DEPARTAMENTO DE ENGENHARIAS E CIÊNCIAS DA COMPUTAÇÃO

MESTRADO EM ENGENHARIA INFORMÁTICA E DE TELECOMUNICAÇÕES

UNIVERSIDADE AUTÓNOMA DE LISBOA

"LUÍS DE CAMÕES"

Segurança das comunicações V2X em ambientes 5G

Dissertação para a obtenção do grau de Mestre em Engenharia Informática e de Telecomunicações

Autor: Lázaro João Apolo Lukombo

Orientador: Joaquim Viana

Número do candidato: 30007608

Outubro de 2022

Lisboa

1 Dedicatória

Dedico este trabalho aos meus amados pais, Manuel Lukombo e Salomé Flora Apolo Lukombo, aos meus irmãos, Bernadeth Feliciano, Mosheta Lukombo, Manuel Deodato Lukombo, Zola Lukombo, Nsimba Lukombo e Flora Lukombo, que sempre estiveram presentes de forma direta e persistentes na minha educação, estre trabalho é fruto do vosso investimento.

2 Agradecimentos

Primeiramente agradecer à Deus pelas bênçãos diárias que me têm sido concedidas. Durante os dois anos de formação muitas foram as pessoas que contribuíram de forma ativa e passiva no meu percurso académico as quais devo o maior agradecimento pelo suporte, força, confiança que depositaram em mim. Quero agradecer aos meus amados pais e queridos irmãos. Um especial agradecimento para as minhas sobrinhas maravilhosas que cujo abraço fraternal foi importante em momentos de fatiga na elaboração deste trabalho, ao meu excelentíssimo orientador Phd. Joaquim Viana, foi um grande incentivador, guia para esta elaboração. A todos os professores que deixaram um pouco da sua sapiência em especial aqueles que sempre insistiram e acreditaram em mim, ao excelentíssimo Phd. Mário Marques. A todos vocês, o meu obrigado.

Resumo

Estamos à beira de uma nova era de veículos autônomos interligados com experiências de utilizadores e segurança rodoviária melhorada em diversos casos de utilização. Esta tese apresenta conceitos baseando-se no estudo, análise da segurança dos novos sistemas de comunicação sem fios para os sistemas de transporte inteligentes, que consistem em exploração de várias tecnologias com o propósito de melhorar a interface entre condutor, o veículo e a estrada. O objetivo dos sistemas de transporte inteligentes é reduzir significativamente os acidentes de viação, o controlo do tráfego e a poluição do trânsito. Os protocolos de comunicação existentes veículo para todos (V2X), especialmente o 5G, permitiram avanços significativos na segurança de condução autónoma. As aplicações de condução autónoma precisam de informação para chegarem ao seu destino o mais rapidamente possível. Com isto em mente, o V2X oferece múltiplas opções de largura de banda e os recursos de transmissão são partilhados entre utilizadores o que permite uma experiência significativamente aprimorada, inteligente e capaz de suportar a troca massiva de informações de forma rápida e com baixa latência. O 5G-V2X, que é um complemento eficaz do LTE V2X e suporta aplicações de condução autónoma que não podem ser suportadas pelo LTE V2X, também inclui bandas mmWave, gama de subtransportadores escaláveis e massive MIMO. Esta tese visa compreender os mecanismos de segurança das comunicações V2X num ambiente 5G, a forma como esta segurança é proporcionada, as suas consequências positivas e negativas, e os benefícios, riscos e impactos da utilização de comunicações 5G para V2X. O objetivo deste documento é discutir os mecanismos utilizados para garantir a segurança das comunicações V2X.

Palavras-Chave: V2X; 5G; 5GNR, LTE, ITS, Condução Autónoma; Segurança;

Abstract

We are on the verge of a new era of connected autonomous vehicles with improved user experiences and road safety in various use cases. This thesis presents concepts based on the study, safety analysis of new wireless communication systems for intelligent transportation systems, which consist of exploration of various technologies for the purpose of improving the interface between driver, vehicle and road. The goal of intelligent transportation systems is to significantly reduce traffic accidents, traffic control, and traffic pollution. Existing vehicle-to-all (V2X) communication protocols, especially 5G, have enabled significant advances in autonomous driving safety. Autonomous driving applications need information to get to their destination as quickly as possible. With this in mind, V2X offers multiple bandwidth options and transmission resources are shared between users which enables a significantly enhanced, intelligent experience capable of supporting the massive exchange of information quickly and with low latency. 5G-V2X, which is an effective complement to LTE V2X and supports autonomous driving applications that cannot be supported by LTE V2X, also includes mmWave bands, scalable subcarrier range and massive MIMO. This thesis aims to understand the security mechanisms of V2X communications in a 5G environment, how this security is provided, its positive and negative consequences, and the benefits, risks and impacts of using 5G communications for V2X. The purpose of this paper is to discuss the mechanisms used to ensure the security of V2X communications.

Keywords: *V2X; 5G; 5GNR, LTE, ITS, Autonomous Driving; Security;*

Índice

3 Lista de figuras

4 Lista de tabelas

5 Glossário

ITS	INTELIGENT TRANSPORT SYSTEM
ADCM	Autonomous Driving Control Message
ATM	Action Triggered Message
ADC	Autonomous Driving Control
ADV	Autonomous Driving Vehicle
ADAS	Advanced Driver Assistance Systems
C-V2X	Cellular Vehicle-to-Everything
D2D	Device to Device
DSRC	Dedicated Short Range Communications
eMBMS	Evolved Multimedia Broadcast Multicast
eMBB	Enhanced Mobile Broadband
3GPP	3rd Generation Partnership Project
FDM	Frequency Division Multiplexing
5G-V2X	Five Generation Vehicle -to- Everything
ITS	Intelligent Transport System
LIDAR	Light Detection and Ranging
LTE	Long Term Evolution
MANET	Mobile Ad-Hoc Network
MIMO	Multiple Input Multiple Output
NAT	Network Access and Transport
NOMA	Multiple Non-Orthogonal
NR-V2X	New Radio Vehicle to Everything
OFDM	Orthogonal Frequency Division Multiplexing
OPEX	Operation Expenditures
OBU	On-Board Unit

PHY	Physical (Layer)
QoS	Quality of Service
RAN	Radio Access Network
RAT	Radio Access Technology
RADAR	Radio Detection and Ranging
RSU	Road-Side Unit
SDN	Signal-to-Noise Ration
TDM	Time Division Multiplexing
UE	User Equipment
VANET	Vehicular Ad-Hoc Network
V2P	Vehicle to Pedestrian
V2I	Vehicle to Infrastructure
V2N	Vehicle to Network
V2X	Vehicle to Everything

Introdução

Com o crescente avanço das tecnologias de informação e comunicação, tem sido maior a necessidade de se melhorar o processo que permite preservar a confidencialidade, a integridade e a disponibilidade da informação partilhada entre sistemas [1] .

