nos experimentos reais e simulações, para as diferentes velocidades e taxas analisadas. Como demonstrado no cenário anterior, e tal qual ocorreu nos experimentos realizados por Sassi *et al.* [52], novamente é possível observar que o uso de taxas de dados mais altas leva a uma piora da qualidade da comunicação.

Entretanto, diferente dos resultados de Sassi *et al.* [52], um compromisso entre o aumento da velocidade do veículo e o aumento da taxa de perda não foi identificado nos experimentos reais desta tese. Em Sassi *et al.* [52], quanto maior foi a velocidade do veículo, maior foi a PLR. Segundo os autores, este resultado pode ser atribuído ao Doppler *shift*. Nos experimentos reais desta tese, é possível observar que, mesmo com o emprego da mobilidade moderada pelo veículo, a PDR é similar àquela observada no Cenário 1, onde o veículo permaneceu parado durante as transmissões. Em alguns casos, a PDR é, inclusive, superior no presente cenário. Por exemplo, em ambos os cenários, nas transmissões realizadas à 24 Mbps, é possível perceber que a PDR se manteve $\approx$100% até 500 m.

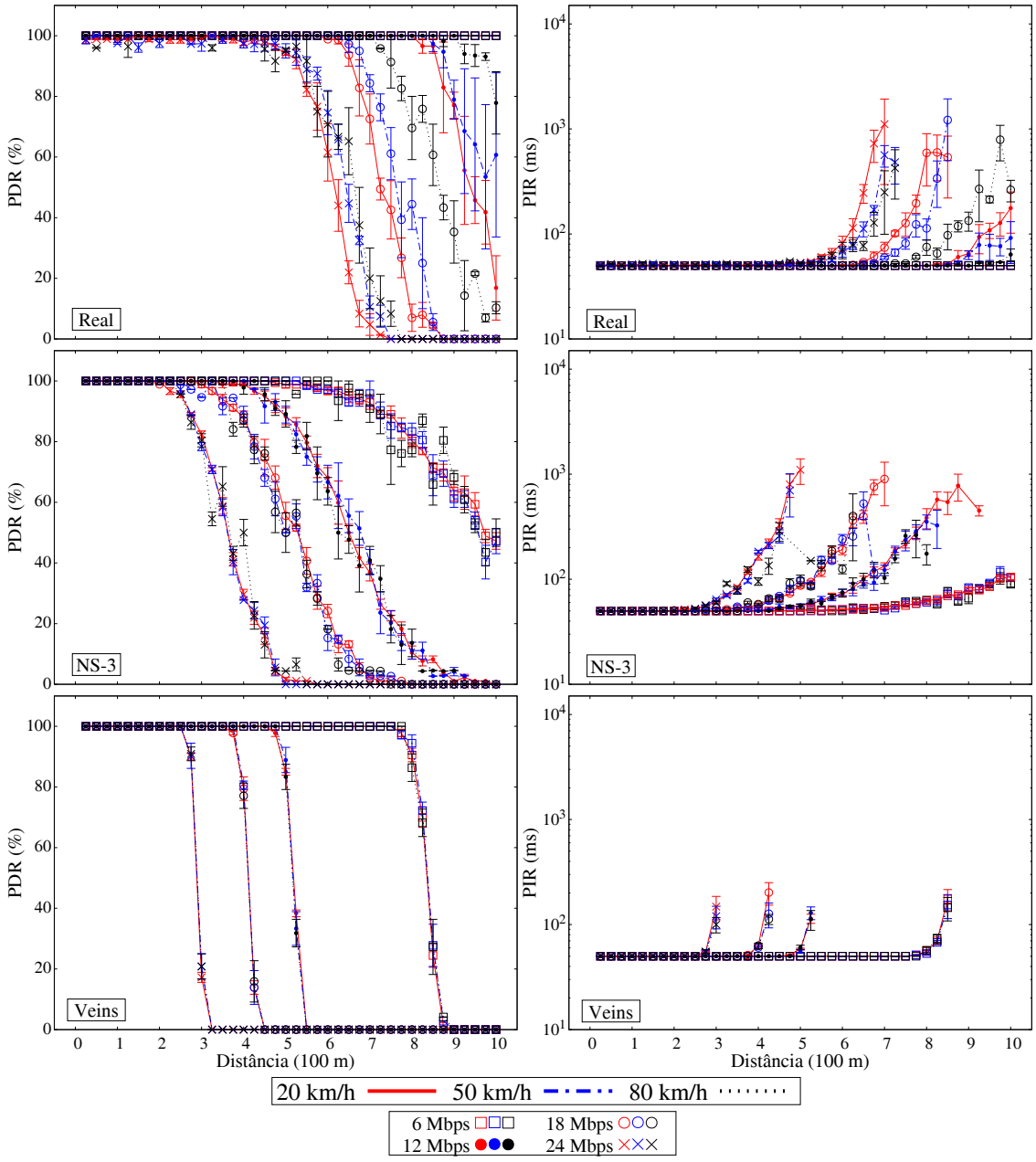

Figura 5.2: Impacto da mobilidade moderada com relação à PDR e ao PIR.

Por outro lado, nas transmissões realizadas à 6 Mbps, é possível observar que a PDR se manteve em 100% até 800 m no cenário anterior, enquanto que no cenário atual a PDR se manteve em 100% até 1000 m, durante todo o percurso do veículo, e independente da velocidade empregada (20 km/h, 50 km/h ou 80 km/h). Estes resultados indicam que a mobilidade moderada do veículo não foi capaz de impactar a comunicação em termos de perdas de pacotes, corroborando a proposição de que o IEEE 802.11p é tolerante ao Doppler *shift*. Além disso, com exceção dos resultados à 6 Mbps, é possível observar um compromisso entre o uso de velocidades menores e uma menor entrega de pacotes: quanto menor é a velocidade do veículo, menor é a PDR. Apesar de inesperado, entende-se que isto se deve ao fato de que, em baixas velocidades (como 20 km/h), o veículo passa mais

tempo fora da região onde é possível obter um alcance efetivo com a RSU. Nesta região, a atenuação do sinal de rádio é mais forte, e as transmissões realizadas no limite da comunicação são mais vulneráveis a falhas de recepção devido ao efeito da borda, reduzindo a PDR. Por outro lado, em velocidades mais altas (como 80 km/h), o veículo passa menos tempo nesta região, percorrendo rapidamente esta zona onde a comunicação é instável.

Os resultados das simulações do NS-3/PhySim e do Veins/MiXiM mostram que, novamente, os simuladores são capazes de reproduzir o padrão de redução da PDR conforme taxas mais altas são usadas. Além disso, os resultados obtidos pelos simuladores concordam com os obtidos nos experimentos reais quanto ao impacto negligenciável da mobilidade moderada na comunicação. Nas simulações do NS-3/PhySim, com exceção dos resultados obtidos à 6 Mbps, a PDR é similar àquela obtida no cenário sem mobilidade. À 6 Mbps, os resultados do NS-3/PhySim mostram uma pequena redução da PDR em comparação ao cenário anterior. Por outro lado, no Veins/MiXiM, a PDR obtida no cenário atual é muito superior àquela obtida no cenário sem mobilidade, especialmente nas transmissões feitas à 12 Mbps, 18 Mbps e 24 Mbps. Em termos de valores absolutos, como esperado, ambos os simuladores apresentam diferenças com relação aos experimentos reais. Entretanto, as curvas no NS3/PhySim, que representam o aumento da PDR conforme o veículo se aproxima da RSU, possuem uma forma mais próxima das curvas nos experimentos reais. Ambas apresentam um crescimento mais gradual que o observado no Veins/MiXiM. Inclusive, com um comportamento menos determinístico, o que pode ser devido ao PhySim atuar como um emissor/receptor real na codificação/decodificação do sinal. Em ambos os simuladores, diferente do que ocorre nos experimentos reais, não é possível identificar um compromisso entre o emprego de altas velocidades (como 80 km/h) e o aumento da probabilidade do pacote ser entregue com sucesso devido ao menor tempo que o veículo permanece na zona de comunicação instável. Como é possível observar na Figura 5.2, as barras de erro nas curvas demonstram a impossibilidade de determinar tal compromisso.

Quanto ao PIR, novamente é possível observar uma correlação negativa desta métrica com a PDR, que no geral varia de forte a muito forte à medida que aumenta a distância entre os nós nos experimentos reais. Mais uma vez, isto é devido ao efeito de borda. Com exceção das transmissões feitas à 6 Mbps, quanto menor foi a PDR, maior foi o PIR. Devido à PDR de 100% em todos os trechos de 25 m, não foi possível calcular a correlação entre PDR e PIR para 6 Mbps. A Tabela 5.2 apresenta os graus de correlação calculados. Em dois trechos de 25 m (18 Mbps/50 km/h/850 m e 24 Mbps/20 km/h/700 m), a mediana do PIR é $\geq$1 s. Como é possível observar, o PIR tende a crescer em transmissões realizadas em grandes distâncias e usando modulações de mais alta ordem. Apesar disso, a região onde as BSMs são importantes, próxima ao transmissor da BSM, não é impactada. Segundo Hartenstein *et al.* [19], *beacons* periódicos (ou BSMs, como nesta tese) são mensagens enviadas em *broadcast* em um salto, que devem possuir alta probabilidade de recepção próximo ao emissor, porém são menos importantes em distâncias maiores.

Como já mencionado, ainda segundo os autores, o VSC sugere que transmissões periódicas em um salto – necessárias em aplicações como FCW – tenham latência máxima e taxa/alcance mínimos de 100 ms, 10 Hz e 150 m, respectivamente. Com base nisso, pode-se afirmar que, mesmo com o aumento do PIR devido ao efeito de borda, na região onde as BSMs são importantes (≈200 m de distância entre transmissor e receptor), o mesmo é semelhante à taxa de geração de 50 ms das BSMs, independente da taxa de dados usada. É importante salientar, como mencionado na Seção 1.2, que os experimentos foram realizados em condições ideais de propagação, com transmissões feitas com LoS, sem interferência de outras redes, disputa pelo canal, colisões, entre outros, condições que dificilmente serão encontradas no mundo real. Tais condições podem levar a resultados otimistas.

Novamente, apesar das diferenças em termos de valores com os experimentos reais, a correlação negativa entre PDR e PIR é corretamente reproduzida no NS-3/PhySim e Veins/MiXiM, também variando entre forte e muito forte de acordo com o Coeficiente de Pearson (Tabela 5.2). Como nos experimentos reais, nas simulações do NS-3/PhySim, há um trecho onde a mediana do PIR é $\geq$1 s. Novamente, isto ocorreu a uma grande distância e usando uma taxa de dados mais alta (24 Mbps/20 km/h/500 m). Conforme esperado, devido aos resultados da PDR, as curvas que representam a redução do PIR conforme o veículo se aproxima da RSU possuem um decaimento mais gradual no NS-3/PhySim, com forma e comportamento mais próximos aos obtidos nos experimentos reais. Por fim, em ambos simuladores, a região onde as BSMs são importantes não é afetada. Nesta região, o PIR é semelhante à taxa de geração das BSMs, independente da taxa usada.

Tabela 5.2: Coeficiente de correlação (Cenário 2).

Testes Reais	**6 Mbps**	**12 Mbps**	**18 Mbps**	**24 Mbps**
20 km/h	NA	-0,97961	-0,89997	-0,83425
50 km/h	NA	-0,96585	-0,75199	-0,88450
80 km/h	NA	-0,99714	-0,76730	-0,87269
NS-3/PhySim	**6 Mbps**	**12 Mbps**	**18 Mbps**	**24 Mbps**
20 km/h	-0,98116	-0,84790	-0,80118	-0,77631
50 km/h	-0,97837	-0,90967	-0,76600	-0,76977
80 km/h	-0,97824	-0,90294	-0,81620	-0,85932
Veins/MiXiM	**6 Mbps**	**12 Mbps**	**18 Mbps**	**24 Mbps**
20 km/h	-0,97301	-0,99420	-0,98819	-0,99752
50 km/h	-0,97893	-0,99549	-0,99617	-0,99848
80 km/h	-0,98000	-0,99731	-0,99795	-0,99995

5.3 Impacto da Mobilidade Intensa

Por fim, esta seção tem como objetivo avaliar o impacto do emprego, pelo veículo, de velocidades intensas na comunicação. Mais uma vez, entende-se que é importante avaliar

tal cenário já que o senso comum indica que a comunicação feita em altas velocidades pode levar à perda de pacotes, devido por exemplo ao Doppler *shift*. Como nos demais cenários, também são consideradas diferentes modulações/taxas de dados nos experimentos. Assim como no cenário anterior, o cálculo da PDR e do PIR é feito a cada trecho 25 m, com base na transmissão contínua de BSMs feita pelo veículo transmissor conforme este se aproxima do veículo receptor, até o eventual cruzamento. Portanto, diferente do cenário anterior, no cenário atual são consideradas transmissões de BSMs feitas em altas velocidades relativas (40 km/h, 100 km/h e 160 km/h), alcançadas mediante o cruzamento dos dois veículos se locomovendo em direções opostas da via. Mais uma vez, a transmissão só foi iniciada após os veículos atingirem a velocidade desejada. A Figura 5.3 apresenta a PDR e o PIR obtidos, nos experimentos reais e simulações. Novamente, tal qual nos experimentos de Sassi *et al.* [52], observa-se que o uso de taxas mais altas leva a uma piora da comunicação.

Como é possível perceber, com exceção dos resultados à 6 Mbps, a PDR é ligeiramente mais baixa no cenário atual se comparada ao cenário anterior. Entretanto, entende-se que este resultado não é consequência do impacto da mobilidade intensa na comunicação. Por exemplo, não é possível distinguir os resultados da PDR enquanto o veículo se locomoveu a velocidades relativas de 40 km/h, 100 km/h ou 160 km/h. As barras de erro nas curvas demonstram a impossibilidade de atribuir que o impacto seja proveniente, por exemplo, do Doppler *shift*. Se fosse este o caso, a PDR deveria ser mais baixa em velocidades relativas mais altas. Assume-se que a ligeira redução da PDR em comparação ao cenário anterior seja devido ao menor ganho de antena do receptor. Como mencionado na Seção 4.2, no cenário atual o receptor é uma OBU, cujo ganho de antena é 5 dBi, enquanto que no cenário anterior o receptor é uma RSU, cujo ganho é 6 dBi. Outra diferença com relação ao cenário anterior é que, naquele cenário, o emprego de velocidades mais altas fez com que a PDR fosse mais alta em comparação com a PDR obtida ao empregar velocidades mais baixas. No cenário anterior, é possível perceber um compromisso entre usar velocidades mais altas e obter uma maior probabilidade de recepção do pacote. Já no cenário atual, as barras de erro nas curvas demonstram a impossibilidade de observar tal compromisso. Inclusive, é interessante notar o aumento das barras de erro em relação ao cenário anterior. Como a velocidade relativa é o dobro do cenário que avalia o impacto da velocidade moderada, o número de BSMs transmitidas é em torno da metade, diminuindo o tamanho do conjunto de dados. Mais uma vez, os resultados diferem dos resultados obtidos nos experimentos realizados por Sassi *et al.* [52] em condições de alta mobilidade. Nestas condições, os resultados de Sassi *et al.* [52] indicam um forte compromisso entre o aumento da velocidade do veículo e o aumento da PLR.

Já os resultados do NS-3/PhySim e Veins/MiXiM mostram que, mais uma vez, ambos os simuladores são capazes de reproduzir o comportamento da PDR com relação às diferentes taxas de dados. Novamente, as simulações concordam com os experimentos reais quanto ao impacto negligenciável da mobilidade intensa na comunicação. Entretanto,

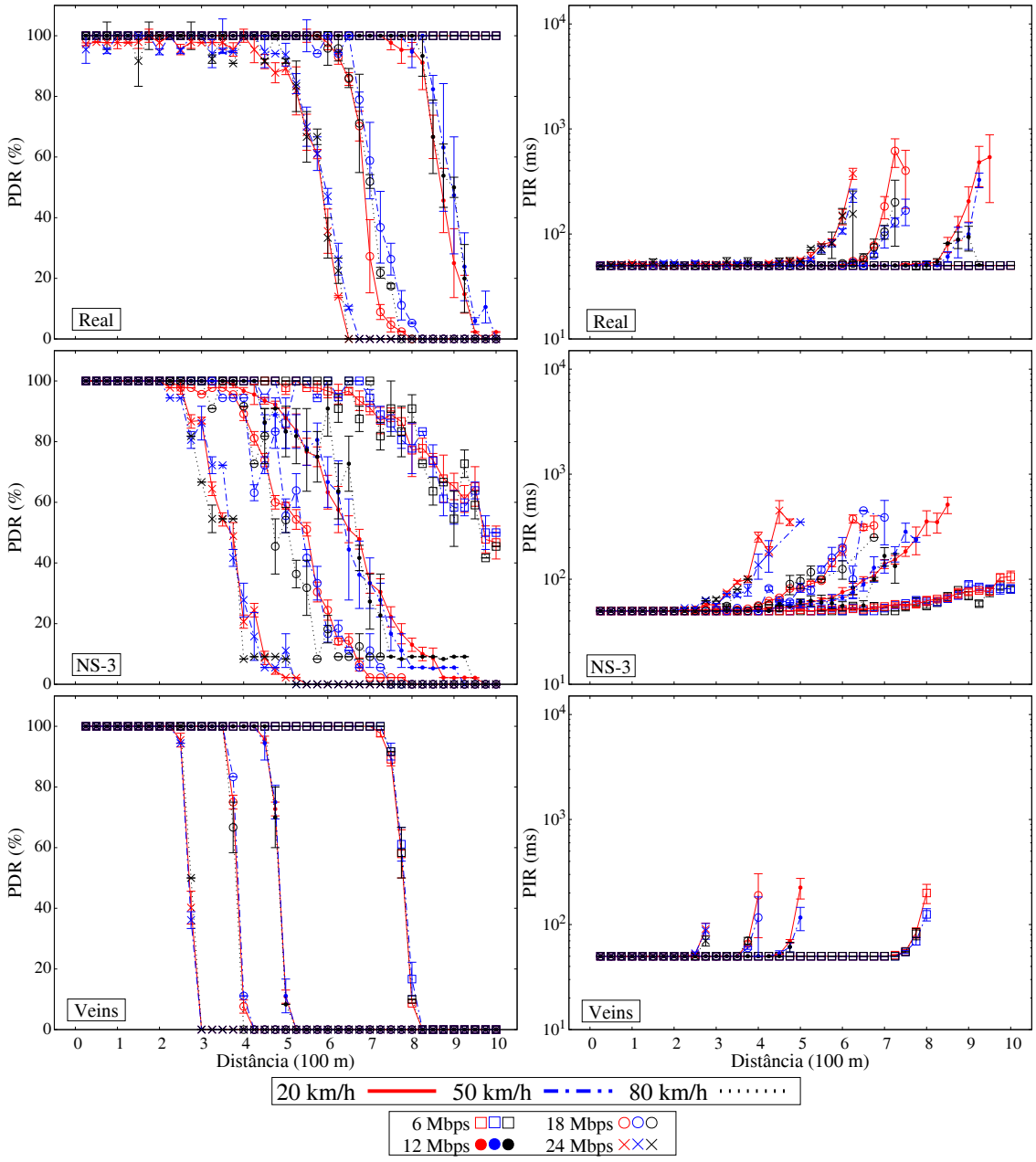

Figura 5.3: Impacto da mobilidade intensa com relação à PDR e ao PIR.

uma diferença pode ser observada, especialmente no NS3/PhySim. No cenário atual, os experimentos reais mostram que a PDR é inferior à PDR obtida no cenário anterior, com exceção das transmissões à 6 Mbps. Como mencionado, tal redução foi atribuída à diferença no ganho de antena entre OBU e RSU. Este comportamento não é reproduzido no NS3/PhySim. No NS-3/PhySim, os resultados são muito similares aos obtidos no cenário anterior, com as curvas reproduzindo o mesmo comportamento. A principal diferença está nas variações das amostras e, por consequência, nas barras de erro, o que é justificável dada a diminuição pela metade do número de BSMs transmitidas. Isto pode indicar uma imprecisão da modelagem do menor ganho da antena da OBU, em comparação com a RSU. Ao contrário do NS-3/PhySim, nas simulações do Veins/MiXiM os resultados indicam que a

diferença no ganho de antena do receptor é bem modelada, já que é possível perceber uma ligeira redução na PDR em comparação ao cenário anterior, independente da taxa usada, tal qual ocorre nos experimentos reais. Apesar das divergências esperadas em termos de valores, e com exceção dos resultados à 6 Mbps, novamente as curvas do NS-3/PhySim possuem um crescimento gradual, mais parecido com o que ocorre nos experimentos reais, inclusive em termos de comportamento. Como nos experimentos reais, nos simuladores não é possível identificar um compromisso entre o uso de altas velocidades relativas e o aumento da PDR.

Quanto ao PIR, nos experimentos reais é possível observar novamente uma correlação negativa desta métrica com a PDR, que no geral varia de forte a muito forte. Mais uma vez, isto é devido ao efeito de borda. Apesar disso, novamente há algumas exceções. Por exemplo, em 12 Mbps/160 km/h a correlação foi moderada. Além disso, como no cenário anterior, dada a PDR de 100% em todos os trechos de 25 m, não foi possível calcular a correlação entre PDR e PIR para as transmissões feitas à 6 Mbps nos experimentos reais. A Tabela 5.3 mostra os graus de correlação. Tanto o NS-3/PhySim quanto o Veins/MiXiM reproduzem essa correlação, embora a forma e o comportamento das curvas no NS-3/PhySim sejam mais próximos aos obtidos pelas curvas nos experimentos reais. Ao contrário do cenário anterior, no cenário atual, nenhum trecho apresenta uma mediana de PIR $\geq$1 s, independente do ambiente. Como no cenário anterior, independente do ambiente, a mediana do PIR obtida na região onde as BSMs são importantes permaneceu próxima à taxa de geração das BSMs: 50 ms, para qualquer taxa de dados usada.

Tabela 5.3: Coeficiente de correlação (Cenário 3).

Testes Reais	**6 Mbps**	**12 Mbps**	**18 Mbps**	**24 Mbps**
40 km/h	NA	-0,91048	-0,90382	-0,88538
100 km/h	NA	-0,87347	-0,98172	-0,89581
160 km/h	NA	-0,66314	-0,96377	-0,97545
NS-3/PhySim	**6 Mbps**	**12 Mbps**	**18 Mbps**	**24 Mbps**
40 km/h	-0,97407	-0,85417	-0,89258	-0,89662
100 km/h	-0,97225	-0,89990	-0,80273	-0,83091
160 km/h	-0,95259	-0,93216	-0,85798	-0,79404
Veins/MiXiM	**6 Mbps**	**12 Mbps**	**18 Mbps**	**24 Mbps**
40 km/h	-0,97462	-0,98157	-0,98776	-0,99951
100 km/h	-0,98233	-0,99377	-0,99925	-0,99999
160 km/h	-0,99915	-1	-1	-1

Concluído o capítulo que apresentou os resultados da avaliação do IEEE 802.11p, no próximo capítulo é feita a descrição dos experimentos envolvendo o Wi-Fi Direct.

Capítulo 6

Experimentos com o Wi-Fi Direct

Este capítulo descreve a configuração dos experimentos para análise de viabilidade do Wi-Fi Direct. Os experimentos consistem de medições reais usando *smartphones* comerciais, das fabricantes Xiaomi e Asus, e simulações executadas no INET. O capítulo descreve os cenários de avaliação, a configuração dos experimentos reais, bem como a descrição dos parâmetros usados nas simulações. Também serão mostrados os detalhes de avaliação do método de transmissão oportunística baseado na técnica *beacon-stuffing*.

6.1 Cenários de Avaliação

Como nos cenários de avaliação do IEEE 802.11p, definidos na Seção 4.1 com base nos cenários propostos em [52], foram definidos três cenários baseados no envio de mensagens de segurança, contendo dados posicionais e cinemáticos. Tais cenários têm como base a via sinalizada da Figura 3.1. Como descrito na Seção 3.2, em tais vias, pedestres podem realizar a travessia na faixa mesmo sem autorização semafórica, colocando em risco sua própria vida e também a vida dos motoristas. Por exemplo, um estudo mostrou que mais de 80% das fatalidades com pedestres ocorreram durante uma travessia perpendicular à rota de um veículo, que se locomovia por uma via reta [41, 130]. Além disso, é comum existirem obstáculos, como um ônibus coletando passageiros, entre os veículos e o pedestre que tenta atravessar. Isto pode impedir o funcionamento de sistemas tradicionais de detecção de usuários vulneráveis das vias, já que sensores e câmeras requerem LoS para operar corretamente [71]. Já com relação ao Wi-Fi Direct, a presença de obstáculos pode impedir o estabelecimento da conexão antes que o pedestre inicie a travessia. Com isso, diferente do IEEE 802.11p, a análise do Wi-Fi Direct consistiu de cenários LoS e NLoS, e transmissão V2P. A avaliação é composta por um pedestre, que atua como cliente do grupo P2P, e por um veículo, que atua como GO. Ambos portavam um *smartphone*. A Figura 6.1 apresenta os três cenários de avaliação.

- **Cenário 1 – Impacto do Aumento da Distância:** como no IEEE 802.11p, permite

avaliar o impacto do aumento da distância entre os nós devido ao desvanecimento em larga-escala, permitindo a análise do alcance do Wi-Fi Direct. Também serve como referência para avaliar os resultados envolvendo mobilidade. Neste cenário, após o estabelecimento da conexão, dois pedestres estáticos portando *smartphones* se comunicam por meio da transmissão de mensagens de segurança. A avaliação é baseada na transmissão de 500 mensagens, realizada em trechos de 10 m. Iniciando a 50 m do pedestre receptor, após transmitir 500 mensagens, o pedestre transmissor se posiciona 10 m mais distante e repete o procedimento. O procedimento é repetido de 10 m em 10 m, até que os dispositivos estejam a 150 m de distância. Nos experimentos reais, uma transmissão em 200 m também foi realizada para avaliar se o alcance máximo do Wi-Fi Direct corresponde ao alcance teórico de 200 m. Novamente, são avaliados o alcance máximo e efetivo da comunicação.

- **Cenário 2 – Impacto da Mobilidade com LoS:** permite avaliar o impacto da mobilidade no desempenho do Wi-Fi Direct. O objetivo principal é analisar o impacto do CET no tempo de contato entre os dispositivos. Com isso, é possível analisar a viabilidade do Wi-Fi Direct em suportar uma aplicação de prevenção de colisão entre veículo e pedestre. Como mencionado na Seção 1.1, um CET longo pode fazer com que a mensagem de segurança não seja recebida em tempo no veículo, diminuindo a janela de atuação da aplicação, e fazendo com que o tempo disponível para parar o veículo após acionamento dos freios seja insuficiente. Neste cenário, enquanto o pedestre se mantém estático e, após o estabelecimento da conexão, transmitindo mensagens de segurança continuamente, o veículo se locomove em direção ao pedestre com velocidades de 20 km/h, 60 km/h e 100 km/h. O veículo inicia sua rota a uma distância de aproximadamente 500 m do pedestre, grande o suficiente para entrar no alcance de comunicação do pedestre com a velocidade desejada. Cabe ressaltar que o estabelecimento da conexão acontece durante o percurso do veículo em direção ao pedestre. Diferente da análise feita no Cenário 1, dividida em trechos de 10 m, neste cenário todas as transmissões feitas pelo pedestre em direção ao veículo são contabilizadas, e os resultados são divididos em trechos de 20 m cada.

  Cenário 3 – Impacto da Mobilidade com NLoS: similar ao cenário anterior, com o adendo de inserir um veículo de médio porte (sem Wi-Fi Direct) entre o pedestre e o veículo atuando como GO. O objetivo é analisar o impacto causado pela obstrução do sinal de rádio, causada por condições NLoS na comunicação em um ambiente mais realista. No mundo real, não existem garantias de linha de visada entre transmissor e receptor. A propagação do sinal pode ser afetada por árvores, edificações ou outros veículos presentes na via. Portanto, é preciso avaliar se as mensagens de segurança serão capazes de alertar o veículo em movimento sobre a travessia indevida do pedestre, que pode não possuir informação visual devido ao obstáculo.

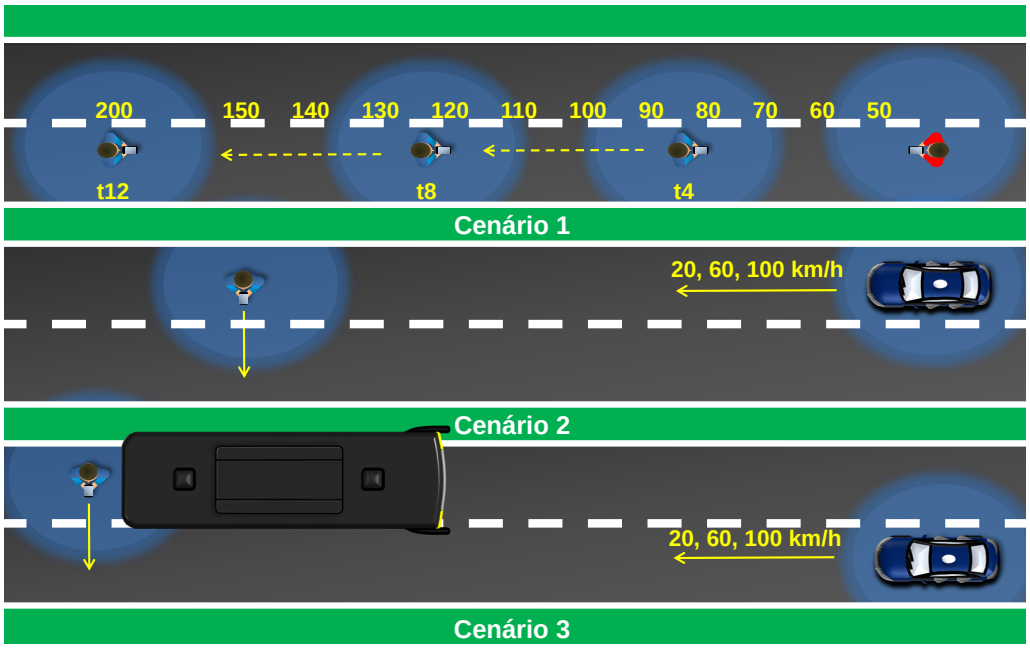

Figura 6.1: Cenários avaliados nos experimentos do Wi-Fi Direct.

Como no IEEE 802.11p, a investigação que visa responder se os resultados de experimentos reais e simulações são equivalentes tem como base a PDR e o PIR. Novamente, exceto em 200 m (Cenário 1) – onde o total de rodadas planejado foi cinco – e a 100 km/h (Cenário 3) – onde em apenas seis das dez rodadas foi possível estabelecer a conexão e transmitir dados –, tentou-se executar dez rodadas para cada permutação de cenário nos experimentos reais. Porém, o total de rodadas consideradas válidas foi variável. Em certos casos, algumas rodadas foram consideradas com possível erro. Por exemplo, para os cenários 2 e 3: (1) casos onde houve transmissões apenas a longas distâncias (cerca de 80 m); e (2) casos onde a distância entre veículo e pedestre só aumentou, ao invés de diminuir progressivamente e, após a ultrapassagem do pedestre feita pelo veículo, aumentar. Em alguns casos, a conexão só foi estabelecida, por exemplo, após a ultrapassagem. Para os cenários 2 e 3, especificamente, consideram-se como rodadas válidas aquelas onde a conexão e transmissão de dados acontecera antes da ultrapassagem – após esta, a aplicação era encerrada. Assim, para tais cenários, os dados entendidos como corretos são aqueles que indicam uma aproximação progressiva do veículo em direção ao pedestre, admitindo-se um afastamento após a ultrapassagem. Em resumo, no Cenário 1, na avaliação de 50 m a 150 m, dez rodadas foram executadas. Em 200 m, cinco. Já no Cenário 2, à 20 km/h, foram nove rodadas válidas, enquanto que à 60 km/h e 100 km/h foram dez. Por fim, no Cenário 3, à 20 km/h, foram nove rodadas válidas, enquanto que à 60 km/h e 100 km/h, foram oito e seis, respectivamente. Novamente, nas simulações sempre foram executadas dez rodadas para cada permutação. A Tabela 6.1 resume os cenários de avaliação.

Cabe ressaltar também que, nos experimentos reais, em alguns casos houve certa dificuldade em estabelecer uma conexão entre os nós e transmitir dados, como em longas

distâncias, altas velocidades e condições NLoS. Na avaliação dos cenários 1, 2, e 3, os experimentos foram executados até que fosse possível estabelecer uma conexão entre os nós em cerca das dez rodadas planejadas para execução de cada permutação de cenário. Mais uma vez, transmissões simultâneas não são consideradas na análise de similaridade entre os ambientes.

Tabela 6.1: Características dos cenários dos experimentos com Wi-Fi Direct.

Cenário	Investigação	Condição	Vel. Pedestre (km/h)	Vel. Veículo (km/h)
1	Aumento da distância	LoS	Estático (0)	–
2	Impacto da mobilidade	LoS	Estático (0)	20-60-100
3	Impacto da mobilidade	NLoS	Estático (0)	20-60-100

6.2 Configuração dos Experimentos Reais

Os experimentos foram feitos usando dois *smartphones* comerciais. No veículo, foi usado um modelo Xiaomi MI A2, com processador Octa-Core de 2,0 GHz e com 4 GB de RAM, que atuou como GO do grupo P2P. No lado do pedestre, foi usado um modelo Asus Zenfone Live L1, com processador Octa-Core de 1,4 GHz e com 2 GB de RAM, que atuou como cliente do grupo P2P. A altura do *smartphone* dentro do veículo era de aproximadamente 1,3 m, enquanto que a altura do *smartphone* portado pelo pedestre era em torno de 1,6 m. As versões do Android dos dispositivos são a 9.0 *One Pie*, com API (*Application Programming Interface*) 28, para o Xiaomi, e a 8.0 *Oreo*, com API 26, para o Asus. A aplicação para transmissão de mensagens de segurança sobre Wi-Fi Direct foi implementada tendo como base a API do Google `android.net.wifi.p2p`[1], bem como o código disponibilizado pelo canal Sarthi Technology, que possui uma série de vídeos tutoriais sobre implementação do Wi-Fi Direct para Android, no Youtube[2]. A implementação foi feita usando o *software* Android Studio.

Como mencionado na Seção 1.2, visando analisar a viabilidade do Wi-Fi Direct sob aspectos de rede, o atraso para seleção, na tela do dispositivo, do nó ao qual se deseja conectar, foi desconsiderado nos experimentos. Isto foi feito pois a conexão pode ser realizada automaticamente invocando o método de conexão do Wi-Fi Direct dentro do método `PeerListListener`, que é responsável por mostrar na tela a lista de pares disponíveis após a conclusão da etapa de descoberta, e passando de maneira explícita o ID do dispositivo desejado (GO). Como mencionado, tal ID pode ser obtido após filtrar, entre os dispositivos descobertos na rede, aquele que possui em seu nome uma *string* que, por exemplo, identifica uma dada aplicação. O mesmo se deu em relação à transmissão das mensagens de segurança nos cenários com mobilidade. Tão logo o grupo é formado, o cliente do

[1] https://developer.android.com/reference/android/net/wifi/p2p/package-summary

[2] https://www.youtube.com/watch?v=nw627o-8Fok&list=PLFh8wpMiEi88SIJ-PnJjDxktry4lgBtN3

grupo P2P transmite as mensagens via *socket* UDP ao GO, sem que o usuário precise interagir com a aplicação para iniciar a transmissão. Além disso, o atraso da interação do usuário com a tela para dar o aceite à conexão por meio do clique de um botão também foi desconsiderado. O aceite da conexão foi dado em um primeiro momento. As demais conexões foram feitas, portanto, no modo persistente. De acordo com o nosso conhecimento, a etapa do aceite da conexão só pode ser ignorada fazendo *root* no dispositivo, que não é uma opção considerada nesta tese.