"A indústria automóvel está no meio de uma mudança para condução automatizada e desenvolvimento de sistemas avançados de assistência ao condutor (ADAS) onde os veículos podem reagir rapidamente a alterações de ambientes complexas, estimulando assim a mudança para um sistema de transporte inteligente (ITS)" [2]. A comunicação veículo para todos (V2X) é um meio que serve para instruir veículos conectados num sistema e com grandes competências de comunicação para se orientarem com segurança por meio de transmissão de mensagens, no intuito de se prevenir acidentes de trânsito, passar informações relativamente às condições das estradas, meteorologia, aproximação de pedestres bem como melhorar o conforto dos passageiros [3].

As comunicações V2X (veículo para todos) têm desempenhado uma função importante na melhoria da segurança e eficiência do mundo automotivo, devido ao crescente índice de tecnologias de veículos conectados e ao V2X. Esta tecnologia visa controlar a comunicação automotiva e as comunicações para operações específicas em um veículo que tem à capacidade de comunicar com qualquer entidade na rede. No entanto, surgiu a necessidade de dar solução a algumas debilidades das comunicações de veículos para infraestrutura (V2I) e veículos para veículos (V2V) [2], [3].

Justificativa

A escolha do tema da presente dissertação baseou-se no facto de a introdução do 5G ter sido considerada uma solução integral com grandes melhorias em relação à versão anterior que não suportava as exigências de alta produção, com segurança ultra alta, latência superbaixa ao lado dos seus meios de segurança. Desde o seu desenvolvimento, foram criados padrões para que possam suportar as redes móveis, veículos corporativos e a *IoT* (Internet das coisas) [2].

O 5G é uma tecnologia com poucos anos de desenvolvimento, surgiu em 2015, existem já alguns estudos que abordam sobre a sua implementação e impacto nas comunicações V2X [2], como o trabalho de I. Mabiala [4] que aborda conceitos gerais sobre a condução autónoma em comunicações sem fio, onde centra o seu foco no estudo e analise da evolução dos protocolos de comunicação e a introdução da tecnologia 5G, porém a segurança da implementação desta tecnologia em comunicações V2X, não constitui um tema suficientemente discutido [2]. Entretanto, tendo em vista dar mais um contributo científico pretendemos analisar os requisitos que permitem garantir a segurança nas comunicações V2X dentro do ambiente 5G, em diversos casos passíveis de utilização a serem abordados, avaliar o seu impacto atualmente e estimar nos anos vindouros e com base nesta análise e pesquisa, os problemas levantados e apresentando eventuais propostas de melhoria.

Problemática de investigação

- Quais são os métodos que garantem a segurança das comunicações V2X em ambientes 5G?
- Como deve ser garantida esta segurança?
- Quais os seus impactos, positivos e negativos
- Quais são os benefícios, riscos e impacto do 5G se for implementado para comunicações V2X?

A presente dissertação tem como **objetivo geral** analisar os métodos utilizados para garantir a segurança na comunicação a partir de veículos com algum grau de autonomia em ambiente 5G.

Como objetivos específicos temos os seguintes:

- Identificar os mecanismos de segurança usados na atualidade em comunicações V2X.
- Compreender o impacto do 5G para comunicações V2X.
- Analisar e procurar compreender as vulnerabilidades dos mecanismos de segurança estudados em ambientes 5G
- Descrever as eventuais melhorias propostas para dar solução às vulnerabilidades estudadas.

Sumário

A presente dissertação estará organizada em 4 capítulos:

Capítulo 1 – Introdução

O presente capítulo com a introdução, justificativa, problemas de investigação e objetivos geral e específicos

Capítulo 2 - Fundamentação Teórica/ Estudo da Arte

Neste capítulo efetuaremos um breve estudo sobre condução autónoma, os sistemas de transporte inteligentes, sua arquitetura, principais aplicações e os níveis de segurança que apresentam, estado das comunicações V2X, o 5G em comunicações V2X e um breve estudo sobre a nova rádio 5G.

Capítulo 3 - Analise dos Mecanismos de Segurança

Neste capítulo analisaremos os métodos de segurança usados com base em casos de uso a serem estudados como sistema de transporte inteligente neste capítulo.

Capítulo 4 - Conclusão

Feita a revisão de literatura e a análise comparativa dos métodos de segurança empregados nas comunicações V2X estaremos aptos para fazer uma breve conclusão sobre o estado da segurança das comunicações V2X, dentro dos parâmetros abordados na dissertação.

6 Fundamentação Teórica/Estado da Arte

A quarta revolução industrial tem provocado inúmeras alterações na sociedade, em que a condução autónoma constitui uma parte importante deste progresso, contribuindo na facilitação da mobilidade de pessoas portadoras de deficiência, reduzindo também o número de acidentes e dando a capacidade de partilha de dados e informação aos veículos [5]. Neste capítulo faremos uma síntese do estado da arte do nosso tema de pesquisa delimitado em redes veiculares, sistemas de transportes inteligentes, as comunicações V2X, 5G e o novo rádio para as tecnologias 5G (NR).

6.1 Redes Veiculares

Cada entidade de uma rede veicular, seja veículo ou infraestrutura, é considerada uma parte importante da rede e é chamada um nó, a arquitetura de uma rede veicular define como estes se comunicam e se organizam. A comunicação entre nós é caracterizada pela comunicação veículo-veículo (V2V) e são trocadas mensagens entre nós para obter informações sobre o ambiente que podem contribuir para a redução de acidentes e congestionamentos [6] [7].

Cada OBU (On-Board Unit) opera em modo *ad hoc* e pode enviar mensagens em um ou mais pulos, ou seja, as mensagens entre veículos dentro da mesma gama de comunicação sem fios são enviadas por múltiplos veículos intermediários [6]. No entanto, neste modo de funcionamento, a conectividade da rede depende da densidade de veículos no ambiente, ou seja, se houver poucos veículos, a informação pode não chegar ao seu destino, enquanto se houver muitos veículos, são necessários algoritmos sofisticados para evitar colisões entre mensagens [8].

A comunicação entre nós e infraestrutura (modo infraestrutura) é chamada comunicação veículo-a-infra-estrutura (V2I) e, pode ser alargada para comunicar com outras redes e serviços, visando que o custo de implementação destes sistemas aumenta devido à necessidade de instalar equipamento ao longo do percurso [9]. Existem três tipos de arquitetura ou topologias de rede e podem ser caracterizadas da seguinte forma:

1) Pura arquitetura *ad hoc* - VANET, onde os veículos não precisam de qualquer infraestrutura externa para trocar informações desde que estejam suficientemente próximos de outros veículos;

2) Uma arquitetura apoiada em infraestruturas onde a comunicação tem lugar entre os veículos e as infraestruturas na estrada;
3) Arquitetura híbrida, caracterizada pela presença de comunicação tanto V2V como V2I. Os dispositivos executam tarefas de agregação, processamento de redes, acesso a Internet, ou dispositivos de segurança [7].

As redes *ad hoc* são fáceis de estabelecer, não requerem instalação e só existem quando é necessário transmitir dados [10].