A comunicação entre pedestre e veículo consiste no envio, via *unicast*, de mensagens de segurança contendo dados cinemáticos. As mensagens possuem cerca de 80 bytes e são enviadas a cada 100 ms. Cada mensagem possui um contador, as coordenadas geográficas do dispositivo, velocidade, sentido de direção, e *timestamp* da informação, obtidos pelo GPS do *smartphone* à taxa de 1 Hz. Neste ponto, cabe ressaltar que, além de possíveis bloqueios de sinais enviados pelos satélites, como os provocados por túneis [91], receptores GNSS também apresentam erros de precisão da localização. Por exemplo, medições feitas usando GPS demonstraram que tais erros podem ser de até 10 m, mesmo em boas condições climáticas [41, 131]. Em termos de aplicações de segurança para veículos, a precisão de posicionamento pode ser classificada em três níveis: *which-road*, com até 5,0 m de precisão, *which-lane*, com até 1,5 m, e *where-in-lane*, até 1,0 m de precisão [132, 133]. Segundo Pinto Neto *et al.*, considerando ruas e faixas com largura entre 2,5 m e 3,5 m, as medições feitas por um sistema de posicionamento do tipo *lane-level*, baseado em um receptor GNSS *Autonomous Single Carrier* (L1), não seriam confiáveis, dado que os erros e as larguras das faixas são da mesma ordem de magnitude. Na maioria das aplicações, o nível *which-lane* é necessário. É importante ressaltar que, nos experimentos reais desta tese, nenhum processamento ou técnica foi usada visando corrigir os erros de precisão das coordenadas geográficas obtidas pelo GPS dos *smartphones*. Portanto, na análise do risco de colisão, os cálculos feitos com base nas latitudes e longitudes obtidas pelo GPS podem incluir erros de posição, como 10 m. E conforme Sewalkar *et al.* [41], a ausência de dados precisos de localização pode comprometer a precisão do cálculo do risco de acidente entre veículos e usuários vulneráveis das vias. Além disso, é importante considerar também que a taxa de atualização do GPS (1 Hz) é dez vezes superior ao requisito de latência máxima de aplicações de segurança (100 ms).

Como no IEEE 802.11p, e de certa forma baseado em Sassi *et al.* [52], os experimentos reais foram feitos no aeroporto desativado da cidade de Leopoldina – MG, Brasil. As janelas do veículo permaneceram fechadas durante os experimentos. A Figura 6.2(a) apresenta os dispositivos utilizados. Já as Figuras 6.2(b), 6.2(c), e 6.2(d) apresentam a avaliação em progresso nos três cenários.

(a) Dispositivos utilizados. (b) Alcance máximo.

(c) Mobilidade com LoS. (d) Mobilidade com NLoS.

Figura 6.2: Cenário dos experimentos reais com o Wi-Fi Direct.

6.3 Configuração das Simulações no INET

As simulações são baseadas na implementação do Wi-Fi Direct, disponível para INET. Nas simulações, veículo e pedestre são modelados como nós de rede que possuem uma interface sem-fio compatível com Wi-Fi Direct. São usadas as versões do INET 3.4, OMNeT 5.0, SUMO 0.32.0 e Veins 4.5. Como no IEEE 802.11p, a geração da rota do veículo se deu configurando um *trace* de mobilidade no SUMO. Visando refletir as condições do cenário real, mais uma vez muitos dos recursos de mobilidade do SUMO não foram usados. Novamente, a via foi baseada no aeroporto dos experimentos reais, apesar do comprimento ser menor devido ao menor alcance do Wi-Fi Direct. A modelagem da via foi feita com as ferramentas NETEDIT e NETCONVERT, do SUMO. O subprojeto Veins_INET foi usado para criação do ambiente veicular pelo Veins, como pelo uso de um modelo de mobilidade nos nós definidos no INET. Baseado nos experimentos reais, a altura dos dispositivos é definida como 1,3 m para o nó modelado como veículo e 1,6 m para aquele modelado como pedestre. Como nos experimentos reais, nas simulações do INET, as mensagens de segurança possuem 80 bytes e são transmitidas a cada 100 ms. A transmissão e recepção de dados são baseadas em tráfego UDP. Para isso, usou-se como base as rotinas de transmissão/recepção definidas nos arquivos `UDPBasicApp` e `UDPSink`, respectivamente, disponíveis no diretório de aplicações do INET. A coleta de métricas também foi feita em tais arquivos. Como nos experimentos reais, a transmissão de dados inicia após

a associação do cliente do grupo P2P ao GO. Isto é controlado pelo estado `P2PClient`, no método `handleBeaconFrame` do arquivo `Ieee80211MgmtSTAWifiDirect`. A configuração dos parâmetros das simulações foi baseada na configuração padrão do arquivo `omnetpp.ini`, com base no exemplo de simulação fornecido por Iskounen *et al.*, em [63]. Como no IEEE 802.11p, parâmetros presentes em `omnetpp.ini`, considerados inadequados para as simulações desta tese, foram comentados ou tiveram seus valores modificados para representar os cenários de avaliação. A seguir, são apresentados os parâmetros cujos valores foram modificados.

Baseado nas especificações do *smartphone* Asus Zenfone, que atua como transmissor nos experimentos reais, a potência de transmissão foi definida como 13,9 dBm [134]. A posição dos nós é obtida com base nas coordenadas cartesianas x, y, z, fornecidas pelo modelo de mobilidade. Baseado no valor proposto por Bloessl *et al.* [127], o ruído de fundo foi definido como -98 dBm. Apesar do Wi-Fi Direct suportar uma taxa de dados máxima teórica de 250 Mbps, a taxa de dados definida nas simulações foi 54 Mbps (IEEE 802.11g). De acordo com o nosso conhecimento, esta é a taxa máxima suportada pela versão do INET usada. O atraso de propagação foi definido como constante. O tamanho do cabeçalho, bem como o limite de retransmissões na camada MAC foram definidos como 0. O desvanecimento em larga-escala foi gerado pelo modelo de propagação `LogNormalShadowing`. Como ocorreu no IEEE 802.11p, nas simulações do INET este modelo foi capaz de reproduzir o comportamento da atenuação do sinal de rádio conforme a distância entre os nós aumentava. No `LogNormalShadowing`, o parâmetro `alpha` foi definido empiricamente como 2,21, na etapa de calibração das simulações, com base nos resultados dos experimentos reais de avaliação do alcance da comunicação. Similar ao que foi feito para o IEEE 802.11p, o processo de calibração consistiu em obter, nas simulações, no trecho que corresponde à distância de 150 m entre os nós, uma PDR semelhante à PDR obtida no mesmo trecho nos experimentos reais. Após este procedimento, é feita a investigação quanto à equivalência dos resultados obtidos nos dois ambientes.

No Cenário 3, que avalia o impacto das condições NLoS na comunicação feita com Wi-Fi Direct, um obstáculo foi inserido entre o veículo e o pedestre – a 5 m de distância deste último –, simulando um ônibus parado coletando passageiros. O obstáculo possui 10 m de comprimento, 2,5 m de largura, e 2,5 m de altura. O mesmo é constituído por dois materiais: (1) alumínio, com espessura de 1,5 cm e altura de 1,8 m para cada lado, 2,5 m para a parte traseira e 1,5 m para a parte frontal; e (2) vidro, que completa a altura total do obstáculo e possui espessura de 1,0 cm. Tais medidas e informações sobre os tipos de material que compõem o obstáculo são necessárias para calcular a constante dielétrica do mesmo, que permitirá ou não a passagem do sinal de rádio incidente. A implementação original do alumínio, definida no arquivo `MaterialRegistry`, disponível na versão usada do INET, foi modificada, uma vez que na mesma não estão definidos os valores relativos à permissividade e permeabilidade do material. Tais parâmetros foram definidos como 8,1

Tabela 6.2: Parâmetros das simulações do INET.

Modelo	Parâmetro	Valor
udpApp	typename	UDPBasicApp (pedestre)
	messageLength	80 bytes
	typename	UDPSink (veículo)
wlan	mgmtType	Ieee80211MgmtSTAWifiDirect
	bitrate	54Mbps
wlan.radio.transmitter	power	24.60mW (13,9 dBm)
	headerBitLength	0 bits
wlan.mac	retryLimit	0
radioMedium	obstacleLossType	DielectricObstacleLoss
	pathLossType	LogNormalShadowing
	pathLoss.alpha	2.21
	backgroundNoise.typename	IsotropicScalarBackgroundNoise
	backgroundNoise.power	-98 dBm
	propagation.typename	ConstantSpeedPropagation
VeinsInetMobility	height	1.6 (pedestre), 1.3 (veículo)

e 1,00002, respectivamente, com base em [135, 136]. A Tabela 6.2 apresenta, em resumo, os valores dos parâmetros de simulação definidos no INET.

Configuração para Avaliação do *Beacon-Stuffing*

A avaliação de um método simples de transmissão de informação baseado em *beacon-stuffing* também foi feita via simulações no INET, além de ser baseada em um pequeno cenário real. O objetivo é avaliar uma possível melhora na distância de recepção das mensagens de segurança, em relação ao Cenário 3 (NLoS). No método em questão, o campo de 32 bytes do nome do dispositivo Wi-Fi Direct deve ser modificado para transmitir mensagens de segurança. Como o método que permite modificar o nome do dispositivo Wi-Fi Direct não é acessível diretamente via API `android.net.wifi.p2p`, nos experimentos reais, tal modificação foi feita usando Java Reflection. Assim, foi possível modificar o nome do dispositivo Wi-Fi Direct, preenchendo-o com uma *string* fixa, que contém dados que representam alguns dados cinemáticos que podem ser obtidos do receptor GNSS embarcado no dispositivo, como as coordenadas geográficas (latitude e longitude), direção da viagem e velocidade, bem como um ID/contador da mensagem de segurança. Tais campos fornecem as informações básicas para uma aplicação de segurança prevenir colisões entre veículos e pedestres. Diferente da avaliação nos Cenários 1, 2, e 3, na avaliação do método de transmissão baseado em *beacon-stuffing*, o pedestre atua como GO de um grupo P2P autônomo, transmitindo, *em broadcast*, mensagens de segurança na rede.

No transmissor, o método consiste em: (1) criar um grupo P2P autônomo; (2) coletar os dados do receptor GNSS embarcado no dispositivo portado pelo pedestre; (3) construir a mensagem de segurança com base nos dados coletados e inserir um ID/contador para a mensagem; (4) modificar o campo de 32 bytes do nome do dispositivo Wi-Fi Direct pelo conteúdo da mensagem de segurança; (5) remover o grupo P2P autônomo criado ante-

riormente e, imediatamente, (6) recriar o grupo P2P. As etapas (2) à (6) são realizadas à cada 1 s. A remoção/criação periódica do grupo P2P autônomo é necessária pois, conforme os experimentos realizados, de outro modo, a descoberta de dispositivos realizada no receptor (veículo) não é capaz de mostrar o nome do dispositivo Wi-Fi Direct mais recente. Não é possível obter, por exemplo, os dados posicionais mais recentes do pedestre, que são carregados oportunisticamente como uma mensagem de segurança conforme o nome do dispositivo Wi-Fi Direct é modificado. Nos testes práticos, mesmo que o nome do dispositivo Wi-Fi Direct fosse modificado periodicamente para compor a mensagem de segurança mais recente, sem remover/recriar o grupo P2P autônomo no transmissor, o nome mostrado pelo receptor sempre fora aquele inicialmente descoberto. Assume-se que, depois de remover/recriar o grupo P2P, o Android atualiza o nome do dispositivo Wi-Fi Direct carregado nos quadros de controle. Assume-se também que a alteração deste nome pelo Android, após a remoção/recriação do grupo P2P, possibilita ao receptor considerar o dispositivo descoberto como um novo dispositivo, levando-o a mostrar o nome atualizado.

Após recriar o grupo P2P autônomo, o transmissor inicia o envio de *beacons*. Com base no envio feito a cada 100 ms, em torno de dez *beacons* são enviados a cada segundo carregando a mensagem de segurança. Nos testes práticos feitos com um *laptop* cuja interface de rede sem-fio operava em modo monitor, a taxa de recepção dos *beacons* apresentou, visualmente, pequenos atrasos, devido à remoção/recriação periódica do grupo P2P autônomo. No receptor, o método consiste em: (1) coletar periodicamente os dados do receptor GNSS embarcado no dispositivo portado pelo veículo e (2) executar continuamente o método `PeerListListener`, da API do Wi-Fi Direct no Android. Dado o modo de operação do Wi-Fi Direct, principalmente na descoberta de dispositivos, assume-se que a descoberta dos dados transmitidos pelo transmissor no receptor acontecerá quando: (1) o transmissor enviar *beacons* no mesmo canal que o receptor escolheu escutar na fase de *Listen*; ou (2) quando o receptor receber *probe responses* do transmissor após enviar, durante a fase de *Search*, *probe requests* no mesmo canal que o transmissor está operando. Visando possibilitar recepção contínua, o método `PeerListListener` foi configurado para reiniciar sempre que a aplicação detectar sua interrupção. Isso garante a execução contínua do método. No transmissor, o método `PeerListListener` foi desabilitado, pois assume-se que a comunicação entre pedestre e veículo é unidirecional. Apenas o pedestre transmite mensagens de segurança, por meio da modificação do nome do dispositivo Wi-Fi Direct.

A avaliação do método por meio de experimentos reais foi realizada em um pequeno cenário, onde dois *smartphones* foram colocados lado a lado. Um deles atuou como GO do grupo P2P autônomo e o outro como receptor. No experimento prático, 1000 mensagens de segurança foram transmitidas pelo GO. Ou seja, por 1000 s, o nome do dispositivo foi modificado, bem como o grupo P2P autônomo foi removido/recriado a cada 1 s, permitindo que o método `PeerListListener`, em execução contínua no receptor, apresentasse

o nome do dispositivo Wi-Fi Direct mais recente. O teste prático foi realizado em um ambiente sem interferência e com a coleta de dados realizada pelo receptor GNSS desativada nos dispositivos. O motivo foi eliminar possíveis problemas de desempenho causados por especificidades de *hardware*. Com isso, na *string* que compõe a mensagem de segurança, apenas o ID/contador da mensagem foi modificado periodicamente como forma de avaliar a viabilidade do método de transmissão. Cabe ressaltar que, no processo de remoção/recriação do grupo P2P autônomo, o canal de operação do GO pode ser diferente do canal usado anteriormente. Entretanto, nos testes práticos feitos com a interface de rede sem-fio do *laptop* em modo monitor, na maioria das vezes o GO definiu o mesmo canal. De acordo com nosso conhecimento, nativamente não é possível definir o canal utilizado pelo GO.

O método também foi avaliado no INET. Nas simulações, o GO do grupo P2P autônomo transmite *beacons* a cada 100 ms. Dado que, nos experimentos reais, o GO quase sempre definiu o mesmo canal de operação após a remoção/recriação do grupo P2P autônomo, nas simulações o GO também transmite *beacons* no mesmo canal. Diferente dos testes práticos, no INET não há a etapa de remover/recriar o grupo P2P após a modificação do nome do dispositivo. Como nos testes práticos, os *beacons* também carregam uma *string* de dados fixa que simboliza os dados cinemáticos inseridos em uma mensagem de segurança. Como os *beacons* são transmitidos a cada 100 ms, de forma a simular a modificação do nome do dispositivo Wi-Fi Direct feita a cada 1 s, o ID/contador da mensagem é incrementado sempre que dez *beacons* são transmitidos. Conforme já mencionado, assume-se que o GO pode ser descoberto não só pela recepção de *beacons*, mas também por *probe responses*, enviados pelo GO após a recepção de *probe requests*. Deste modo, a *string* fixa que representa a mensagem de segurança também é carregada por *probe responses*. Como já mencionado, o objetivo das simulações no INET é avaliar uma possível melhora na distância de recepção das mensagens de segurança, em relação ao que foi obtido no Cenário 3 (NLoS). Assim, a avaliação se baseia na suposição de que, com o *beacon* ou *probe response* carregando os dados cinemáticos do pedestre, a recepção destes dados no veículo permitiria ao condutor evitar a colisão.

A transmissão/recepção de mensagens é baseada nas rotinas de transmissão/recepção de *beacons* e *probe responses* definidas no arquivo `Ieee80211MgmtSTAWifiDirect`. O receptor inicialmente executa um *scan* ativo nos canais sociais. Se nenhum grupo P2P for identificado, o nó então executa continuamente a descoberta de dispositivos. O provisionamento WPS foi desabilitado. No receptor, apenas a primeira de uma série de até dez mensagens de segurança recebidas com mesmo ID/contador é contabilizada. Isso é necessário para simular a forma como a "recepção" – a percepção da mudança do nome do dispositivo – ocorre nos testes práticos, já que o `PeerListListener` só considera a descoberta de um novo dispositivo nos casos onde o conteúdo (ID/contador) da mensagem é diferente do anterior – significando que o nome do dispositivo Wi-Fi Direct foi modificado.

Para simular esta modificação, foi adicionado à classe `Ieee80211BeaconFrameBody`, do arquivo `Ieee80211MgmtFrames`, um campo relacionado ao nome do dispositivo.

O método de transmissão também foi avaliado em um ambiente com interferência. Quatro cenários de simulação foram definidos baseados na variação do número de nós atuando como GOs (pedestres) transmitindo *beacons* periodicamente no mesmo canal de operação. O número de transmissores simultâneos variou entre dois, quatro, seis e oito. Em todos os casos, existe apenas um receptor (veículo).

Neste capítulo, foram mostrados os detalhes dos experimentos com o Wi-Fi Direct. Seguindo a estrutura definida, no próximo serão apresentados os resultados da avaliação desta tecnologia, através de experimentos práticos e simulações.

Capítulo 7

Resultados dos Experimentos com o Wi-Fi Direct

Este capítulo mostra os resultados da análise de viabilidade do Wi-Fi Direct, por meio de testes práticos usando *smartphones* comerciais e simulações no INET. Primeiramente, como no IEEE 802.11p, os resultados obtidos em ambos os ambientes são confrontados como forma de avaliar a capacidade de mimetização do modelo de simulação do Wi-Fi Direct disponível no INET. Novamente, os resultados são baseados na mediana da PDR e do PIR, apresentada por meio de gráficos com barras de erro verticais que correspondem ao desvio absoluto da mediana. Como descrito na Seção 6.1, com algumas exceções, nos testes práticos tentou-se executar dez rodadas para cada permutação de cenário. Mais uma vez, para cálculo da mediana, são considerados os casos onde foi possível receber mensagens de segurança em pelo menos metade das rodadas, se o total de rodadas é par, e metade mais um, se o total é ímpar. Novamente, as simulações foram executadas em um *laptop* Intel Core i7-7500U, de 2,7 GHz, e 16 GB de RAM. Nas simulações, o total de rodadas executadas para cada permutação foi sempre dez. Em seguida, o método de transmissão baseado no *beacon-stuffing* também é avaliado. Na avaliação feita em um simples cenário real, foram executadas cinco rodadas. Os resultados são baseados na mediana da PDR e do PIR, obtida nas cinco rodadas. O método também é avaliado via simulações no INET, onde dez rodadas foram executadas. Os resultados são baseados na mediana do número de mensagens de segurança recebidas em cada trecho de 20 m, obtida nas dez rodadas.

7.1 Impacto e Duração do CET

Esta seção tem como objetivo apresentar alguns resultados preliminares com relação ao impacto que um longo CET pode gerar na comunicação entre dispositivos baseada no Wi-Fi Direct. Tais resultados são gerados a partir de simulações executadas no INET, cujo objetivo é analisar a viabilidade do Wi-Fi Direct com base na avaliação dos Cenários 1, 2, e 3,

apresentados na Seção 6.1. Como mencionado na Seção 6.1, tanto nos experimentos reais quanto nas simulações, em alguns casos houve certa dificuldade em estabelecer uma conexão entre os nós e transmitir dados. No modo de operação tradicional do Wi-Fi Direct, a transmissão de dados só é possível após o estabelecimento da conexão. Deste modo, os resultados da avaliação dos Cenários 1, 2, e 3, apresentados neste capítulo, são baseados nas rodadas em que a conexão foi corretamente estabelecida entre os nós, tornando possível a transmissão das mensagens de segurança do pedestre (cliente do grupo P2P) ao veículo (GO). Na avaliação dos Cenários 1, 2, e 3, as simulações foram executadas até que fosse possível estabelecer a conexão entre os nós nas dez rodadas planejadas para execução, para cada permutação de cenário. A Figura 7.1 mostra, para cada cenário, a taxa de sucesso no estabelecimento da conexão com Wi-Fi Direct, levando em consideração a razão entre as dez rodadas bem-sucedidas, e o total de tentativas feitas para cada permutação. Por exemplo, nas simulações do Cenário 1, em 150 m, foram feitas 40 tentativas para que fosse possível estabelecer a conexão em 10 delas, levando a uma taxa de sucesso de 25%. Como pode ser visto, em trechos mais distantes (Cenário 1), usando velocidades mais altas (Cenários 2 e 3), e em condições com NLoS (Cenário 3), os resultados indicam que é mais difícil estabelecer uma conexão. Tais resultados demonstram o quão desafiador pode ser usar o Wi-Fi Direct como uma tecnologia de rádio alternativa ao IEEE 802.11p, especialmente em cenários de mobilidade.

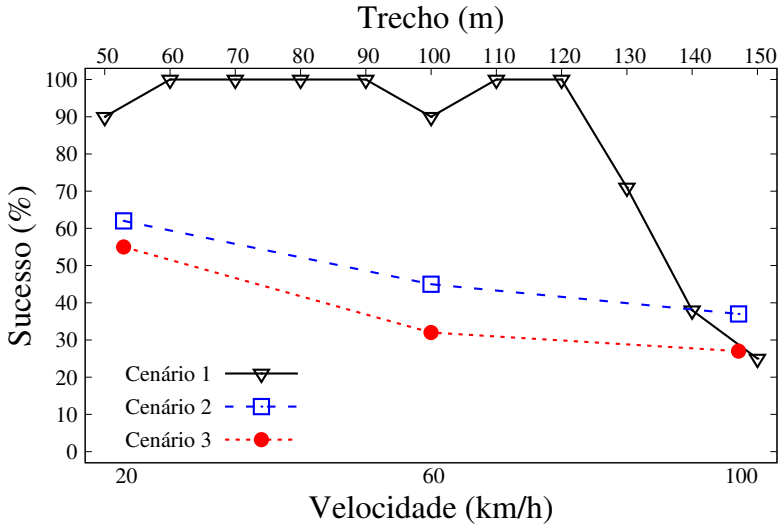

Figura 7.1: Taxa de sucesso no estabelecimento da conexão com Wi-Fi Direct.

Já a Figura 7.2 mostra a mediana da duração do CET na avaliação dos Cenários 1, 2, e 3 nas simulações. As barras de erro verticais correspondem ao desvio absoluto da mediana. A duração do CET é calculada como o intervalo de tempo a partir da recepção do primeiro *probe request*, pelo pedestre, até a associação do mesmo com o veículo. Isto é controlado pelos estados `ListenFindPhase/P2PGroupOwner`, no método `handleProbeRequestFrame` do arquivo `Ieee80211MgmtSTAWifiDirect`. Como nos

experimentos reais, nas simulações dos Cenários 1, 2, e 3 no INET, o veículo sempre atua como GO do grupo P2P. Concluído o estabelecimento da conexão, o pedestre pode iniciar a transmissão das mensagens de segurança ao veículo. Como é possível observar, os resultados indicam que o CET é menos afetado pela distância (Cenário 1) do que pela mobilidade (Cenários 2 e 3). Além disso, apesar de inesperado, também é possível observar que o CET é maior em velocidades mais baixas. Uma explicação possível para este resultado está no fato de que, em velocidades mais baixas, o veículo leva mais tempo para alcançar o pedestre a partir da primeira recepção de um *probe request*. Nestes casos, a maior duração de tempo pode auxiliar no estabelecimento da conexão, pois o veículo tem mais tempo para realizar todo o processo, conforme descrito na Seção 2.3, se recuperando de possíveis perdas de quadros de controle ocorridas no trajeto. Conforme o nosso entendimento, em velocidades mais altas, para ter sucesso, todo o processo deve ser concluído possivelmente sem perdas, levando a um CET mais baixo. É importante ressaltar que, nos experimentos reais, a coleta dos dados de conexão não foi realizada.

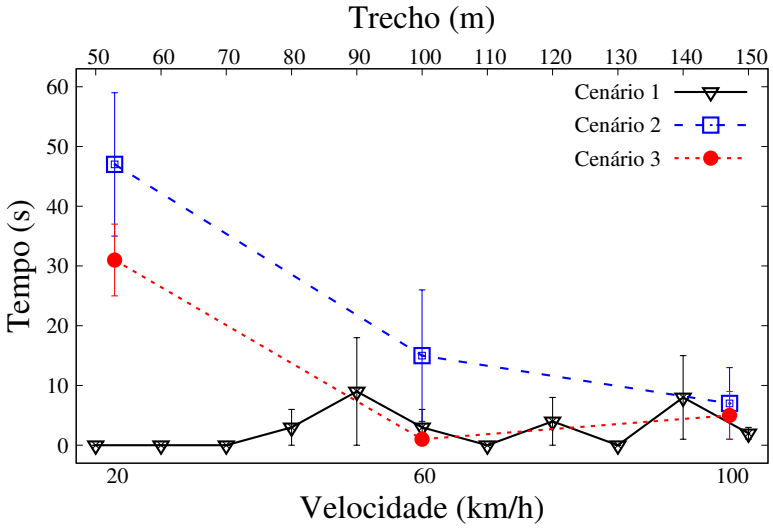

Figura 7.2: Duração do CET no Wi-Fi Direct.

7.2 Impacto do Aumento da Distância

Como no IEEE 802.11p, esta seção avalia o impacto do aumento da distância entre os nós e investiga o alcance obtido pelo Wi-fi Direct. Antes de considerar o Wi-Fi Direct como uma tecnologia de rádio alternativa ao IEEE 802.11p, é necessário analisar se os dispositivos são capazes de se comunicar nas distâncias definidas como requisito de algumas aplicações. Por exemplo, como mencionado na Seção 2.3, segundo Jeong *et al.* [2], com base nas especificações do padrão SAE J2735, uma aplicação como alerta de mudança de faixa poderia, teoricamente, ser suportada pelo Wi-Fi Direct, já que tal aplicação opera dentro de um alcance de 100 m. Novamente, conforme definido por Huang *et al.* [123], são

avaliados o alcance máximo e efetivo da comunicação. Como no IEEE 802.11p, o alcance efetivo é definido como a distância máxima na qual o pedestre receptor é capaz de receber, pelo menos, 80% das mensagens de segurança enviadas pelo pedestre transmissor [126]. Os resultados deste cenário também são usados como referência para a etapa de calibração do modelo de propagação `LogNormalShadowing` do INET, visando aproximar o ambiente simulado do real.

A Figura 7.3 apresenta a PDR e o PIR, nos experimentos reais e simulações, conforme a distância entre os nós aumenta a cada 10 m. Conforme é possível observar nos experimentos reais, entre 50 m e 100 m é possível obter uma PDR $\approx$100%. Devido à atenuação do sinal de rádio, a partir de 110 m a redução da PDR com o aumento da distância fica perceptível. Entretanto, entre 110 m e 120 m, ainda é possível obter um alcance efetivo com os dispositivos Wi-Fi Direct (PDR $\geq$80%). Também é possível observar que, entre 50 m e 150 m, a PDR é sempre $\geq$60%. Portanto, mesmo considerando a comunicação no trecho mais distante, ainda é possível obter um alcance satisfatório entre os dispositivos. Dependendo dos requisitos de uma dada aplicação, a PDR de $\approx$60% poderia ser suficiente para suportar o funcionamento de uma aplicação de segurança, especialmente se dedicada a usuários vulneráveis da via. Conforme análise feita por Sewalkar *et al.* [41], em aplicações de segurança V2P baseadas em *smartphones* e Wi-Fi, o alcance normalmente varia entre 100 m e 150 m. Segundo os autores, tal alcance pode ser suficiente em áreas urbanas, com veículos se locomovendo a até 50 km/h. Apenas para fins de investigar se o alcance máximo teórico de 200 m do Wi-Fi Direct pode ser obtido na prática, uma medição baseada em cinco rodadas foi realizada com os *smartphones* separados por 200 m. Os resultados deste teste indicaram uma PDR $\approx$20%, e PIR $\approx$120 ms (não mostrados na Figura 7.3). Apesar de ainda ser possível receber mensagens de segurança, a baixa PDR pode não permitir a plena operação de uma aplicação de segurança neste ponto da via. Devido à etapa de calibração, nas simulações do INET é possível obter uma PDR muito próxima à obtida nos experimentos reais. Como no IEEE 802.11p, apesar das diferenças em termos de valores absolutos, o simulador é capaz de reproduzir o comportamento de queda da PDR conforme a distância entre os nós aumenta.

Quanto ao PIR, os resultados dos experimentos reais indicam, da mesma forma que na avaliação do IEEE 802.11p, um relacionamento entre o aumento da distância e o aumento desta métrica. Como a potência de transmissão é fixa, quanto maior é a distância, mais forte é a atenuação do sinal [52]. Assim, devido ao efeito de borda, quanto menor é a PDR, maior é o PIR. Apesar disso, é interessante notar que o PIR não aumentou muito mesmo quando a PDR é baixa. No geral, o PIR é ligeiramente similar à taxa de geração das mensagens de segurança (100 ms). Por exemplo, a 200 m, a PDR é $\approx$20%, enquanto que o PIR é $\approx$120 ms. Isso indica que, das 500 mensagens transmitidas nesta distância, $\approx$100 foram recebidas possivelmente em lote. Como mencionado na Seção 5, em cenários mais complexos, tal comportamento pode indicar um alerta para aplicações que dependam de comu-

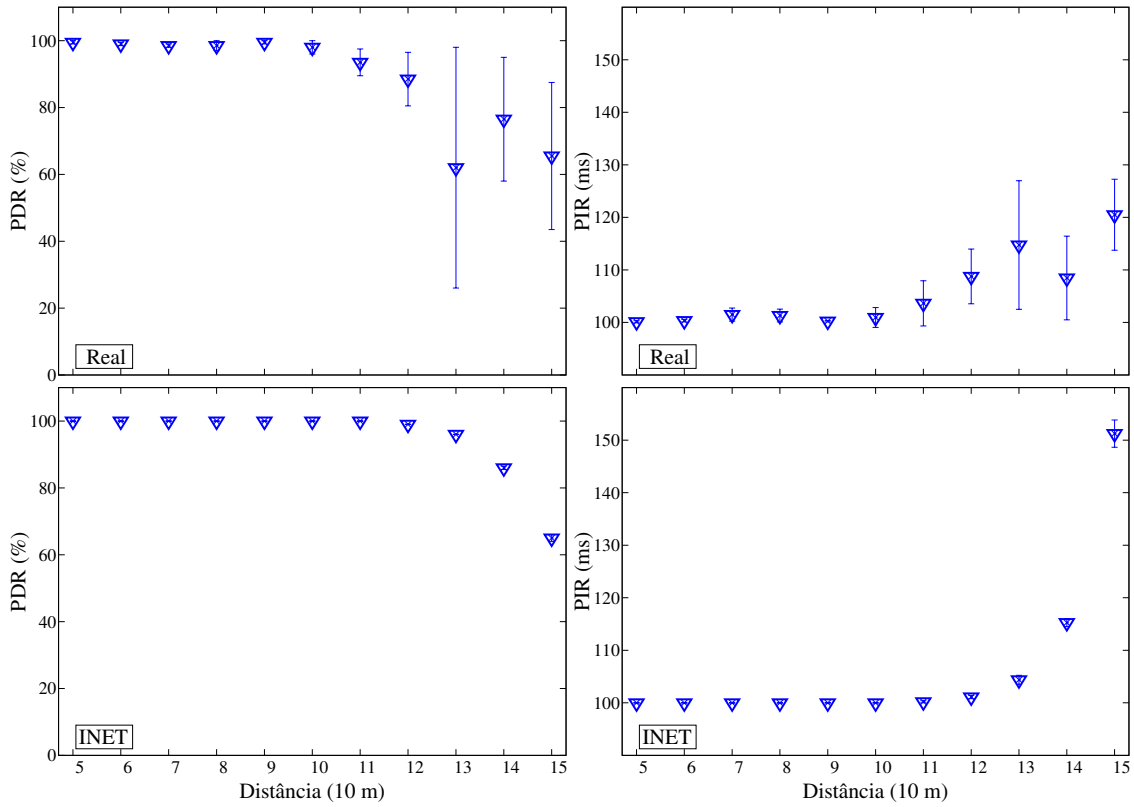

Figura 7.3: Alcance da comunicação com relação à PDR e ao PIR.

nicações a longas distâncias. Uma correlação negativa muito forte entre PIR e PDR pode ser identificada (-0,95014). Tal comportamento é corretamente reproduzido nas simulações (-0,99508), apesar das diferenças em termos de valores absolutos – especialmente em 150 m. Entretanto, ao contrário dos resultados do IEEE 802.11p, no Wi-Fi Direct a correlação entre as métricas ocorreu apenas no Cenário 1. Nos Cenários 2 e 3, no geral não é possível identificar uma correlação entre as métricas, independente do ambiente.

7.3 Impacto da Mobilidade com LoS

Esta seção avalia o impacto do CET no desempenho do Wi-Fi Direct em um cenário de mobilidade e condições LoS. Em um cenário com mobilidade, o desempenho do Wi-Fi Direct pode ser impactado, por exemplo, pelo Doppler *shift*, que pode levar à perda de quadros de controle trocados durante o estabelecimento da conexão. Isto pode elevar o CET e reduzir o tempo de contato entre os dispositivos. Como descrito na Seção 1.1, com base em uma aplicação de prevenção de colisão entre veículo e pedestre, um CET longo pode fazer com que a mensagem de segurança não seja recebida em tempo no veículo, diminuindo a janela de atuação da aplicação. Mais uma vez, ao contrário da análise por trechos de 10 m, no cenário atual o cálculo da PDR e do PIR é feito a cada 20 m. Isto é feito com base na transmissão contínua, após o estabelecimento da conexão, de mensagens de

segurança feita pelo pedestre para o veículo enquanto este último se locomove em direção ao primeiro. A Figura 7.4 apresenta a PDR e o PIR obtidos, nos experimentos reais e simulações, para as velocidades do veículo de 20 km/h, 60 km/h, e 100 km/h.

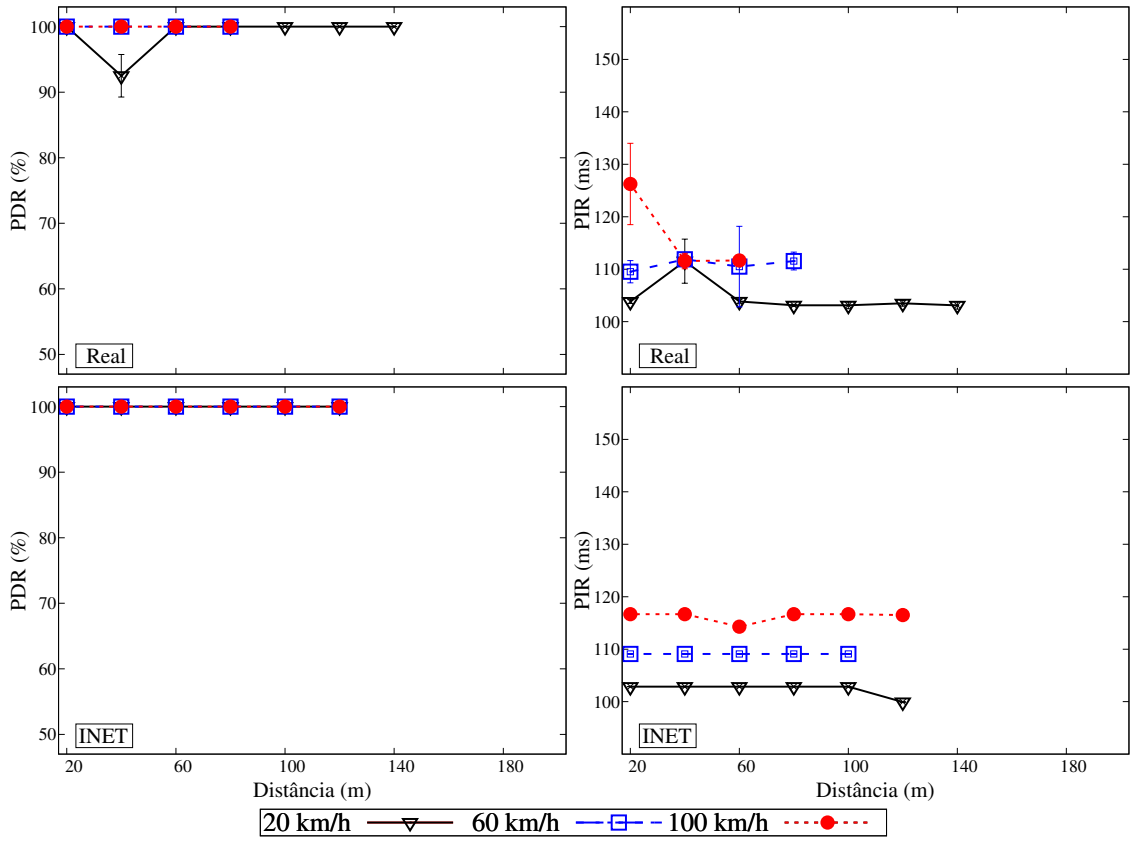

Figura 7.4: Impacto da mobilidade em condições com LoS com relação à PDR e ao PIR.