Como mencionado anteriormente, uma VANET é essencialmente uma rede móvel composta por veículos e é um tipo de MANET que lida com a comunicação entre veículos [11]. Por conseguinte, os problemas encontrados na implantação do MANET são os mesmos que os encontrados na implantação do VANET [12] [4]. As VANETs possuem algumas características, a citar no paragrafo seguinte:

- Densidade variável da rede - esta propriedade varia com o número de veículos, ou seja, alta densidade quando há muitos veículos na rede, por exemplo, durante o congestionamento. Baixa densidade quando o número de veículos é baixo;
- Alta mobilidade: os nós (veículos) da rede estão em constante movimento e movem-se a diferentes velocidades e em diferentes direções, o que os torna difíceis de prever;
- Topologia dinâmica da rede: devido às diferentes velocidades e às mudanças de direção dos nós, a sua posição em relação aos nós vizinhos está em constante mudança, levando a mudanças muito rápidas na topologia da rede;
- Dimensão ilimitada da rede: As VANETs podem ser distribuídas por regiões, cidades e mesmo países inteiros, o que significa que a dimensão da rede é ilimitada em termos de área;
- Paragens frequentes: as interrupções frequentes acontecem devido à dinâmica da rede, a alta mobilidade dos nós, condições meteorológicas, baixa densidade de tráfego e obstáculos temporários;
- Troca rápida de mensagens: Devido à alta velocidade e constante mobilidade dos veículos na rede, a troca de diferentes tipos de mensagens deve ser rápida, ou seja, a mensagem deve ser enviada o mais rapidamente possível para que o destinatário possa responder à mensagem [12] [4].

Os objetivos das VANETs são de assegurar a segurança rodoviária, aumentar a eficiência do tráfego e o conforto dos passageiros dos veículos, e permitir um planeamento eficiente das rotas durante a condução. As aplicações implementadas em VANETs podem ser divididas em dois tipos: aplicações de segurança e aplicações sem segurança [4] [13].

O objetivo das aplicações de segurança é a prevenção de acidentes. O consórcio de Comunicação de Segurança Veicular (VSC) identifica um conjunto de aplicações de segurança que são: aviso de violação de trânsito, comunicação veículo-veículo, aviso de paragem do veículo, travagem de emergência, aviso de saída da faixa de rodagem, travagem, aviso de trânsito e manutenção do sinal. Para estas aplicações, a comunicação veículo-a-veículo e/ou veículo-a-infra-estrutura é essencial [13].

Portanto, os veículos estão equipados com vários sensores que coletam dados de tráfego e efetuam continuamente uma monitoria do ambiente. Além disso, as aplicações de segurança em colaboração permitem aos veículos trocar informações de tráfego em tempo real, enviar e receber notificações para melhorar a segurança do tráfego e prevenir acidentes [4].

As aplicações não de segurança incluem informações sobre o estado das estradas e o desempenho do tráfego, bem como aplicações de conveniência, entretenimento e lazer. Exemplos de tais aplicações incluem a monitorização do tráfego, tais como a monitorização do congestionamento da faixa de rodagem e a hora estimada da ocorrência assim como o aviso de veículos de emergência [13] [12].

6.2 Condução Autónoma

A investigação sobre veículos autónomos começou em 1977 no Laboratório de Engenharia Mecânica de Tsukuba (TMEL) no Japão com o desenvolvimento do primeiro veículo inteligente do mundo capaz de seguir as linhas brancas da estrada e de percorrer até 20 milhas por hora [14].

A condução autónoma apoia-se em sistemas de transporte autónomos, interpretam o ambiente e utilizam várias tecnologias tais como RADAR (deteção e alcance de rádio), LIDAR (deteção e alcance de luz), GPS e visão por computador. Estes veículos podem adaptar o seu estilo de condução em poucos segundos [15].

Os sistemas de transporte autónomos estão equipados com sistemas de condução autónomos que podem ser veículos sem condutor, robotizados ou auto-conduzidos. *A US*

National Highway Traffic Safety Administration redefiniu recentemente versão melhorada dos níveis de condução autónoma existentes, a serem classificados no paragrafo seguinte:

- Sem automatização: o veículo está dependente da intervenção humana em todos os aspetos da condução;
- Assistência ao condutor: Enquanto o condutor executa outras tarefas, o sistema auxilia por vezes em certas tarefas, tais como escolher uma direção ou acelerar e travar;
- Automatização parcial: o sistema assume tarefas como a seleção de direção, aceleração e travagem enquanto o humano assume outras tarefas;
- Automatização condicional: o sistema assume todas as tarefas e monitoriza o ambiente de condução e o humano intervém apenas quando o sistema necessita de ajuda;
- Elevado grau de automatização: o sistema controla e monitoriza o ambiente e condições específicas sem intervenção humana e, em alguns cenários, pode ser considerado totalmente autónomo mesmo que o condutor não responda adequadamente aos pedidos de intervenção;
- Automatização total: o sistema comporta-se como um condutor humano em todas as condições e corresponde ou excede as capacidades humanas em todos os cenários de condução [4] [16].

Entre 1987 e 1995, a Comissão Europeia financiou o programa de investigação do Projecto Eureka Prometheus (EPP) para desenvolver veículos autónomos. Os veículos autónomos Vamp e VITA-2, desenvolvidos por um grupo de engenheiros da Universidade Militar Alemã em Munique em colaboração com a Mercedes-Benz, foram apresentados na apresentação final do projeto Eureka em Paris em 1994 [4].

Utilizam a visão dinâmica para detetar objetos em movimento e podem evitar e ultrapassar outros veículos na via pública. No total, percorreram mais de 1.000 km em tráfego misto e numa autoestrada de três faixas a 130 km/h. Um ano mais tarde, um modelo Mercedes desenvolvido pelo mesmo grupo viajou entre Munique e Copenhaga a 177 km/h com 95% de autonomia [4].

DARPA, a organização de investigação de desenvolvimento tecnológico militar, lançou o programa DARPA Grand Challenge em 2004 para apoiar a investigação e desenvolvimento em veículos autónomos. A DARPA acredita que todas as tarefas perigosas devem ser

executadas por máquinas e não por humanos, a fim de proteger as tropas e utilizar melhor a mão-de-obra, e esta é a filosofia por detrás de todo o investimento do governo dos EUA na condução autónoma [17].

Após o sucesso do Grande Desafio, em Novembro de 2007, a DARPA organizou o Desafio Urbano, a primeira competição de condução autónoma em que os veículos devem operar com ou sem condutor em ambientes urbanos. As equipas foram encarregadas de desenvolver veículos autónomos que pudessem navegar através do tráfego intenso e efetuar manobras complexas tais como intersecções, manobras evasivas e estacionamento [17].

Os avanços tecnológicos tornaram possível aumentar a capacidade dos sensores e dos sistemas informáticos e assim aumentar a automatização. O objetivo é uma condução totalmente autónoma, onde o condutor humano se torna completamente desnecessário. No entanto, a maioria das marcas de automóveis envolvidas dizem que terão de esperar que a tecnologia "amadureça" e que sejam efetuados testes para provar que a condução autónoma é fiável. Esta experiência é necessária para que as autoridades introduzam regulamentos que permitam a entrada no mercado de veículos autónomos [18].

Recentemente, a indústria automóvel tem o seu foco no desenvolvimento de veículos mais seguros, o que vem aumentando a procura de novos veículos inteligentes com capacidades de condução autónoma.