Nos experimentos reais, os resultados da PDR demonstram o impacto que um longo CET no Wi-Fi Direct pode impor em um cenário com mobilidade. Conforme fora demonstrado na Seção 7.2, na avaliação do cenário sem mobilidade, é possível receber mensagens de segurança até 150 m com PDR $\geq$60%. No cenário atual, com exceção dos resultados obtidos enquanto o veículo se locomoveu à 20 km/h, a distância máxima na qual o pedestre conseguiu estabelecer uma conexão com o veículo – sendo capaz de transmitir mensagens de segurança para o mesmo – está entre 60 m e 80 m, à 60 km/h e 100 km/h. Em distâncias superiores ao trecho que corresponde à distância entre 60 m e 80 m, a PDR é sempre 0. Em condições de baixa mobilidade, como à 20 km/h, a conexão é estabelecida a partir do trecho que corresponde à distância entre 120 m e 140 m. Neste caso, a PDR é sempre $\geq$90% a partir deste trecho. É importante ressaltar que, especialmente em condições de alta mobilidade, o total de mensagens de segurança transmitidas/recebidas em um trecho de 20 m pode ser muito pequeno. Por exemplo, em alguns casos, a PDR de 100% em um trecho de 20 m pode se referir a somente algumas mensagens de segurança que foram corretamente transmitidas/recebidas no dado trecho. Além disso, usando como exemplo os resultados obtidos à 60 km/h e 100 km/h, estes não indicam, necessariamente, que será

possível estabelecer uma conexão entre pedestre e veículo a uma distância de 80 m. Como os resultados se referem ao trecho entre 60 m e 80 m, esta distância pode ser a mínima para o trecho em questão (60 m). O mesmo pode acontecer em condições NLoS. Mesmo que aparentemente seja possível receber mensagens em uma distância de até 20 m, tais mensagens – às vezes apenas uma – podem ser recebidas com o veículo localizado a apenas 1 m de distância do pedestre, o que inviabilizaria completamente a frenagem. Por fim, como mencionado na Seção 6.2, também vale a pena destacar que o cálculo da distância entre pedestre e veículo pode conter erros devido à baixa precisão do GPS embarcado nos *smartphones*, que pode chegar a 10 m [41, 131].

Baseado no que foi feito por Won *et al.* em [68], por meio da transmissão de mensagens de segurança contendo dados cinemáticos, é possível calcular o risco de colisão entre pedestre e veículo com base no tempo que ainda resta para o veículo alcançar o pedestre. Este tempo pode ser calculado com base na soma: (1) do tempo de reação do motorista após a aplicação receber a mensagem de segurança, detectar o risco de colisão e acionar um alarme; e (2) do tempo para parar o veículo após o motorista, tendo compreendido o alerta, iniciar o processo de frenagem. Esses parâmetros são afetados, por exemplo, pela velocidade que o veículo se encontrava no momento do acionamento dos freios, pela capacidade cognitiva do motorista, e pela condição de pneus, freios e estrada. Assim, com base no tempo para parar o veículo completamente após a recepção da mensagem de segurança, a distância percorrida pode ser calculada com base na Equação 7.1:

$$D_{total} = d_{reacao} + d_{frenagem} = v_{veiculo}.t_{reacao} + \frac{v_{veiculo}^2}{2\mu g}, \tag{7.1}$$

onde d_{reacao} é a distância percorrida pelo veículo durante o tempo de reação do motorista ao alarme acionado pela aplicação de prevenção de colisão, e $d_{frenagem}$ é a distância percorrida pelo veículo após o motorista iniciar o processo de frenagem, com base na velocidade do veículo ($v_{veiculo}$), coeficiente de atrito da estrada (μ), aceleração da gravidade (g) e tempo de reação do motorista (t_{reacao}).

No trabalho de Won *et al.* [68], além do tempo de reação do motorista e do tempo para parar o veículo por completo após o acionamento dos freios, os autores também consideraram no cálculo do risco de colisão a latência fim-a-fim com base no RTT, obtido através da troca de mensagens entre pedestre e veículo. Nesta tese, no lugar do RTT (não medido), foi considerado um atraso de 100 ms. Apesar da latência fim-a-fim do Wi-Fi Direct não ser avaliada, assume-se que a definição do atraso de 100 ms seja suficiente. Por exemplo, nos experimentos realizados por Su *et al* [38], com *smartphones* implementando o modo *ad-hoc*, o RTT obtido foi de ≈30 ms. Com relação ao tempo de reação do motorista, foi considerado um tempo de 1 s, com base na definição deste parâmetro por Renda *et al.* [23]. Por fim, g foi definido como 9,81 m/s^2, e dado que as medições foram realizadas em boas condições climáticas, μ foi definido como 0,8, baseado no asfalto seco [137]. Dado que o

veículo se locomove à 20 km/h, 60 km/h, e 100 km/h, com base na Equação 7.1, a distância percorrida pelo veículo entre a transmissão da mensagem de segurança pelo pedestre até sua parada completa após o acionamento dos freios seria de, aproximadamente, 8 m, 36 m e 80 m, respectivamente. Pelos resultados da Figura 7.4, uma colisão entre veículo e pedestre poderia ser evitada à 20 km/h e 60 km/h. Por outro lado, à 100 km/h, existe o risco de colisão. Entretanto, no geral, o limite de velocidade máxima em áreas urbanas na maioria dos países não excede 60 km/h [138]. Neste sentido, em condições específicas de mobilidade, LoS e interferência, o Wi-Fi Direct pode ser viável para permitir a operação de uma aplicação de segurança baseada na prevenção de colisões entre veículos e usuários vulneráveis das vias, em situações envolvendo a travessia em faixa destes últimos.

Os resultados das simulações do INET indicam que o alcance obtido à 20 km/h é menor nas simulações em comparação aos experimentos reais. Além disso, nas simulações, o aumento da velocidade do veículo não impacta o estabelecimento da conexão, conforme ocorre nos experimentos reais. Como é possível observar na Figura 7.4, o estabelecimento da conexão e, consequentemente, a transmissão das mensagens de segurança, ocorre a partir do trecho que corresponde à distância entre 100 m e 120 m, independente da velocidade. A partir deste trecho, a PDR é sempre 100%. Diferente dos experimentos reais, pelos resultados das simulações a colisão poderia ser evitada em qualquer condição de mobilidade. Isto pode estar associado à não aplicação, nas simulações, de um modelo de propagação que considere o impacto da mobilidade do nó na comunicação, por exemplo, devido ao Doppler *shift*. Deste modo, nas simulações, o comportamento dos experimentos reais não foi observado. Quanto ao PIR, com exceção dos resultados à 20 km/h nos experimentos reais, nos demais cenários e nas simulações não foi possível calcular a correlação desta métrica com a PDR devido a esta última ser 100% em todos os trechos de 20 m. À 20 km/h, é possível obter uma correlação negativa muito forte entre PDR e PIR (-0,99438), de acordo com o Coeficiente de Pearson. Apesar da diferença em termos de valores, um comportamento comum nos experimentos reais e nas simulações diz respeito ao leve aumento do PIR conforme empregam-se velocidades mais altas no veículo – mais evidente nas simulações. Apesar deste leve aumento, no geral o PIR não se mostrou muito superior à taxa de geração de 100 ms das mensagens de segurança.

7.4 Impacto da Mobilidade com NLoS

Por fim, esta seção avalia o impacto do CET no desempenho do Wi-Fi Direct em um cenário de mobilidade e condições NLoS. Novamente, o veículo se locomove à 20 km/h, 60 km/h, e 100 km/h em direção ao pedestre. Entretanto, desta vez, um veículo de médio porte (uma caminhonete 4x4) que não possui um dispositivo Wi-Fi Direct, é posicionado de forma estática entre o veículo e o pedestre com o intuito de gerar uma obstrução física ao sinal de rádio. Como no cenário anterior, o cálculo da PDR e do PIR é feito a cada 20 m,

com base na transmissão contínua de mensagens de segurança, feita pelo pedestre após o estabelecimento da conexão com o GO. A Figura 7.5 apresenta a PDR e o PIR obtidos, nos ambientes real e simulado.

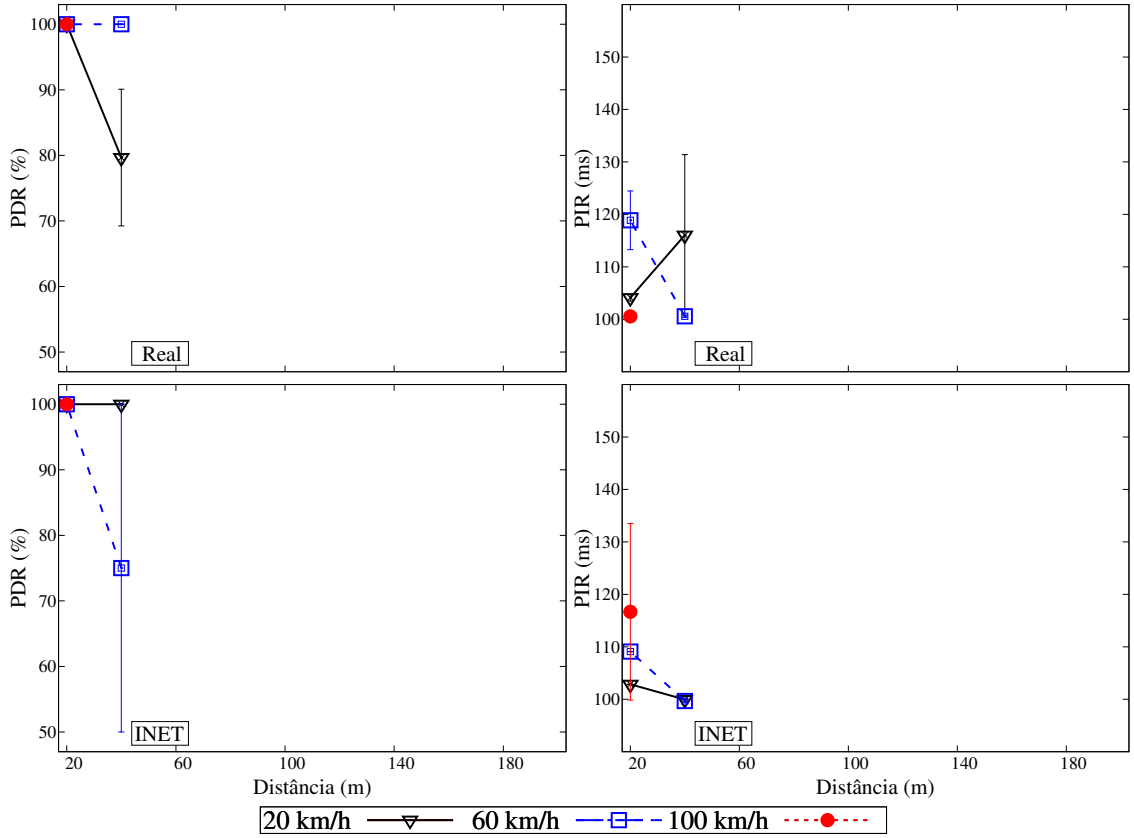

Figura 7.5: Impacto da mobilidade em condições com NLoS com relação à PDR e ao PIR.

Conforme é possível observar, nos experimentos reais, é nítida a diminuição da PDR em comparação ao cenário anterior, com LoS. No cenário atual, a forte atenuação do sinal de rádio gerada pelo obstáculo faz com que, na melhor das hipóteses, o pedestre conclua o estabelecimento da conexão e inicie a transmissão das mensagens de segurança apenas no trecho que compreende a distância entre 20 m e 40 m, com o veículo se locomovendo à 20 km/h ou 60 km/h. Este resultado indica que, em condições NLoS, um longo CET pode tornar o uso do Wi-Fi Direct no ambiente veicular ainda mais proibitivo, já que o tempo para transmissão das mensagens e atuação da aplicação de prevenção de colisões após a recepção da mensagem pode ser insuficiente. Pelas distâncias calculadas no cenário anterior para parar o veículo por completo após a recepção do alerta (8 m, 36 m, e 80 m), os resultados indicam que, em condições NLoS, existe um grande risco de que uma colisão entre veículo e pedestre não possa ser evitada à 60 km/h e 100 km/h. Apesar das diferenças em termos de valores, especialmente com relação à PDR obtida à 20 km/h e 60 km/h no trecho entre 20 m e 40 m, o mesmo comportamento pode ser visto nas simulações do INET, indicando que o efeito do obstáculo é bem modelado pelo simulador.

Com relação ao PIR, nos experimentos reais é possível obter uma correlação negativa muito forte entre esta métrica e a PDR apenas à 20 km/h (-1). Nas simulações do INET, uma correlação positiva muito forte ocorre apenas à 60 km/h (1). Nos demais casos, não é possível calcular a correlação. Nas simulações, ainda é possível perceber um leve compromisso entre o uso de velocidades mais altas e o aumento do PIR. Novamente, em ambos os ambientes o PIR não se mostrou muito superior à taxa de geração das mensagens de segurança.

7.5 Transmissão Baseada no *Beacon-Stuffing*

Os resultados anteriores indicam que, em ambientes realistas e condições NLoS, o uso do Wi-Fi Direct como uma tecnologia de rádio alternativa ao IEEE 802.11p é desafiador mesmo em cenários específicos, devido ao CET. Assim, soluções que eliminem ou minimizem o CET são necessárias para permitir usar o Wi-Fi Direct no ambiente veicular. Deste modo, esta seção avalia um método simples de transmissão para Wi-Fi Direct baseado na técnica de *beacon-stuffing*. Conforme descrito na Subseção 6.3, a avaliação consiste de um pequeno experimento real, além de simulações executadas no INET. No experimento real, cinco rodadas foram executadas. Com base nos resultados da mediana das cinco rodadas, uma PDR de 99% é obtida para o cenário de avaliação descrito na Subseção 6.3. Ou seja, no experimento real, o receptor foi capaz de mostrar a modificação do nome do dispositivo Wi-Fi Direct em 99% das vezes. Os resultados da mediana também indicaram um PIR de $\approx$1 s, similar à taxa de modificação do nome do dispositivo Wi-Fi Direct.

Quanto à avaliação feita no INET, os resultados dizem respeito à quantidade de mensagens de segurança recebidas em cada trecho de 20 m, com base nas mensagens transmitidas pelo pedestre posicionado mais próximo do obstáculo, a 5 m do mesmo. Na avaliação, tal pedestre simula aquele que tenta atravessar pela faixa sem estar ciente do veículo que se aproxima, uma vez que seu campo visual é obstruído pelo obstáculo. Conforme mencionado na Subseção 6.3, desta vez todos os pedestres atuam como GO de um grupo P2P autônomo. Todos os pedestres – o GO posicionado mais próximo do obstáculo e outros atuando como nós geradores de interferência – estão posicionados à 3 m de distância um do outro. A Figura 7.6 apresenta o total de recepções pelo veículo no cenário que avalia as transmissões com Wi-Fi Direct baseada no *beacon-stuffing* em condições NLoS e interferência. Dez rodadas são realizadas para cada permutação de cenário.

Dado que através do *beacon-stuffing* não é necessário o estabelecimento da conexão para trocar dados, com exceção dos resultados obtidos com oito transmissores simultâneos, é possível observar a recepção, no veículo, de pelo menos uma mensagem simbolizando a posição e velocidade do pedestre com pelo menos 100 m de distância entre os nós, à 20 km/h e 60 km/h. Dada a distância calculada para parar o veículo completamente após o acionamento do alarme (8 m, 36 m, e 80 m), a recepção de um *beacon* ou *probe response*

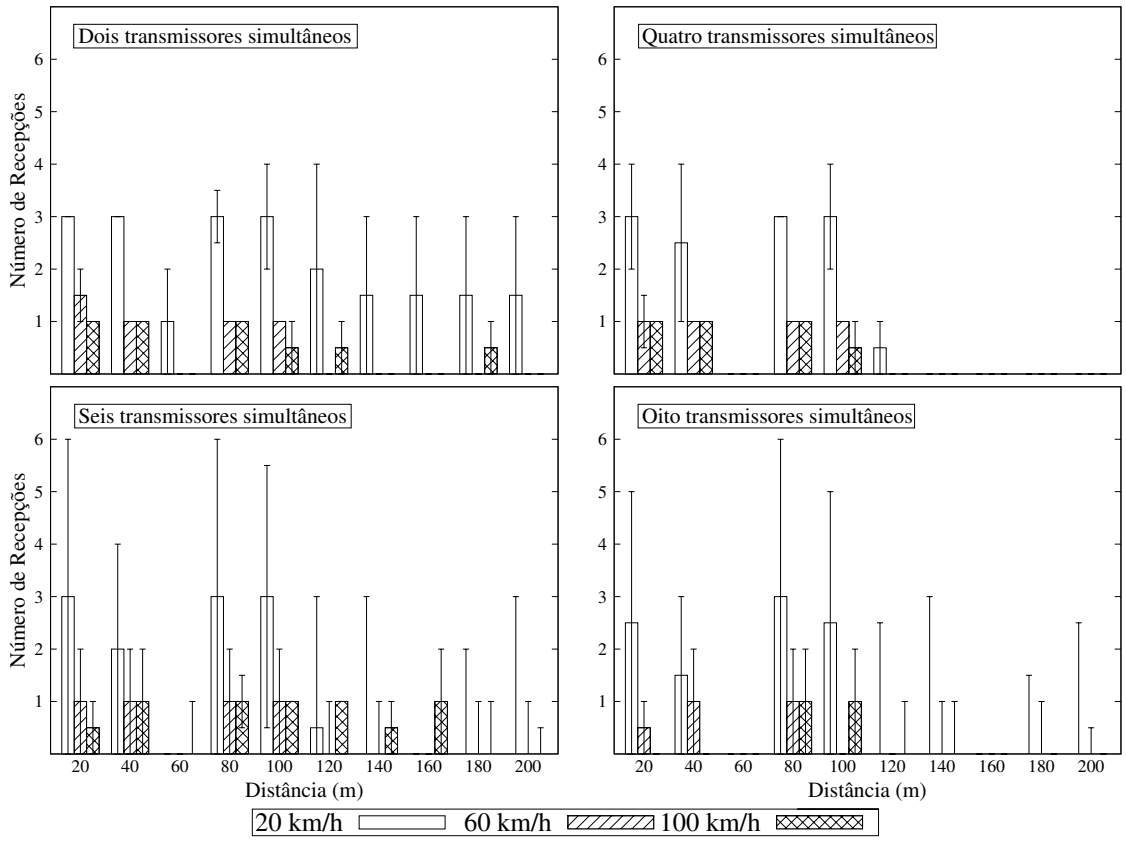

Figura 7.6: Transmissão de dados via Wi-Fi Direct baseado no *beacon-stuffing*.

carregando os dados cinemáticos do pedestre (representados nas simulações pela alteração do ID/contador da mensagem) neste ponto da via permitiria que o motorista tomasse conhecimento da presença do pedestre, iniciando o processo de frenagem e parando o veículo a tempo, de forma a evitar a colisão. Como a recepção de apenas uma mensagem de segurança é suficiente para calcular o risco de colisão entre veículo e pedestre [67], o método de transmissão do Wi-Fi Direct baseado no *beacon-stuffing* poderia minimizar o impacto causado por um longo CET, especialmente em condições NLoS.

Concluída a apresentação dos resultados que analisam a viabilidade do Wi-Fi Direct no ambiente veicular, em seguida serão mostradas as conclusões obtidas com base no que foi mostrado nesta tese, bem como as sugestões de direções futuras.

Capítulo 8

Conclusões

Esta tese avaliou o desempenho do IEEE 802.11p tendo como base os resultados de uma aplicação para transmissão periódica, e em *broadcast*, de BSMs, base para aplicações de segurança em redes veiculares. Por meio de experimentos reais usando OBUs e RSUs comerciais, o desempenho do padrão foi avaliado em cenários de comunicação V2I e V2V, variando a distância entre os nós, a velocidade do veículo, e as diferentes taxas de dados suportadas. Como métricas de desempenho, foram usadas a PDR e o PIR. Uma comparação dos resultados obtidos nos experimentos reais com aqueles obtidos em simulações executadas no NS-3/PhySim e Veins/MiXiM também foi realizada. O objetivo foi analisar a capacidade destes simuladores em reproduzir o comportamento obtido nos testes práticos. No geral, apesar das diferenças em termos de valores absolutos, os resultados indicam que os simuladores são capazes de reproduzir tal comportamento. Por exemplo, quanto à redução da PDR – e aumento do PIR – com a distância/uso de taxas mais altas, e quanto ao impacto negligenciável da mobilidade na comunicação. Entretanto, a forma das curvas no NS-3/PhySim se mostrou mais próxima daquela nos experimentos reais. Assumindo que a definição do ganho de antena na configuração das simulações está correta, pelos resultados, uma revisão da modelagem deste ganho no NS-3/PhySim pode ser necessária. Igualmente, um novo modelo de desvanecimento em pequena-escala, específico para ambientes com propagação com LoS predominante pode ser necessário. Conforme o nosso conhecimento, o MiXiM não possui este modelo e a modificação do parâmetro `fadingPaths` do modelo `JakesFading` pode não ser apropriada para refletir as condições LoS dos experimentos reais desta tese.

Esta tese também analisou a viabilidade do Wi-Fi Direct no ambiente veicular. Apesar das limitações, para alguns cenários e em condições específicas o Wi-Fi Direct pode ser viável como opção ao IEEE 802.11p. Por exemplo, para aplicações que previnam colisões entre veículos e usuários vulneráveis das vias. Em experimentos reais usando *smartphones* comerciais, a viabilidade do Wi-Fi Direct foi analisada tendo como base um cenário de comunicação V2P. Tal cenário é baseado em uma situação do mundo real, onde pedestres e veículos podem provocar colisões devido à travessias inapropriadas, feitas sem

a devida autorização semafórica. Em tal cenário, foram variadas a distância entre os nós e a velocidade do veículo. Um obstáculo também é considerado a fim de tornar a avaliação mais realista e permitir condições NLoS. Novamente, PDR e PIR foram usadas como métricas. Uma diferença entre os resultados do IEEE 802.11p e do Wi-Fi Direct é que, no primeiro, as transmissões de BSMs não são orientadas à conexão. Assim, a PDR cresceu gradualmente, conforme diminuiu a distância entre os nós. Já no Wi-Fi Direct, como a transmissão *unicast* das mensagens só ocorreu após o estabelecimento da conexão, na maioria dos casos a PDR foi $\approx$100%. Se a conexão foi estabelecida com sucesso, entende-se que os veículos estão suficientemente próximos, de tal forma que a força do sinal de rádio permite que o pacote seja detectado/decodificado com sucesso. Os resultados dos experimentos reais indicaram que, em condições específicas de mobilidade, LoS e interferência, o Wi-Fi Direct poderia suportar uma aplicação que previne colisões entre veículos e pedestres, durante a travessia de faixa destes últimos. Como no IEEE 802.11p, os resultados dos experimentos reais foram comparados aos obtidos em simulações executadas no INET, visando analisar a capacidade de mimetização do modelo de simulação. No geral, o simulador foi capaz de reproduzir o comportamento dos experimentos reais em relação à PDR e ao PIR, apesar das esperadas diferenças em termos de valores absolutos. Um método de transmissão baseado em *beacon-stuffing* também foi avaliado. No método, o campo de 32 bytes do nome do dispositivo é modificado pelos dados cinemáticos da mensagem de segurança transmitida pelo pedestre. Os resultados indicaram que este método pode ser uma opção especialmente em condições NLoS, já que aumentou a distância de recepção das mensagens nestas condições.

8.1 Publicações

Nesta seção, estão listadas as publicações que foram obtidas como resultado do desenvolvimento desta tese.

Almeida, T. T., Gomes, L. C., Ortiz, F. M., Ribeiro Júnior, J. G. and Costa, L. H. M. K. "Análise de Desempenho do IEEE 802.11p: Simulações versus Experimentos Reais", in *XXXVI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos* – SBRC 2018, Campos do Jordão, SP, Brazil, Maio de 2018.

Almeida, T. T., Gomes, L. C., Ortiz, F. M., Ribeiro Júnior, J. G. and Costa, L. H. M. K. "IEEE 802.11p Performance Evaluation: Simulations vs. Real Experiments", in *21st IEEE International Conference on Intelligent Transportation Systems* – ITSC 2018, Maui, Hawaii, USA, Novembro de 2018.

Almeida, T. T., Gomes, L. C., Ortiz, F. M., Ribeiro Júnior, J. G. and Costa, L.

H. M. K. “A Comparative Analysis of Vehicular Communications in NS-3 and Veins”, in *IEEE Transactions on Intelligent Transportation Systems*, ISSN 1558-0016, DOI 10.1109/TITS.2020.3014840, English, A4 size, 10 p., Agosto de 2020.

Almeida, T. T., Ribeiro Júnior, J. G., Campista, M. E. M. and Costa, L. H. M. K. “Uma Análise de Desempenho do Wi-Fi Direct para Comunicações Veículo-Pedestre”, in *XXXVIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos* – SBRC 2020, Rio de Janeiro, RJ, Brazil, Dezembro de 2020.

Almeida, T. T., Ribeiro Júnior, J. G., Campista, M. E. M. and Costa, L. H. M. K. “Wi-Fi Direct Performance Evaluation for V2P Communications”, in *Journal of Sensor and Actuator Networks*, vol. 9 (2), 28, MDPI, ISSN: 2224-2708, DOI 10.3390/jsan9020028, English, A4 size, 20 p., Junho de 2020.

8.2 Trabalhos Futuros

Tentativas de vislumbrar o uso do Wi-Fi Direct em determinados cenários de redes veiculares foram feitas, analisando a possibilidade de uso desta tecnologia: (1) integrada ao IEEE 802.11p, de forma a permitir uma rotina de *beaconing* adaptativo visando diminuir a carga de *beacons* no CCH; (2) como suporte a aplicações do tipo *Emergency Electronic Brake Lights*, usando *beacon-stuffing*; e (3), para permitir a operação de aplicações do tipo *See-Through*. Como trabalhos futuros, no contexto da análise da viabilidade do Wi-Fi Direct para cenários específicos de uma rede veicular, entende-se que uma opção viável é desenvolver uma aplicação para Android do tipo *See-Through*, que visa estender o campo visual de motoristas em cenários de ultrapassagem, via transmissão de um fluxo de vídeo em tempo real. Este tipo de aplicação é especialmente útil quando a visão para a direção oposta da via está obstruída por um veículo de grande porte. Neste sentido, o veículo de grande porte, através de um *smartphone* posicionado no seu vidro dianteiro atuando como servidor do fluxo de vídeo, será responsável por capturar e transmitir a imagem da via usando o Wi-Fi Direct para o *smartphone* do veículo que deseja fazer a ultrapassagem, atuando como cliente deste fluxo. A conexão cliente-servidor entre os dispositivos será realizada com base na conexão, via Wi-Fi Direct, do cliente do fluxo de vídeo a um grupo P2P autônomo, criado e mantido pelo servidor do fluxo. Para este caso, a avaliação do protótipo da aplicação será feita em cenários com condições LoS e NLoS, com e sem interferência e com transmissão do tipo V2V. Como métricas de avaliação, têm-se a PDR, a latência de rede e a latência fim-a-fim. A latência, por sinal, é uma importante métrica a ser considerada, uma vez que a decisão sobre ultrapassar ou não é baseada no vídeo que o motorista está vendo. Em termos da decisão pela ultrapassagem nos casos onde não há, baseado no vídeo, veículo vindo na direção oposta, é necessário que a latência fim-a-fim

seja $\leq$100 ms, conforme definido no Consórcio VSC [19, 84]. Por outro lado, em termos da decisão pela não ultrapassagem nos casos onde há, baseado no vídeo, veículo vindo na direção oposta, entende-se que a latência fim-a-fim possa ser superior à 100 ms. De acordo com Wang *et al.* [139], cerca de 60% dos acidentes poderiam ser evitados se os motoristas recebessem um alerta com pelo menos meio segundo de antecedência [91]. Por exemplo, se a latência fim-a-fim obtida por uma aplicação de transmissão de fluxo de vídeo em tempo real para auxílio a ultrapassagem, rodando em cima do Wi-Fi Direct, for inferior ou próxima à 500 ms, a análise poderia indicar que o Wi-Fi Direct pode ser viável neste cenário específico. A investigação de protocolos, bibliotecas, *players* e da configuração ideal de parâmetros que auxiliem no aumento da PDR e na redução da latência fim-a-fim caracterizará esta etapa futura da pesquisa.

Além disso, também é uma opção avaliar o desempenho do Wi-Fi Aware (NAN – *Neighbour Awareness Networking*). Devido ao aparente processo de troca de dados mais simplificado em comparação ao Wi-Fi Direct, a ideia é analisar o uso desta tecnologia de rádio no suporte a aplicações de segurança em redes veiculares usando *smartphones*. De acordo com o Wi-Fi Alliance[1], um dos usos emergentes desta tecnologia está relacionado com a transmissão, por veículos autônomos e remotamente controlados, de dados como coordenadas de GPS, altitude, direção de viagem, entre outros. Além disso, diferente do Wi-Fi Direct, o Wi-Fi Aware não requer que um nó atue como GO. Conexões P2P podem ser criadas de forma dinâmica e descentralizada, tornando o uso do Wi-Fi Aware indicado para ambientes de alta mobilidade. Ainda conforme o Wi-Fi Alliance, o Wi-Fi Aware é baseado no modelo *publish/subscribe* de serviços, cuja descoberta pode opcionalmente ser feita via BLE para menor consumo de energia. A eficiência energética também pode ser obtida via sincronização de tempo entre os dispositivos, estabelecendo períodos comuns de atividade/inatividade. Além disso, o envio de dados via *multicast* também é suportado. Como o Wi-Fi Direct, o Wi-Fi Aware possui um alcance similar ao do Wi-Fi, com frequência de operação de 2,4 GHz e 5 GHz, e atua no canal 6. Conforme a visão geral da API do Wi-Fi Aware para Android[2], concluída a descoberta de serviços, o assinante de um dado serviço pode enviar uma mensagem curta (255 bytes) ou estabelecer uma conexão com o emissor do serviço descoberto. Também é possível usar a API Wi-Fi RTT do Android para limitar a descoberta de serviços do Wi-Fi Aware em uma dada área geográfica, baseado na distância medida entre os dispositivos. Para Android, o Wi-Fi Aware está disponível desde a versão 8.0 (*Oreo*). Entretanto, é necessário que o *hardware* do *smartphone* seja compatível. Neste sentido, experimentos reais serão realizados de forma a avaliar o desempenho do Wi-Fi Aware sob diferentes condições. Baseado na caracterização da tecnologia, uma das etapas futuras da pesquisa será o desenvolvimento de um modelo de simulação compatível com o Wi-Fi Aware para o *framework* INET, tal qual foi feito por Iskounen *et al.*

[1] https://www.wi-fi.org/discover-wi-fi/wi-fi-aware

[2] https://developer.android.com/guide/topics/connectivity/wifi-aware?hl=pt-br

para o Wi-Fi Direct em [63], o que permitirá a avaliação da tecnologia em larga-escala.

Referências Bibliográficas

[1] ALVES, R. D. S., CAMPBELL, I. D. V., COUTO, R. D. S., et al. "Redes Veiculares: Princípios, Aplicações e Desafios", *Minicursos do Simpósio Brasileiro de Redes de Computadores, SBRC*, pp. 17–24, 2009.

[2] JEONG, S., BAEK, Y., SON, S. H. "A Hybrid V2X System for Safety-Critical Applications in VANET". In: *2016 IEEE 4th International Conference on Cyber-Physical Systems, Networks, and Applications (CPSNA)*, pp. 13–18, 2016. doi: 10.1109/CPSNA.2016.11.

[3] CAMPS-MUR, D., GARCIA-SAAVEDRA, A., SERRANO, P. "Device-to-Device Communications with Wi-Fi Direct: Overview and Experimentation", *IEEE Wireless Communications*, v. 20, n. 3, pp. 96–104, 2013. doi: 10.1109/MWC.2013.6549288.

[4] NETO, J. B. P., GOMES, L. C., CASTANHO, E. M., et al. "Um Algoritmo para Cálculo de Distância Segura de Frenagem para Prevenção de Colisão Dianteira em Redes Veiculares". In: *XXI Workshop de Gerência e Operaçao de Redes e Serviços*, 2016.

[5] SOARES, R., GALENO, S., SOARES, A. "Simulação de Redes Veiculares", 2016.

[6] WORLD HEALTH ORGANIZATION. "Global Status on Road Safety". 2018. Disponível em: <https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries>. Acesso em Jan. 2021.

[7] MINISTÉRIO DA SAÚDE. "Mortalidade Brasil - Causa CID-BR-10: . 104 Acidentes de Transporte". 2019. Disponível em: <http://tabnet.datasus.gov.br/cgi/tabcgi.exe?sim/cnv/obt10uf.def>. Acesso em Ago. 2021.

[8] GOVERNO DO BRASIL. "Brasil registra queda em número de mortes no trânsito". 2020. Disponível em: <https://www.gov.br/pt-br/noticias/transito-e-transportes/2020/09/brasil-registra-queda-em-numero-de-mortes-no-transito>. Acesso em Jan. 2021.

[9] SINDICATO NACIONAL DA INDÚSTRIA DE COMPONENTES PARA VEÍCULOS AUTOMOTORES - SINDIPEÇAS E ASSOCIAÇÃO BRASILEIRA DA INDÚSTRIA DE AUTOPEÇAS – ABIPEÇAS. "Relatório da Frota Circulante - Edição 2021". 2021. Disponível em: <https://www.sindipecas.org.br/sindinews/Economia/2021/RelatorioFrotaCirculante_Marco_2021.pdf>. Acesso em Ago. 2021.

[10] AUTO ESPORTE. "Frota de carros no Brasil é a mais velha em 25 anos". 2021. Disponível em: <https://autoesporte.globo.com/carros/usados-e-seminovos/noticia/2021/03/frota-de-carros-no-brasil-e-a-mais-velha-em-25-anos.ghtml>. Acesso em Ago. 2021.

[11] INTERNATIONAL ORGANIZATION OF MOTOR VEHICLE MANUFACTURERS. "World Vehicles in Use - All Vehicles". 2015. Disponível em: <https://www.oica.net/wp-content/uploads/Total_in-use-All-Vehicles.pdf>. Acesso em Jan. 2021.

[12] ZEADALLY, S., GUERRERO, J., CONTRERAS, J. "A Tutorial Survey on Vehicle-to-Vehicle Communications", *Telecommunication Systems*, v. 73, n. 3, pp. 469–489, 2020.

[13] CARS GUIDE. "How many cars are in the world?" 2018. Disponível em: <https://www.carsguide.com.au/car-advice/how-many-cars-are-there-in-the-world-70629>. Acesso em Jan. 2021.