Os veículos autónomos estão equipados com módulos de comunicação que permitem a troca de informações em tempo real entre veículos vizinhos e entre veículos e estações de base. Para além do módulo de comunicação, são necessários mais cinco módulos para apoiar a condução autónoma, são estes: a deteção, perceção, planeamento, controlo e controlo do sistema [19].

A deteção refere-se à observação do ambiente do veículo autónomo e à recolha de informação. A função de posicionamento utiliza o *GPS*, previsões e mapas rodoviários para determinar com precisão a posição do veículo na estrada [4]. A função de planeamento determina o comportamento e movimento do veículo autónomo, tendo como base as informações recolhidas pela unidade de deteção e monitorização. Planifica a rota necessária para completar a tarefa de condução, tendo em conta o tempo de viagem, a distância e as condições da estrada. A unidade de controlo é responsável pela execução dos comandos solicitados pela unidade de planeamento e pelo controlo dos atuadores, por exemplo para mover, acelerar e travar um veículo autónomo [4].

Com base em informações de tráfego da função de sensor, informações do veículo e dados de navegação da função de planeamento, o controlador controla o comportamento de condução do condutor, tais como mudança de faixa, travessia da estrada e estacionamento. O módulo de controlo do sistema é responsável pela monitorização do estado global do sistema autónomo do veículo, por exemplo, monitorização de falhas e sistemas de entrada [20].

A aplicação de controlo autónomo de condução (ADC) é responsável pelo controlo e gestão do ADV. O ADC Message Layer (ADCM) é utilizado para apoiar esta aplicação. O ADCM pode ser dividido em dois tipos: PMS e AMT recorrentes, em que AMT é uma mensagem orientada para a ação contendo o conteúdo de uma ação ADV que pode ser utilizada para tomar uma decisão no instante seguinte [4].

No entanto é por meio destas mensagens que o veículo pode conhecer os movimentos exatos de outros veículos, podendo assim tomar uma decisão de forma independente e comunicar o seu estado de movimento a outros veículos [21].

PSM é basicamente uma mensagem periódica utilizada para exibir informação sobre o estado do veículo, como posição e rota. Esta informação é recolhida em veículos próximos e enviada para a estação de base para avaliação dos fatores de segurança antes da tomada de medidas. Com base no PSM, o centro de serviços analisa os dados e compila estatísticas de tráfego. A AMT é uma mensagem de ativação de ação contendo conteúdo ADV, que pode então ser utilizada para a tomada de decisões. Só através destas mensagens os veículos podem conhecer os movimentos exatos de outros veículos. Desta forma, podem tomar as melhores decisões de forma independente e comunicar a situação do tráfego a outros veículos[22][23].

6.3 Sistema de transporte inteligente (ITS)

O conceito de Sistemas de transporte inteligente surgiu quando o transporte profissional reconheceu que as tecnologias eletrónicas podem começar a desempenhar um papel significativo na otimização do transporte de superfície [24].

Desde então, as tecnologias de sistema informáticos de comunicação e sensores melhoraram de uma forma significativa, e as tecnologias de sistema de transporte inteligente surgiram nas jurisdições de autoestradas e transportes públicos em todo o mundo para desenvolver e implementar comunicações V2X nas últimas duas décadas [24].

Os Sistemas de transportes inteligentes são compostos por uma vasta gama de tecnologias, incluindo eletrónica, processamento de informação, comunicações e controlos sem fios – destinados a melhorar a segurança, eficiência e conveniência da rede global de transporte e eliminar [24][25]. Dentro das comunicações V2X estão incluídas as comunicações veículo-para-veículo (V2V), veículo para rede (V2N), veículo para infraestrutura (V2I), Unidade de Veículos Laterais (V2R) e Veículo Pedonal (V2P). A pesquisa resultou num primeiro conjunto de padrões de rádio para V2X concluído em 2010. Estas normas baseiam-se na tecnologia IEEE 802.11p e são referidas como comunicações de curto alcance dedicadas (DSRC) [26].

6.3.1 Arquitetura

A ETSI TS 102 940 [27] descreve uma arquitetura sistema de transporte inteligente com base em quatro camadas de processamento que são: camada de acesso, camada de transporte, camada de instalações e camada de aplicação.

Em seu documento R. Zaragatzky [28] faz um esclarecimento a detalhes sobre a arquitetura dos sistemas de transporte inteligentes, onde explica que, a camada de aplicação consiste no conjunto básico de aplicações, estas aplicações solicitam serviços da camada de facilidades para a codificação de mensagens. Estas mensagens são enviadas para a camada de transporte com o seu serviço de encaminhamento ponta-ponta sem conexão que, envia o pacote para o protocolo de geo - networking, ainda dentro da camada de transporte, responsável por encaminhar os pacotes pela rede. Por fim a camada de acesso é usada para transmissão de pacotes em um quadro.

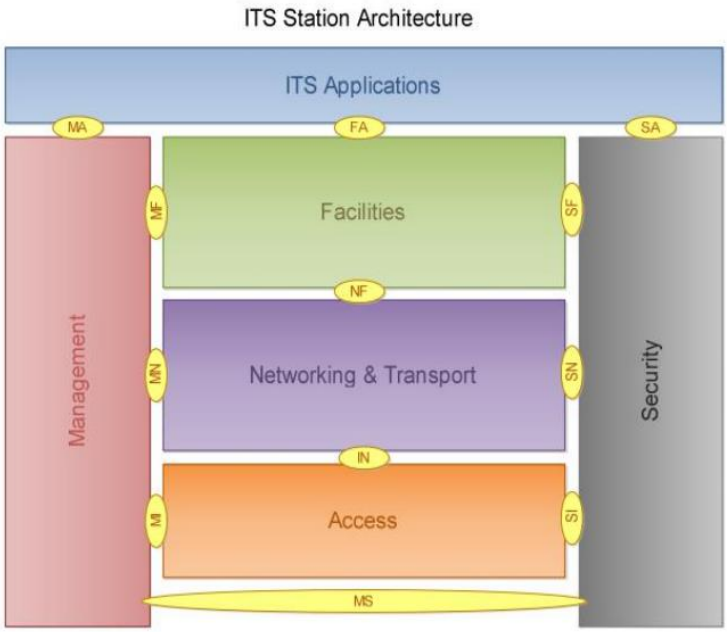

Figura 1: Arquitetura dos Sistemas de Transportes Inteligentes. Imagem retirada em [27]

6.3.2 Conjunto básico de aplicações

Segundo R. Moalla [29] em seu artigo, define uma aplicação como sendo uma associação de duas ou mais aplicações ITS complementares, sendo que são agrupadas pelos seguintes padrões: segurança no trânsito e eficiência no trânsito entre outros. Sendo a segurança no trânsito a maior preocupação de classe de aplicações [28]. R. Moala [29] menciona ainda que as classes de aplicações a serem implementadas devem satisfazer requisitos relacionados com a confidencialidade, segurança, latência e parâmetros de desempenho.