[14] INRIX ANALYTICS. "INRIX 2019 Global Traffic Scorecard". 2019. Disponível em: <https://inrix.com/scorecard/>. Acesso em Jan. 2021.

[15] INRIX RESEARCH. "US Traffic Hotspots: Measuring the Impact of Congestion in the United States". 2017. Disponível em: <https://www2.inrix.com/us-traffic-hotspot-study-2017>. Acesso em Jan. 2021.

[16] AFRIN, T., YODO, N. "A Survey of Road Traffic Congestion Measures towards a Sustainable and Resilient Transportation System", *Sustainability*, v. 12, n. 11, 2020. ISSN: 2071-1050. doi: 10.3390/su12114660. Disponível em: <https://www.mdpi.com/2071-1050/12/11/4660>.

[17] AFTABUZZAMAN, M. "Measuring Traffic Congestion-a Critical Review". In: *30th Australasian Transport Research Forum*, pp. 1–16, 2007.

[18] SASSI, A., CHARFI, F., KAMOUN, L., et al. "Experimental Measurement for Vehicular Communication Evaluation using OBU ARADA System". In: *2015*

International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 1358–1364, 2015. doi: 10.1109/IWCMC.2015.7289280.

[19] HARTENSTEIN, H., LABERTEAUX, L. P. "A Tutorial Survey on Vehicular Ad Hoc Networks", *IEEE Communications Magazine*, v. 46, n. 6, pp. 164–171, 2008. doi: 10.1109/MCOM.2008.4539481.

[20] SHARMA, S., KAUSHIK, B. "A Survey on Internet of Vehicles: Applications, Security Issues & Solutions", *Vehicular Communications*, v. 20, pp. 100182, 2019. ISSN: 2214-2096. doi: https://doi.org/10.1016/j.vehcom.2019.100182. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2214209619302293>.

[21] BILA, C., SIVRIKAYA, F., KHAN, M. A., et al. "Vehicles of the Future: A Survey of Research on Safety Issues", *IEEE Transactions on Intelligent Transportation Systems*, v. 18, n. 5, pp. 1046–1065, 2017. doi: 10.1109/TITS.2016.2600300.

[22] AL-SULTAN, S., AL-DOORI, M. M., AL-BAYATTI, A. H., et al. "A Comprehensive Survey on Vehicular Ad Hoc Network", *Journal of Network and Computer Applications*, v. 37, pp. 380–392, 2014. ISSN: 1084-8045. doi: https://doi.org/10.1016/j.jnca.2013.02.036. Disponível em: <https://www.sciencedirect.com/science/article/pii/S108480451300074X>.

[23] RENDA, M. E., RESTA, G., SANTI, P., et al. "IEEE 802.11p VANets: Experimental Evaluation of Packet Inter-Reception Time", *Computer Communications*, v. 75, pp. 26–38, 2016. ISSN: 0140-3664. doi: https://doi.org/10.1016/j.comcom.2015.06.003. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0140366415002182>.

[24] ARENA, F., PAU, G. "An Overview of Vehicular Communications", *Future Internet*, v. 11, n. 2, pp. 27, 2019.

[25] JI, B., ZHANG, X., MUMTAZ, S., et al. "Survey on the Internet of Vehicles: Network Architectures and Applications", *IEEE Communications Standards Magazine*, v. 4, n. 1, pp. 34–41, 2020. doi: 10.1109/MCOMSTD.001.1900053.

[26] JIANG, D., DELGROSSI, L. "IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments". In: *VTC Spring 2008 - IEEE Vehicular Technology Conference*, pp. 2036–2040, 2008. doi: 10.1109/VETECS.2008.458.

[27] "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)*, pp. 1–51, 2010. doi: 10.1109/IEEESTD.2010.5514475.

[28] ANWAR, W., FRANCHI, N., FETTWEIS, G. "Physical Layer Evaluation of V2X Communications Technologies: 5G NR-V2X, LTE-V2X, IEEE 802.11bd, and IEEE 802.11p". In: *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, pp. 1–7, 2019. doi: 10.1109/VTCFall.2019.8891313.

[29] COHDA WIRELESS. "Cohda wireless V2X tech gives germain firefighters the green light". 2021. Disponível em: <https://cohdawireless.com/cohda-wireless-v2x-tech-gives-german-firefighters-the-green-light>. Acesso em Jan. 2021.

[30] COHDA WIRELESS. "Australia's largest connected vehicle trial a model for others to follow". 2021. Disponível em: <https://cohdawireless.com/australias-largest-connected-vehicle-trial-a-model-for-others-to-follow/>. Acesso em Jan. 2021.

[31] COHDA WIRELESS. "Connected vehicle technology is coming to the streets of New York City". 2021. Disponível em: <https://cohdawireless.com/connected-vehicle-technology-is-coming-to-the-streets-of-new-york-city>. Acesso em Jan. 2021.

[32] COHDA WIRELESS. "Cohda selected for Berlin test-field". 2021. Disponível em: <https://cohdawireless.com/cohda-selected-for-berlin-test-field/>. Acesso em Jan. 2021.

[33] RHOADES, B. B., CONRAD, J. M. "A Survey of Alternate Methods and Implementations of an Intelligent Transportation System". In: *SoutheastCon 2017*, pp. 1–8, 2017. doi: 10.1109/SECON.2017.7925303.

[34] SINGH, P. K., NANDI, S. K., NANDI, S. "A Tutorial Survey on Vehicular Communication State of the Art, and Future Research Directions", *Vehicular Communications*, v. 18, pp. 100164, 2019. ISSN: 2214-2096. doi: https://doi.org/10.1016/j.vehcom.2019.100164. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2214209618300901>.

[35] SIEGEL, J. E., ERB, D. C., SARMA, S. E. "A Survey of the Connected Vehicle Landscape—Architectures, Enabling Technologies, Applications, and Development Areas", *IEEE Transactions on Intelligent Transportation Systems*, v. 19, n. 8, pp. 2391–2406, 2018. doi: 10.1109/TITS.2017.2749459.

[36] DEMMEL, S., GRUYER, D., RAKOTONIRAINY, A. "V2V/V2I Augmented Maps: State-of-the-Art and Contribution to Real-Time Crash Risk Assessment". In: Suggett, J. (Ed.), *Proceedings of the 20th Canadian Multidisciplinary Road Safety Conference*, Canadian Association of Road Safety Professionals, pp. 1–14, CD Rom, 2010. Disponível em: <https://eprints.qut.edu.au/39123/>.

[37] MIUCIC, R., BAI, S. "Performance of Aftermarket (DSRC) Antennas inside a Passenger Vehicle", *SAE International Journal of Passenger Cars - Electronic and Electrical Systems*, v. 4, n. 1, pp. 150–155, apr 2011. ISSN: 1946-4614. doi: https://doi.org/10.4271/2011-01-1031. Disponível em: <https://doi.org/10.4271/2011-01-1031>.

[38] SU, K., WU, H., CHANG, W., et al. "Vehicle-to-Vehicle Communication System through Wi-Fi Network Using Android Smartphone". In: *2012 International Conference on Connected Vehicles and Expo (ICCVE)*, pp. 191–196, 2012. doi: 10.1109/ICCVE.2012.42.

[39] MANAMPERI, W., SAMARASINGHE, T., DIAS, D. "Enhancing the Wi-Fi Direct Protocol for Data Communication in Vehicular Ad-hoc Networks". In: *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, pp. 812–817, 2018. doi: 10.1109/ITSC.2018.8569741.

[40] BALASUNDRAM, A., SAMARASINGHE, T., DIAS, D. "Performance Analysis of Wi-Fi Direct for Vehicular Ad-Hoc Networks". In: *2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pp. 1–6, 2016. doi: 10.1109/ANTS.2016.7947854.

[41] SEWALKAR, P., SEITZ, J. "Vehicle-to-Pedestrian Communication for Vulnerable Road Users: Survey, Design Considerations, and Challenges", *Sensors*, v. 19, n. 2, 2019. ISSN: 1424-8220. doi: 10.3390/s19020358. Disponível em: <https://www.mdpi.com/1424-8220/19/2/358>.

[42] STATISTA. "Global smartphone penetration rate as share of population from 2016 to 2020". 2021. Disponível em: <https://www.statista.com/statistics/203734/global-smartphone-penetration-per-capita-since-2005/>. Acesso em Jan. 2021.

[43] STATISTA. "Number of smartphone users worldwide from 2016 to 2021". 2021. Disponível em: <https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide>. Acesso em Jan. 2021.

[44] STATISTA. "Number of smartphone users by country as of September 2019 (in millions)*". 2021. Disponível em: <https://www.statista.com/statistics/748053/worldwide-top-countries-smartphone-users/>. Acesso em Jan. 2021.

[45] ZME SCIENCE. "Your smartphone is millions of times more powerful than the Apollo 11 guidance computers". 2020. Disponível em: <https://www.zmescience.com/science/news-science/smartphone-power-compared-to-apollo-432/>. Acesso em Jan. 2021.

[46] VERDICT. "How your smartphone could help power vital research projects". 2019. Disponível em: <https://www.verdict.co.uk/smartphone-processing-power/>. Acesso em Jan. 2021.

[47] VODAFONE. "Help with COVID-19 and cancer research". 2021. Disponível em: <https://www.vodafone.co.uk/mobile/dreamlab>. Acesso em Ago. 2021.

[48] WU, X., MIUCIC, R., YANG, S., et al. "Cars Talk to Phones: A DSRC Based Vehicle-Pedestrian Safety System". In: *2014 IEEE 80th Vehicular Technology Conference (VTC2014-Fall)*, pp. 1–7, 2014. doi: 10.1109/VTCFall.2014.6965898.

[49] IEEE SPECTRUM. "Superaccurate GPS Coming to Smartphones in 2018". 2017. Disponível em: <https://spectrum.ieee.org/semiconductors/design/superaccurate-gps-coming-to-smartphones-in-2018>. Acesso em Jan. 2021.

[50] TECHPP. "Here's How the Dual-Frequency GPS Works on the Xiaomi Mi 8". 2020. Disponível em: <https://techpp.com/2018/05/31/xiaomi-mi-8-dual-frequency-gps-tracking/>. Acesso em Ago. 2021.

[51] XIAOMI. "Mi 8: The 2018 Xiaomi Flagship". 2018. Disponível em: <https://www.mi.com/global/mi8/>. Acesso em Ago. 2021.

[52] SASSI, A., ELHILLALI, Y., CHARFI, F. "Evaluating Experimental Measurements of the IEEE 802.11 p Communication using ARADA LocoMate OBU Device compared to the Theoretical Simulation Results", *Wireless Personal Communications*, v. 97, n. 3, pp. 3861–3874, 2017.

[53] BARCELOS, V. P., AMARANTE, T. C., DRURY, C. D., et al. "Vehicle Monitoring System using IEEE 802.11p Devices". In: *2014 Brazilian Symposium on Computer Networks and Distributed Systems*, pp. 460–467, 2014. doi: 10.1109/SBRC.2014.55.

[54] LIANG, W., LI, Z., ZHANG, H., et al. "Vehicular Ad Hoc Networks: Architectures, Research Issues, Methodologies, Challenges, and Trends", *International Journal of Distributed Sensor Networks*, v. 11, n. 8, pp. 745303, 2015. doi: 10.1155/2015/745303. Disponível em: <https://doi.org/10.1155/2015/745303>.

[55] WANG, Y., HU, J., ZHANG, Y., et al. "Reliability Evaluation of IEEE 802.11p-based Vehicle-to-Vehicle Communication in an Urban Expressway", *Tsinghua Science and Technology*, v. 20, n. 4, pp. 417–428, 2015. doi: 10.1109/TST.2015.7173456.

[56] GHAFOOR, K. Z., LLORET, J., BAKAR, K. A., et al. "Beaconing Approaches in Vehicular Ad Hoc Networks: A Survey", *Wireless personal communications*, v. 73, n. 3, pp. 885–912, 2013.

[57] HENDERSON, T. R., LACAGE, M., RILEY, G. F., et al. "Network Simulations with the NS-3 Simulator", *SIGCOMM Demonstration*, v. 14, n. 14, pp. 527, 2008.

[58] PAPANASTASIOU, S., MITTAG, J., STRÖM, E. G., et al. "Bridging the Gap between Physical Layer Emulation and Network Simulation". In: *2010 IEEE Wireless Communication and Networking Conference*, pp. 1–6, 2010. doi: 10.1109/WCNC.2010.5506341.

[59] MITTAG, J., PAPANASTASIOU, S., HARTENSTEIN, H., et al. "Enabling Accurate Cross-Layer PHY/MAC/NET Simulation Studies of Vehicular Communication Networks", *Proceedings of the IEEE*, v. 99, n. 7, pp. 1311–1326, 2011. doi: 10.1109/JPROC.2010.2103291.

[60] SOMMER, C., GERMAN, R., DRESSLER, F. "Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis", *IEEE Transactions on Mobile Computing*, v. 10, n. 1, pp. 3–15, 2011. doi: 10.1109/TMC.2010.133.

[61] WESSEL, K., SWIGULSKI, M., KÖPKE, A., et al. "MiXiM: The Physical Layer an Architecture Overview". In: *Proceedings of the 2nd International Conference on Simulation Tools and Techniques*, Simutools '09, Brussels, BEL, 2009. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering). ISBN: 9789639799455.

doi: 10.4108/ICST.SIMUTOOLS2009.5555. Disponível em: <https://doi.org/10.4108/ICST.SIMUTOOLS2009.5555>.

[62] KÖPKE, A., SWIGULSKI, M., WESSEL, K., et al. "Simulating Wireless and Mobile Networks in OMNeT++ the MiXiM Vision". In: *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops*, Simutools '08, Brussels, BEL, 2008. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering). ISBN: 9789639799202.

[63] ISKOUNEN, S., THI MAI TRANG, N., MONNET, S. "WiFi-Direct Simulation for INET in OMNeT++", *arXiv preprint arXiv:1609.04604*, 2016.

[64] ELBATT, T., GOEL, S. K., HOLLAND, G., et al. "Cooperative Collision Warning using Dedicated Short Range Wireless Communications". In: *Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks*, VANET '06, p. 1–9, New York, NY, USA, 2006. Association for Computing Machinery. ISBN: 1595935401. doi: 10.1145/1161064.1161066. Disponível em: <https://doi.org/10.1145/1161064.1161066>.

[65] CHANDRA, R., PADHYE, J., RAVINDRANATH, L., et al. "Beacon-Stuffing: Wi-Fi without Associations". In: *Eighth IEEE Workshop on Mobile Computing Systems and Applications*, pp. 53–57, 2007. doi: 10.1109/HotMobile.2007.16.

[66] MAO, Y., WANG, J., COHEN, J. P., et al. "PASA: Passive Broadcast for Smartphone Ad-Hoc Networks". In: *2014 23rd International Conference on Computer Communication and Networks (ICCCN)*, pp. 1–8, 2014. doi: 10.1109/ICCCN.2014.6911820.

[67] DHONDGE, K., SONG, S., CHOI, B., et al. "WiFiHonk: Smartphone-Based Beacon Stuffed WiFi Car2X-Communication System for Vulnerable Road User Safety". In: *2014 IEEE 79th Vehicular Technology Conference (VTC Spring)*, pp. 1–5, 2014. doi: 10.1109/VTCSpring.2014.7023146.

[68] WON, M., SHRESTHA, A., EUN, Y. "Enabling Wifi P2P-based Pedestrian Safety App", *arXiv preprint arXiv:1805.00442*, 2018.

[69] TURKES, O., SCHOLTEN, H., HAVINGA, P. J. "Cocoon: A Lightweight Opportunistic Networking Middleware for Community-oriented Smart Mobile Applications", *Computer Networks*, v. 111, pp. 93 – 108, 2016. ISSN: 1389-1286. doi: https://doi.org/10.1016/j.comnet.2016.08.021. Disponível em: <http://www.sciencedirect.com/science/article/pii/

S1389128616302742>. Cyber-physical systems for Mobile Opportunistic Networking in Proximity (MNP).

[70] SHIMIZU, T., LU, H., KENNEY, J., et al. "Comparison of DSRC and LTE-V2X PC5 Mode 4 Performance in High Vehicle Density Scenarios". In: *Proc. ITS World Congr.*, pp. 1–7, 2019.

[71] MASINI, B. M., SILVA, C. M., BALADOR, A. "The Use of Meta-Surfaces in Vehicular Networks", *Journal of Sensor and Actuator Networks*, v. 9, n. 1, pp. 15, 2020.

[72] MANNONI, V., BERG, V., SESIA, S., et al. "A Comparison of the V2X Communication Systems: ITS-G5 and C-V2X". In: *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, pp. 1–5, 2019. doi: 10.1109/VTCSpring.2019.8746562.

[73] ALESSANDRO FEITOSA JR, G1. "Guia do 5G: quando a tecnologia chegará ao Brasil? Veja perguntas e respostas". 2021. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2021/03/12/guia-do-5g-quando-a-tecnologia-chegara-ao-brasil-veja-perguntas-e-respostas.ghtml>. Acesso em Mar. 2021.

[74] RAVIGLIONE, F., MALINVERNO, M., CASETTI, C. "Characterization and Performance Evaluation of IEEE 802.11p NICs". In: *Proceedings of the 1st ACM MobiHoc Workshop on Technologies, MOdels, and Protocols for Cooperative Connected Cars*, TOP-Cars '19, p. 13–18, New York, NY, USA, 2019. Association for Computing Machinery. ISBN: 9781450368070. doi: 10.1145/3331054.3331548. Disponível em: <https://doi.org/10.1145/3331054.3331548>.

[75] COHDA WIRELESS. "Cohda Wireless features in Volkswagen New Golf 8 with Car2X". 2021. Disponível em: <https://cohdawireless.com/cohda-wireless-features-in-volkswagen-new-golf-8-with-car2x/>. Acesso em Jan. 2021.

[76] FORBES. "Volkswagen Adds 'Vehicle-To-Everything' Communications To Revamped Golf With NXP Chips". 2019. Disponível em: <https://www.forbes.com/sites/samabuelsamid/2019/10/28/volkswagen-includes-nxp-v2x-communications-in-8th-gen-golf/?sh=376b4e7d16bc>. Acesso em Jan. 2021.