As normas ETSI ITS (Instituto Europeu de Padrões de Telecomunicações) [30] classificaram o conjunto básico de aplicações veiculares, em classes, com diversos casos de uso como mostra a tabela 1, sendo a **Segurança rodoviária ativa**, que tem como foco principal das suas aplicações, melhorar a segurança rodoviária. No entanto, reconhece-se que na melhoria da segurança rodoviária podem também oferecer benefícios secundários, que não estão diretamente associados com a segurança na estrada; **eficiência de trânsito** cujo objetivo principal das aplicações na classe de gestão do trânsito é a melhoria da fluidez do trânsito; **serviços globais de internet, serviços cooperativos locais**, servem para reportar e fornecer pedido de informações para a passagem de veículos. Estes serviços podem incluir serviço de informação e entretenimento, conforto do veículo ou serviço de gestão de

ciclo de vida. Os serviços cooperativos locais são fornecidos a partir de dentro da infraestrutura de rede. Os serviços globais de internet são adquiridos a fornecedores através da internet e outras aplicações.

Tabela 1: Conjunto básico de aplicações segundo a ETSI ITS. Fonte: ETSI, "ETSI TR 102 638 V1.1.1 [30]

Classe de aplicações	**Aplicação**	**Caso de uso**
Segurança rodoviária ativa	Assistência à condução - Consciência cooperativa	Alerta de Veículo de emergência
		Indicação de veículo lento
		Interseção, Alerta de colisão
		Indicação de aproximação de motocicleta
	Assistência à condução - Estrada Aviso de perigo	Alerta de ultrapassagem de veículo
		Mudança de pista
		Redução de brilho
		Travagem eletrónica luzes de emergência
		Aviso de condução de forma errada
		Veículo estacionado- acidente
		Veículo estacionado- avarias
		Aviso sobre o estado do transito
		Aviso de violação de sinal
		Aviso de estrada
		Aviso de colisão
		Dados descentralizados do carro fluente – localização perigosa
		Dados descentralizados do carro fluente- precipitações
		Dados descentralizados do carro fluente- adesão rodoviária
		Dados descentralizados do carro fluente- visibilidade
		Dados descentralizados do carro fluente- vento
Eficiência de trânsito corporativo	Gestão de velocidade	Notificação de limites de velocidade
		Notificação de limites de velocidade regularmente/ contextual
		Aviso de velocidade ideal para semáforos

	Navegação cooperativa	Informações de trânsito e itinerário recomendado
		Orientação e navegação melhoradas da rota
		Aviso de acesso limitado e notificação de desvio
		Sinalização no veículo
Serviços locais cooperativos	Serviços baseados na localização	Ponto de notificação de juros
		Controlo automático de acessos e gestão de estacionamento
		ITS comércio eletrónico local
		Download de média
Serviços Globais de internet	Serviços comunitários	Seguros e serviços financeiros
		Gestão de frota
		Gestão de zona de carregamento
	Gestão do ciclo de vida da estação ITS	software de veículos / fornecimento de dados e atualização
		Calibração de dados do veículo e da RSU.

6.3.3 Segurança

A ETSI TS 102 940 [27] testa a segurança dos diversos casos de uso com base na autenticação, autorização, confidencialidade. Os serviços de segurança são fornecidos camada a camada, subdividindo-os em camadas básicas de processamento ITS. No mesmo documento sobre especificações técnicas dos ITS [27] ainda é referenciado que além dos serviços de processamento de segurança, a entidade de segurança deve ser capaz de fornecer duas subpartes adicionais, que são os serviços de gestão de segurança e a camada de defesa de segurança do ITS. Onde a camada de defesa é responsável por evitar ataques diretos contra ativos e dados críticos do sistema e aumenta a probabilidade de o invasor do sistema ser detetado. Podendo assim conter meios de detecção e prevenção de invasão, atividades de *firewall*, meios de resposta a invasão e funcionalidades de mau comportamento.

6.4 O modelo V2X como plataforma de comunicação

V2X é um conjunto de protocolos baseado na WLAN onde as informações de sensores e outras fontes são transmitidas através de links com alta largura de banda, baixa latência e alta confiabilidade, permitindo a melhoria da condução totalmente autónoma e a partilha de informação com qualquer dispositivo na rede [31][32].

A comunicação V2X pode ser vista como um sensor adicional no veículo, vai alem de outros sensores ativos limitados como RADAR, LIDAR e câmaras. Os sensores V2X sem fios, que monitorizam e comunicam ativamente com outros veículos mesmo sem contacto visual direto, também recolhem informação sobre as intenções do condutor para melhor compreender o que está a acontecer à volta do veículo. Outro benefício dos serviços V2X é que os utilizadores de veículos podem comunicar com o seu meio envolvente. Isto abre muitas novas aplicações e serviços, uma vez que os passageiros podem aceder aos seus próprios dados e suportes e utilizar a Internet dentro do veículo [32].

O tráfego IEEE 802.11 pode frequentemente ser suportado, especialmente em configurações de *hotspot*. Isto pode ser usado como ponto de referência para distinguir entre versões com e sem fios de Wi-Fi, uma vez que Wi-Fi tem uma alta taxa de transmissão devido à contenção de canais, interferência ou congestionamento de Mac. Como resultado, apenas 40% do tempo do pacote de dados é gasto na transmissão. Isto porque a maioria das retransmissões são utilizadas para amplificar e controlar os sinais de rádio [33].

O IEEE 802.11p é proposto como um complemento ao IEEE 802.11. Apoia o intercâmbio de tráfego de veículos utilizando um mecanismo centralizado de camada MAC baseado no acesso melhorado a canais distribuídos (EDCA) da norma 802.11e e o tráfego multicanais do sistema WAVE [14].

A norma IEEE 802.11p/DSRC tem uma arquitetura distribuída baseada no OFDM (*Orthogonal Frequency Division Multiplexing*) e a camada MAC (*Medium Access Technology*) lida com diferentes limiares de QoS e dá prioridade ao tráfego [4].

O protocolo funciona de forma totalmente distribuída e independente da rede através da comunicação direta entre os terminais de origem e destino, permitindo uma transferência de dados eficiente e direta entre veículos. Contudo, a velocidade de transmissão e a latência entre terminais cai rapidamente à medida que a carga da rede aumenta e não é fiável fora do alcance da comunicação, que é tipicamente de várias centenas de metros [34].

Para resolver os pontos fracos do protocolo IEEE 802.11p/DSRC, surge o IEEE 802.11px, uma versão melhorada do protocolo que melhora o desempenho da transmissão em canais ruidosos, aumenta a produção de pacotes e, introduz um mecanismo de codificação de blocos espaço-tempo que aumenta a capacidade dos canais para fornecer melhores circuitos OFDM e capacidades de antena MIMO numa estrutura altamente eficiente [35].

A própria comunicação V2X leva a um número ilimitado de aplicações. Nos veículos, contribui para uma melhor gestão do tráfego, sistemas de transporte inteligentes (ITS) e muitos outros benefícios. As duas principais tecnologias de acesso rádio (RATs) que permitem atualmente a comunicação V2X são a comunicação dedicada de curto alcance (DSRC) e a comunicação celular V2X (C-V2X) [33].

O DSRC baseia-se na norma IEEE 802.11p para a camada física (PHY) e camada de acesso aos meios de comunicação (MAC). O DSRC utiliza um protocolo MAC simples e bem conhecido, que é adequado para uso distribuído. No entanto, a implantação do DSRC em veículos tem sido atrasada devido à fraca escalabilidade e a problemas de comunicação em ambientes de alta mobilidade. A 3GPP (*Third Generation Partnership Project*) desenvolveu o CV2X-LTE, que permite aos veículos operarem de forma distribuída sem infraestruturas móveis, ao mesmo tempo que utiliza infraestruturas para atribuir recursos de forma eficiente [33].

6.5 Redes 5G

O 5G é um novo sistema de comunicação móvel a ser desenvolvido, consideradas como uma tecnologia disruptiva que permitirá uma sociedade totalmente movel e conectada [13]. Ao contrário das gerações anteriores, 5G será mais do que uma simples rede móvel e oferecerá uma vasta gama de aplicações para diferentes serviços. Uma das características mais excitantes do *design* 5G é a sua flexibilidade, conhecida como 'divisão de rede' [4][36], que permitirá oferecer uma gama muito mais ampla de serviços diferentes do que nas gerações anteriores [37].

A investigação sobre elevados débitos de dados está a impulsionar o desenvolvimento de redes móveis de terceira geração (3G). A quarta geração 4G (LTE) oferece um melhor desempenho do que a 3G, mas é claramente insuficiente para as taxas de dados devido a problemas de latência [37].

Por conseguinte, 5G oferece característica chave tais como flexibilidade, escalabilidade e fiabilidade, e tem um desempenho superior às tecnologias anteriores em muitas áreas. 5G não irá substituir estas tecnologias, mas todas elas podem trabalhar em conjunto e potencialmente contribuir para uma prestação de serviços eficiente [37]. A figura a seguir ilustra em resumo as diferenças principais entre as redes 5G e o 4G.

Figura 2: Comparação entre as redes 4G e 5G. Imagem retirada em [38]

O mundo enfrenta um futuro tecnologicamente avançado onde 5G dará acesso a aplicações de apoio a diferentes sectores da sociedade. Este cenário inclui veículos autónomos. Em segundo lugar, permitirá o desenvolvimento de pequenas células ou células de curto alcance, que têm uma série de vantagens, tais como altas velocidades de transmissão e segurança. A comunicação 5G cobre três casos de utilização e permite várias aplicações tais como a realidade virtual, veículos autónomos e cidades inteligentes, que são elementos importantes da Indústria 4.0 [39].

1) Banda larga móvel melhorada (eMBB – *Enhanced Mobile Broadband*): Este cenário inclui múltiplos cenários para cobrir grandes áreas e *hotspots* com necessidades diferentes. Em áreas com alta densidade de utilizadores, é necessária uma largura de banda muito alta, enquanto os requisitos de mobilidade são baixos e as taxas de dados dos utilizadores são elevadas;
2) Comunicações de Alta Fiabilidade e Baixa Latência (URLLC – *Ultra-Reliable and Low Latency Comunication*): Este cenário aplica-se a serviços com elevada latência, fiabilidade e requisitos de disponibilidade, uma vez que a comunicação é centrada no ser humano e na máquina;

3) mMTC (Mass Machine Type Communication): caracterizado pela comunicação centrada na máquina e tecnologia 5G com requisitos mais elevados.

A Internet das Coisas (IoT) é reconhecida como uma aplicação chave de rede para 5G. Significa ligar dispositivos inteligentes e pessoas à Internet, recolher e transmitir informação a pedido, automatizando processos e serviços [40].

Alguns dos requisitos principais do 5G apresentam que as tendências tecnológicas das redes sem fios, tais como as 5G, estão associadas à capacidade de lidar com volumes de tráfego e utilizadores mais elevados a taxas de dados elevadas, mas são apenas parte dos requisitos relevantes. Nas recomendações ITU-R M: 2410-0 [40], ITU-R M: 2411-0 [41] e ITUR M: 2412-0 [42] define-se as capacidades, requisitos e critérios de aceitação para os requisitos básicos para a implantação 5G. Esta recomendação ITU-R M:2410 define requisitos mínimos de desempenho para interfaces de rádio. Por outro lado, ITU-R M: 2411 define os modelos de circuitos a serem utilizados para o desenvolvimento da tecnologia 5G. ITU-R M: 2412 descreve as ferramentas a utilizar para verificar os requisitos necessários da rede 5G [14].

Recomendação ITU-R M: 2410-0 [4][15] especifica diferentes requisitos para as funções de interface de rádio 5G:

- Taxa de dados: o eMBB requer até 10 Gbps na direção da ligação ascendente e até 20 Gbps na direção da ligação descendente;
- Eficiência espectral: a taxa máxima de dados (bit/s/Hz) é normalizada para a largura de banda do canal, que é de 15 bit/s/Hz para a ligação ascendente e 30 bit/s/Hz para a ligação descendente;
- Velocidade da experiência do utilizador: Ligação ascendente de 50 Mbps e ligação descendente de 100 Mbps;
- Atraso: O tempo necessário para enviar pacotes da fonte e receber dados do recetor, em ms. É necessário um atraso de 4 ms e 1 ms para suportar as aplicações eMBB e URLLC. No entanto, é necessário um atraso de 20 ms, que é o tempo entre a transição do estado ocioso e o início da transmissão de dados, e um atraso adicional de 10 ms;
- Largura de banda: suporta uma largura de banda de 100 MHz, no mínimo, e até 1 GHz, no máximo, para casos em que opere em bandas de frequência mais altas, sobretudo acima dos 6GHz.

Portanto, podemos expressar os requisitos como sendo: taxa de dados bastante elevada, taxa de dados do utilizador muito elevada e garantida, apenas melhor eficiência espectral, flexibilidade espectral e largura de banda elevada [15].

6.6 Arquitetura 5G e Segurança

As redes 5G consistem em fornecer altas taxas de dados e maior cobertura da estação base por meio de uma vasta implementação com maior capacidade e melhor qualidade de serviço que as tecnologias de redes anteriores [43]. A figura 3 ilustra a arquitetura da rede 5G.

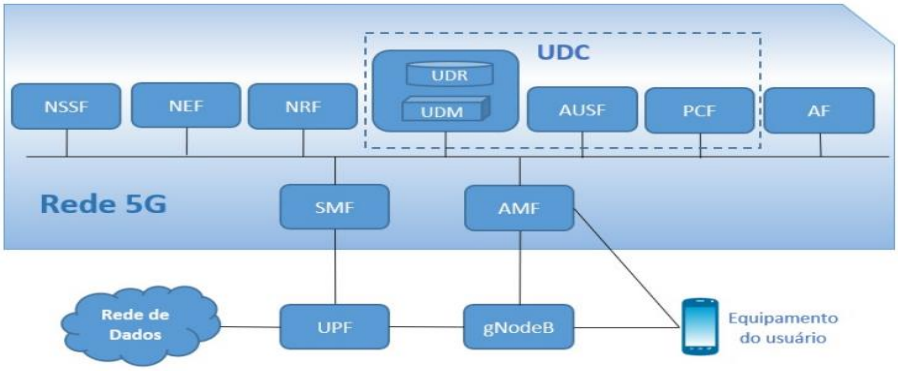

Figura 3: Arquitetura do 5G. Imagem retirada em [38]

Espera-se que as redes 5G forneçam suporte para todos os tipos de comunicação com protocolos programáveis de sistema que podem ser ajustados de acordo com requisitos do utilizador [43]. O 5G pretende equilibrar este fator utilizando mudanças estruturais de arquitetura, desde o *design* focado em células e focado no dispositivo. O aspeto fundamental do *design* do 5G é trazer uma solução unificada em termos de hardware e software para os utilizadores finais e rede de operadores, aparecendo como um sistema transparente integrado com transmissão e tecnologias inovadoras com componentes que fornecem uma experiência de utilizadores perfeita [43].