[77] KHAN, M. A., CHERIF, W., FILALI, F., et al. "Wi-Fi Direct Research - Current Status and Future Perspectives", *Journal of Network and Computer Applications*,

v. 93, pp. 245–258, 2017. ISSN: 1084-8045. doi: https://doi.org/10.1016/j.jnca.2017.06.004. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1084804517302230>.

[78] FRANK, R., BRONZI, W., CASTIGNANI, G., et al. "Bluetooth Low Energy: An Alternative Technology for VANET Applications". In: *2014 11th Annual Conference on Wireless On-demand Network Systems and Services (WONS)*, pp. 104–107, 2014. doi: 10.1109/WONS.2014.6814729.

[79] JEONG, S., BAEK, Y., SON, S. H. "Hierarchical Network Architecture for Non-Safety Applications in Urban Vehicular Ad-Hoc Networks", *Sensors*, v. 19, n. 19, 2019. ISSN: 1424-8220. doi: 10.3390/s19194306. Disponível em: <https://www.mdpi.com/1424-8220/19/19/4306>.

[80] TOUATI, F., TABISH, R., MNAOUER, A. B. "A Real-time BLE enabled ECG System for Remote Monitoring", *APCBEE Procedia*, v. 7, pp. 124–131, 2013. ISSN: 2212-6708. doi: https://doi.org/10.1016/j.apcbee.2013.08.022. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2212670813001243>. The 3rd International Conference on Biomedical Engineering and Technology - ICBET 2013.

[81] PARK, Y., HA, J., KUK, S., et al. "A Feasibility Study and Development Framework Design for Realizing Smartphone-Based Vehicular Networking Systems", *IEEE Transactions on Mobile Computing*, v. 13, n. 11, pp. 2431–2444, 2014. doi: 10.1109/TMC.2014.2309959.

[82] INTELLIGENT TRANSPORTATION SYSTEMS JOINT PROGRAM OFFICE. "National ITS Reference Architecture". 2021. Disponível em: <https://www.its.dot.gov/research_archives/arch/index.htm>. Acesso em Nov. 2021.

[83] BLUM, J., ESKANDARIAN, A., HOFFMAN, L. J. "Performance Characteristics of Inter-Vehicle Ad Hoc Networks". In: *Proceedings of the 2003 IEEE International Conference on Intelligent Transportation Systems*, v. 1, pp. 114–119 vol.1, 2003. doi: 10.1109/ITSC.2003.1251931.

[84] KARAGIANNIS, G., ALTINTAS, O., EKICI, E., et al. "Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions", *IEEE Communications Surveys Tutorials*, v. 13, n. 4, pp. 584–616, 2011. doi: 10.1109/SURV.2011.061411.00019.

[85] COHDA WIRELESS. "Platooning". 2021. Disponível em: <https://cohdawireless.com/platooning/>. Acesso em Mar. 2021.

[86] NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION. "Automated Vehicles for Safety". 2021. Disponível em: <https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety>. Acesso em Nov. 2021.

[87] AHMED, E., GHARAVI, H. "Cooperative Vehicular Networking: A Survey", *IEEE Transactions on Intelligent Transportation Systems*, v. 19, n. 3, pp. 996–1014, 2018. doi: 10.1109/TITS.2018.2795381.

[88] IEEE. "News Releases". 2012. Disponível em: <https://www.ieee.org/about/news/2012/5september-2-2012.html>. Acesso em Jan. 2021.

[89] KEYSIGHT TECHNOLOGIES. "5G & Beyond For Dummies®, Keysight Technologies Special Edition". 2021. Disponível em: <https://www.keysight.com/br/pt/assets/7121-1150/ebooks/5G-and-Beyond-For-Dummies.pdf>. Acesso em Nov. 2021.

[90] JAFARI, A., AL-KHAYATT, S., DOGMAN, A. "Performance Evaluation of IEEE 802.11p for Vehicular Communication Networks". In: *2012 8th International Symposium on Communication Systems, Networks Digital Signal Processing (CSNDSP)*, pp. 1–5, 2012. doi: 10.1109/CSNDSP.2012.6292712.

[91] LI, J., CUI, X., LI, Z., et al. "Method to Improve the Positioning Accuracy of Vehicular Nodes Using IEEE 802.11p Protocol", *IEEE Access*, v. 6, pp. 2834–2843, 2018. doi: 10.1109/ACCESS.2017.2785443.

[92] JÚNIOR, J. G. R., QUINTANILHA, I. M., CAMPISTA, M. E. M., et al. "Sistema para Monitoramento Descentralizado de Trânsito baseado em Redes Veiculares Infraestruturadas", *SBRC 2013 (Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos)*, 2013.

[93] HEINOVSKI, J., KLINGLER, F., DRESSLER, F., et al. "A Simulative Analysis of the Performance of IEEE 802.11p and ARIB STD-T109", *Computer Communications*, v. 122, pp. 84–92, 2018. ISSN: 0140-3664. doi: https://doi.org/10.1016/j.comcom.2018.03.016. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0140366417305017>.

[94] GRÄFLING, S., MÄHÖNEN, P., RIIHIJÄRVI, J. "Performance Evaluation of IEEE 1609 WAVE and IEEE 802.11p for Vehicular Communications". In: *2010 Second International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 344–348, 2010. doi: 10.1109/ICUFN.2010.5547184.

[95] SHAHIN, A. A., YOUNIS, M. "Alert Dissemination Protocol using Service Discovery in Wi-Fi Direct". In: *2015 IEEE International Conference on Communications (ICC)*, pp. 7018–7023, 2015. doi: 10.1109/ICC.2015.7249445.

[96] HENDERSON, T. R., ROY, S., FLOYD, S., et al. "NS-3: Project Goals". In: *Proceeding from the 2006 Workshop on Ns-2: The IP Network Simulator*, WNS2 '06, p. 13–es, New York, NY, USA, 2006. Association for Computing Machinery. ISBN: 1595935088. doi: 10.1145/1190455.1190468. Disponível em: <https://doi.org/10.1145/1190455.1190468>.

[97] AHMED, B., MALIK, A. W., HAFEEZ, T., et al. "Services and Simulation Frameworks for Vehicular Cloud Computing: a Contemporary Survey", *EURASIP Journal on Wireless Communications and Networking*, v. 2019, n. 1, pp. 1–21, 2019.

[98] MARTINEZ, F. J., TOH, C. K., CANO, J.-C., et al. "A Survey and Comparative Study of Simulators for Vehicular Ad Hoc Networks (VANETs)", *Wireless Communications and Mobile Computing*, v. 11, n. 7, pp. 813–828, 2011.

[99] GRZYBEK, A., SEREDYNSKI, M., DANOY, G., et al. "Aspects and Trends in Realistic VANET Simulations". In: *2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pp. 1–6, 2012. doi: 10.1109/WoWMoM.2012.6263793.

[100] LOPEZ, P. A., BEHRISCH, M., BIEKER-WALZ, L., et al. "Microscopic Traffic Simulation using SUMO". In: *The 21st IEEE International Conference on Intelligent Transportation Systems*. IEEE, 2018. Disponível em: <https://elib.dlr.de/124092/>.

[101] RAMAMOHANARAO, K., XIE, H., KULIK, L., et al. "SMARTS: Scalable Microscopic Adaptive Road Traffic Simulator", *ACM Trans. Intell. Syst. Technol.*, v. 8, n. 2, dec 2016. ISSN: 2157-6904. doi: 10.1145/2898363. Disponível em: <https://doi.org/10.1145/2898363>.

[102] TREIBER, M., KESTING, A. "An Open-Source Microscopic Traffic Simulator", *IEEE Intelligent Transportation Systems Magazine*, v. 2, n. 3, pp. 6–13, 2010. doi: 10.1109/MITS.2010.939208.

[103] VARGA, A., HORNIG, R. "An Overview of the OMNeT++ Simulation Environment". In: *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops*, Simutools '08, 2008. ISBN: 9789639799202.

[104] LANTZ, B., HELLER, B., MCKEOWN, N. "A Network in a Laptop: Rapid Prototyping for Software-Defined Networks". In: *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks*, Hotnets-IX, New York, NY, USA, 2010. Association for Computing Machinery. ISBN: 9781450304092. doi: 10.1145/1868447.1868466. Disponível em: <https://doi.org/10.1145/1868447.1868466>.

[105] AMOOZADEH, M., DENG, H., CHUAH, C.-N., et al. "Platoon Management with Cooperative Adaptive Cruise Control enabled by VANET", *Vehicular Communications*, v. 2, n. 2, pp. 110–123, 2015. ISSN: 2214-2096. doi: https://doi.org/10.1016/j.vehcom.2015.03.004. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2214209615000145>.

[106] TREIBER, M., HENNECKE, A., HELBING, D. "Congested Traffic States in Empirical Observations and Microscopic Simulations", *Phys. Rev. E*, v. 62, pp. 1805–1824, Aug 2000. doi: 10.1103/PhysRevE.62.1805. Disponível em: <https://link.aps.org/doi/10.1103/PhysRevE.62.1805>.

[107] TREIBER, M., HELBING, D. "Realistische Mikrosimulation von Strassenverkehr mit einem einfachen Modell". In: *16th Symposium Simulationstechnik ASIM*, v. 2002, p. 80, 2002.

[108] ARBABI, H., WEIGLE, M. C. "Highway Mobility and Vehicular Ad-Hoc Networks in NS-3". In: *Proceedings of the 2010 Winter Simulation Conference*, pp. 2991–3003, 2010. doi: 10.1109/WSC.2010.5678993.

[109] AHMED, M. S., HOQUE, M. A., PFEIFFER, P. "Comparative Study of Connected Vehicle Simulators". In: *SoutheastCon 2016*, pp. 1–7, 2016. doi: 10.1109/SECON.2016.7506701.

[110] NSNAM. "NS-3: Network Simulator". 2021. Disponível em: <https://www.nsnam.org>. Acesso em Fev. 2021.

[111] MITTAG, JENS AND PAPANASTASIOU, STYLIANOS. "NS-3 Reference Manual – Module: PhySim-WiFi". 2012. Disponível em: <https://dsn.tm.kit.edu/medien/downloads_old/Manual-PhySimWiFi-1.2.pdf>. Acesso em Fev. 2021.

[112] VEINS. "Veins: The Open Source Vehicular Network Simulation Framework". 2021. Disponível em: <https://veins.car2x.org/>. Acesso em Fev. 2021.

[113] INET FRAMEWORK. "What Is INET Framework?" 2021. Disponível em: <https://inet.omnetpp.org/Introduction.html>. Acesso em Mar. 2021.

[114] RASHDAN, I., SCHMIDHAMMER, M., DE PONTE MUELLER, F., et al. "Performance Evaluation of Vehicle-to-Vehicle Communication for Cooperative Collision Avoidance at Urban Intersections". In: *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, pp. 1–5, 2017. doi: 10.1109/VTCFall.2017.8288274.

[115] SHAGDAR, O., NASHASHIBI, F., TOHME, S. "Performance Study of CAM over IEEE 802.11p for Cooperative Adaptive Cruise Control". In: *2017 Wireless Days*, pp. 70–76, 2017. doi: 10.1109/WD.2017.7918118.

[116] NOOR-A-RAHIM, M., ALI, G. G. M. N., NGUYEN, H., et al. "Performance Analysis of IEEE 802.11p Safety Message Broadcast With and Without Relaying at Road Intersection", *IEEE Access*, v. 6, pp. 23786–23799, 2018. doi: 10.1109/ACCESS.2018.2829897.

[117] CAO, S., LEE, V. C. "An Accurate and Complete Performance Modeling of the IEEE 802.11p MAC Sublayer for VANET", *Computer Communications*, v. 149, pp. 107–120, 2020. ISSN: 0140-3664. doi: https://doi.org/10.1016/j.comcom.2019.08.026. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0140366419303299>.

[118] ZHENG, J., WU, Q. "Performance Modeling and Analysis of the IEEE 802.11p EDCA Mechanism for VANET", *IEEE Transactions on Vehicular Technology*, v. 65, n. 4, pp. 2673–2687, 2016. doi: 10.1109/TVT.2015.2425960.

[119] TEIXEIRA, F. A., E SILVA, V. F., LEONI, J. L., et al. "Vehicular Networks using the IEEE 802.11p Standard: An Experimental Analysis", *Vehicular Communications*, v. 1, n. 2, pp. 91–96, 2014. ISSN: 2214-2096. doi: https://doi.org/10.1016/j.vehcom.2014.04.001. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2214209614000151>.

[120] VIVEK, N., SRIKANTH, S. V., SAURABH, P., et al. "On Field Performance Analysis of IEEE 802.11p and WAVE Protocol Stack for V2V & V2I Communication". In: *International Conference on Information Communication and Embedded Systems (ICICES2014)*, pp. 1–6, 2014. doi: 10.1109/ICICES.2014.7033960.

[121] RAJPUT, N. S. "Measurement of IEEE 802.11p Performance for Basic Safety Messages in Vehicular Communications". In: *2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pp. 1–4, 2018. doi: 10.1109/ANTS.2018.8710108.

[122] BLOESSL, B., SEGATA, M., SOMMER, C., et al. "Performance Assessment of IEEE 802.11p with an Open Source SDR-Based Prototype", *IEEE Transactions on Mobile Computing*, v. 17, n. 5, pp. 1162–1175, 2018. doi: 10.1109/TMC.2017.2751474.

[123] HUANG, X., ZHAO, D., PENG, H. "Empirical Study of DSRC Performance Based on Safety Pilot Model Deployment Data", *IEEE Transactions on Intelligent Transportation Systems*, v. 18, n. 10, pp. 2619–2628, 2017. doi: 10.1109/TITS.2017.2649538.

[124] COHDA WIRELESS. "V2X: Vehicle–to–Everything". 2021. Disponível em: <https://cohdawireless.com/sectors/v2x/>. Acesso em Mar. 2021.

[125] SATISH, C. *Inter-Vehicular Communication for Collision Avoidance using Wi-Fi Direct*. M. Sc. dissertation, Rochester Institute of Technology, Rochester, New York, USA, 2014.

[126] BAI, F., STANCIL, D. D., KRISHNAN, H. "Toward Understanding Characteristics of Dedicated Short Range Communications (DSRC) from a Perspective of Vehicular Network Engineers". In: *Proceedings of the Sixteenth Annual International Conference on Mobile Computing and Networking*, MobiCom '10, p. 329–340, New York, NY, USA, 2010. Association for Computing Machinery. ISBN: 9781450301817. doi: 10.1145/1859995.1860033. Disponível em: <https://doi.org/10.1145/1859995.1860033>.

[127] BLOESSL, B., O'DRISCOLL, A. "A Case for Good Defaults: Pitfalls in VANET Physical Layer Simulations". In: *2019 Wireless Days (WD)*, pp. 1–6, 2019. doi: 10.1109/WD.2019.8734227.

[128] RAPPAPORT, T. S. *Wireless Communications: Principles and Practice*. 2nd ed. Upper Saddle River, NJ 07458, Prentice Hall, 2002.

[129] HILT, B., BERBINEAU, M., VINEL, A., et al. *Networking Simulation for Intelligent Transportation Systems: High Mobile Wireless Nodes*. 1st ed. 27-37 St George's Road, London SW19 4EU, UK and 111 River Street, Hoboken, NJ 07030, USA, ISTE Ltd and John Wiley & Sons, Inc., 2017.

[130] CARPENTER, M. G., MOURY, M. T., SKVARCE, J. R., et al. *Objective Tests for Forward Looking Pedestrian Crash Avoidance/Mitigation Systems, Final Report*. Relatório técnico, National Highway Traffic Safety Administration, US Department of Transportation, USA, 2014.

[131] ANAYA, J. J., MERDRIGNAC, P., SHAGDAR, O., et al. "Vehicle to Pedestrian Communications for Protection of Vulnerable Road Users". In: *2014 IEEE Intelligent Vehicles Symposium Proceedings*, pp. 1037–1042, 2014. doi: 10.1109/IVS.2014.6856553.

[132] PINTO NETO, J. B., GOMES, L. C., ORTIZ, F. M., et al. "An Accurate Cooperative Positioning System for Vehicular Safety Applications", *Computers & Electrical Engineering*, v. 83, pp. 106591, 2020. ISSN: 0045-7906. doi: https://doi.org/10.1016/j.compeleceng.2020.106591. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0045790618326776>.

[133] WILLIAMS, T., ALVES, P., LACHAPELLE, G., et al. "Evaluation of GPS-based Methods of Relative Positioning for Automotive Safety Applications", *Transportation Research Part C: Emerging Technologies*, v. 23, pp. 98–108, 2012.

[134] ASUS. "ZA550KL: Guia do Utilizador". 2018. Disponível em: <https://dlcdnets.asus.com/pub/ASUS/ZenFone/ZA550KL/PG13969_ZA550KL_EM_WEB.pdf>. Acesso em Mar. 2021.

[135] MICROWAVES 101. "Magnetic Materials". 2021. Disponível em: <https://www.microwaves101.com/encyclopedias/magnetic-materials>. Acesso em Mar. 2021.

[136] PANDE, K., NAIR, V., GUTIERREZ, D. "Plasma Enhanced Metal-Organic Chemical Vapor Deposition of Aluminum Oxide Dielectric Film for Device Applications", *Journal of Applied Physics*, v. 54, n. 9, pp. 5436–5440, 1983.

[137] WONG, J. Y. *Theory of Ground Vehicles*. 3rd ed. 111 River Street, Hoboken, NJ 07030, USA, John Wiley & Sons, 2001.

[138] WORLD HEALTH ORGANIZATION. "Table A4: Speed Laws and Enforcement by Country/Area". 2018. Disponível em: <https://www.who.int/violence_injury_prevention/road_safety_status/2018/Table_A4_Speed.pdf?ua=1>. Acesso em Mar. 2021.

[139] WANG, C. D., THOMPSON, J. P. "Apparatus and Method for Motion Detection and Tracking of Objects in a Region for Collision Avoidance utilizing a Real-Time Adaptive Probabilistic Neural Network". mar. 18 1997. US Patent 5,613,039.