S. Sullivan [44] diz que o 5G está a criar uma rede ainda mais interligada, onde dispositivos com diferentes capacidades e qualidade de restrições de serviço precisam de interoperar, no entanto espera-se que o 5G resolva seis desafios, incluindo maior capacidade, maior taxa de dados, menor latência de ponta a ponta, conectividade consistente dos dispositivos, redução de custo e qualidade do serviço (QoS). Com o grande avanço da

computação, aumentam os níveis de ataques *hackers*, sendo cada vez mais dirigidos e potentes relativamente às gerações anteriores.

S. Sullivan [44] ainda diz que apesar da medida de segurança introduzida, o 5G pode ainda ser vulnerável a diferentes tipos de ataques e em seu artigo, menciona algumas vulnerabilidades e soluções identificadas do 5G de acordo com o modelo OSI. Um ponto a destacar sobre as comunicações veiculares, na camada de aplicação do modelo OSI, é que a mesma é explorada para obter a topologia de rede, a configuração de recursos e outras informações para ajustar as configurações atuais da rede. Como vulnerabilidades se destaca o facto de os equipamentos de bordo serem responsáveis por lidar com as identidades de cada veículo. Este aspeto representa uma ameaça à privacidade, porque se um equipamento de bordo estiver a usar a mesma identidade em várias mensagens de transmissão, é possível que um intruso rastreie os movimentos dos veículos e comprometa a sua privacidade [45].

I. Ahmad [43] comenta de uma forma aprofundada sobre os desafios da segurança e do crescente avanço do 5G em computação em nuvem, a Rede Definida de Software (SDN) e a Virtualização da Função de Rede (NFV). Diz ainda que O 5G utilizará nuvens móveis, SDN e NFV para responder a enormes desafios de conectividade, flexibilidade e custos. Para os desafios de segurança do 5G, I. Ahmad [43] diz que uma das principais preocupações a nível de utilizador está relacionada com a privacidade e, podem surgir a partir de dados, localização e identidade.

A maioria das aplicações para *smartphones* requer detalhes das informações pessoais do assinante antes da instalação. Os desenvolvedores de aplicações e empresas dificilmente mencionam como os dados são armazenados e para que finalidades serão utilizados. Ameaças como ataques de informação semântica, ataques de tempo e ataques de limite principalmente visam a privacidade da localização dos assinantes. Zaragatzky [28], que propõe como solução que o 5G deva incorporar abordagens de privacidade por *design*, onde a privacidade é considerada desde o início do sistema e muitas funcionalidades necessárias devem estar disponíveis e embutidas no sistema.

É necessária uma abordagem híbrida baseada na nuvem onde os operadores móveis são capazes de armazenar e processar dados sensíveis elevados localmente e menos sensíveis em nuvens públicas. Desta forma, os operadores terão mais acesso e controlo sobre os dados e poderão decidir onde partilhá-los. Da mesma forma, a privacidade orientada para o serviço no 5G levará a uma solução mais viável para preservar a privacidade.

A. Campolo [46] aborda algumas tecnologias para acesso ao rádio 5G como IEEE 802.11 e o Celular V2X (C-V2X).

- **IEEE 802.11 -** é uma tecnologia de acesso ao rádio que permite comunicações V2V (veículos para veículos) e V2I (veículos para infraestruturas), possuindo uma capacidade de suportar interações entre veículos distribuídas, mesmo na ausência de uma infraestrutura à beira da estrada [46].

- **Celular V2X (C-V2X)** – é parte da versão 14 do padrão 3GPP global, baseando-se na plataforma de conectividade LTE existente para o sector automotivo, aproveita as redes LTE existentes para comunicações V2X [46][2].

6.7 Protocolos de comunicação

Com o desenvolvimento de novas tecnologias avançadas, tais como veículos autónomos, podem ser desenvolvidas tecnologias de acesso via rádio (RAT) para permitir comunicações fiáveis de veículos de baixa latência. As tecnologias celulares dedicadas de curto alcance (DSRC) e celulares V2X (LTE V2X) são tecnologias importantes que podem suportar aplicações em veículos. DSRC e LTE V2X estão atualmente a ser testados e desenvolvidos para apoiar aplicações avançadas de veículos com elevada fiabilidade, baixa latência e requisitos de potência elevados.

6.7.1 LTE V2X

LTE V2X, um protocolo de comunicação iniciado e gerido pela Datang Telecom, fornece alta latência, alta fiabilidade, alta taxa de dados e comunicação segura [16].

O LTE V2X pode funcionar com estações de 10 MHz ou 20 MHz. O tempo é organizado em sub-canais de 1 ms contendo 14 símbolos OFDM e a largura de banda é dividida em blocos de recursos de 180 KHz de largura, constituídos por 12 sub-canais OFDM espaçados 15 KHz entre si [4][18]. Uma vez que os dados e a informação de controlo são encapsulados sob a forma de blocos de transporte (TBS) e informação de controlo de cadeia lateral (SCI), diferentes esquemas de modulação e codificação com codificação turbo e 16 codificações em cada QAM [47].

O bloco de transmissão contém um pacote completo contendo um ou mais sub-canais, dependendo do número de blocos de recursos por sub-canal e cada informação de controlo de extensão está associada a um bloco de transmissão e poupa 2 blocos [4][18]. Um SCI contém informação sobre a descodificação da TB, por exemplo, informação sobre, os blocos de recursos utilizados para transmitir o bloco de transmissão ou os sub-canais atribuídos para transmissões posteriores. O SIC deve ser recebido corretamente para descodificar o bloco de transmissão correto. Ambos são transmitidos no mesmo subquadro [18].

Portanto, o LTE V2X pode funcionar no modo 3 ou 4. No modo 3, a estação base móvel seleciona e controla os sub-canais para a comunicação direta veículo-veículo. No modo 4, os veículos selecionam independentemente os seus próprios sub-canais. Os veículos do modo 4 utilizam um conjunto comum de parâmetros para comunicar entre si. Estes parâmetros incluem o número de sub-canais por sub-canal e o número de RBs por sub-canal [4][18].

Podem ser pré-configurados utilizando, por exemplo, os valores por defeito definidos pelo ETSI [20]. Em alternativa, podem ser configurados através da rede celular se o veículo estiver na rede celular. No modo LTE V2X 4, os veículos devem usar programação semipermanente baseada em sensores (SPS) conforme definido no Release 14 [18]-[48] para selecionar independentemente os seus sub-canais.

Um esquema de programação baseado em sensores é utilizado pelos veículos para detetar e selecionar sub-canais que não estão sendo utilizados. Com isto, o esquema de programação possui um processo de reserva em que os veículos notificam os veículos vizinhos dos sub-canais que selecionaram e reservaram. Os veículos informam os veículos vizinhos quando podem utilizar um sub-canal reservado para a sua próxima transmissão através do Intervalo de Reserva de Recursos (RRI), que faz parte do SIC [49].

Um veículo que utiliza um sub-canal específico para transmitir a TB atual ao SCI atual utiliza o RRI para informar os veículos vizinhos que pretende utilizar o mesmo sub-canal para a próxima transmissão no RRI e para impedir que outros veículos utilizem o mesmo sub-canal. Assim, o RRI pode ser fixado igualmente entre 20 ms, 50 ms e 100 ms ou múltiplos de 100 ms [48].

Os autores [48],[4] definem o processo de seleção e atribuição de um novo sub-canal chama-se reselecção. O Autotool seleciona um novo sub-canal para sistemas PLC baseados no reconhecimento, executando os três passos seguintes:

- Primeiro, o ego-agente identifica recursos individuais adequados, recursos de sub-canal (CSRs), dentro de uma janela de seleção. A janela de seleção é o tempo de atraso (até 100 ms) entre T e o pacote de entrada [18];
- O ego-agente exclui alguns RSCs para serem utilizados de uma forma diferente. Com isto, deteta transmissões de outros veículos dentro da chamada janela de deteção. A janela de deteção é o seguinte intervalo de tempo T, que contém os últimos 1000 subquadros antes de T;
- O ego-agente gera uma lista CSRs com o menor valor no Índice de Força do Sinal do Receptor (*RSSI*) para todos os seus blocos de recursos.

6.8 Nova Rádio (NR) V2X

A nova rádio foi pensada para que a comunicação pudesse ocorrer com diferentes tipos de sistemas, desenvolvida para fornecer melhorias na flexibilidade, escalabilidade e eficiência do uso do espectro[50]. Além de melhorar ainda mais as interfaces LTE, o 3GPP lançou a atividade de normalização NR para a primeira fase do sistema 5G na versão 15, e está pronto para melhorar o C-V2X de várias formas sob a versão 5G NR 16.

Como NR V2X tem especificações, mas ainda não está disponível, é fácil ver o que esperar, em detrimento de muitos. As especificações PHY serão adaptadas para a conectividade 5G NR. O 5G NR suporta OFDM para alto desempenho de largura de banda e DFT - OFDM para dispositivos de baixa velocidade de linha. Por conseguinte, foram definidas e disponibilizadas duas bandas de frequência: sub-6 GHz (FR1: 450 MHz a 6 GHz) e ondas milimétricas (FR2: 24,25 GHz a 52,6 GHz). FR1 e FR2 têm uma largura de banda máxima do utilizador de 100 MHz e 400 MHz respetivamente, que é superior à largura de banda máxima de 20 MHz do LTE [32].

O 5G NR tem vantagens em relação às tecnologias anteriores. Como primeiro passo, irá apoiar a utilização de bandas de frequência adicionais onde a tecnologia de acesso rádio é utilizada para permitir o funcionamento em múltiplas bandas de frequência para suportar grandes bandas de frequência. A 5G NR apoiará a operação em bandas de frequência licenciadas abaixo de 1 GHz e até 52,6 GHz, estando previsto o seu alargamento a bandas de frequência não licenciadas [51].

A segunda fase da 5G NR baseia-se em conceções ultra-construídas para a remoção de interferências causadas pela fonte de sinal, a fim de melhorar a eficiência dos recursos. A terceira é a conceção de interfaces rádio e o desenvolvimento de novas tecnologias para permitir novos serviços, a chamada compatibilidade futura [51].

O quarto ponto diz respeito à baixa latência. É de notar que o número de dispositivos e redes em 5G NR é inferior ao de LTE. Finalmente, o quinto ponto diz respeito ao apoio de elementos de antena para transmissão e receção. A formação de feixes é utilizada principalmente para a cobertura de transmissão, enquanto o MIMO agregado é utilizado nas sub-bandas [51].

De acordo com NR V2X [33], NR V2X não foi concebido para substituir LTE V2X, mas para complementar LTE V2X e apoiar casos de utilização que LTE V2X não pode suportar. Como a tecnologia LTE V2X foi normalizada e está em vias de ser implantada comercialmente, é provável que as tecnologias LTE V2X e NR V2X coexistam na mesma área geográfica e os novos veículos terão tanto a funcionalidade LTE V2X como NR V2X. Neste caso, os casos de utilização cujos casos de utilização podem ser apoiados de forma fiável pelo LTE V2X podem utilizar o LTE V2X, enquanto outros casos de utilização podem utilizar os procedimentos NR V2X [52]. Contudo, para que o NR V2X forneça um apoio consistente a todos os utilizadores V2X no futuro, precisa de suportar as aplicações V2X avançadas e as aplicações de segurança básicas suportadas pelo LTE V2X [4].

NR V2X foi concebido para suportar aplicações V2X com diferentes requisitos de latência, fiabilidade e largura de banda. Muitos casos de utilização do NR V2X dependem de uma transmissão de mensagens fiável e não intermitente. Por outra, alguns casos de utilização exigem radiodifusão, enquanto outros, como a programação de veículos, podem ser endereçados enviando mensagens apenas para um conjunto específico de subunidades de veículos [4].

O 3GPP considera em determinados casos de utilização enviar pacotes para uma única unidade veicular [53]. Semelhante a IEEE 802.11bd, NR V2X também considera a utilização de ondas milimétricas para aplicações V2X, especialmente para aplicações de curto alcance e de alto ou muito alto rendimento [53].

O NR V2X define a sua grelha de trabalho os seguintes objetivos.

- Desenho melhorado com cadeias laterais melhores: melhoria dos processos de cadeias laterais para apoiar aplicações V2X avançadas;
- Atualização da interface Uu: A atualização da interface Uu NR deve ser definida para suportar aplicações V2X avançadas;
- Atribuição de configuração Sidechain baseada em interfaces Uu: utilizar interfaces Uu NR para definir atualizações/adições aos recursos de configuração *sidechain*.
- Seleção RAT/interface: investigar mecanismos para determinar a melhor interface (entre LTE sidelink, NR sidelink, LTE Uu e NR Uu) para uma dada transmissão de mensagem V2X;
- Gestão de QoS: investigação de soluções para cumprir os requisitos de QoS para diferentes interfaces rádio;
- Concorrência: Viabilidade e soluções técnicas para a coexistência de LTE V2X e NR V2X num único dispositivo, também conhecido como "on-device concurrency".

Mencionam-se também algumas tecnologias modernas que foram propostas para as camadas físicas do 5G, que são: comunicações de onda milimétrica (mmWave), acesso múltiplo não ortogonal (NOMA), Massive MIMO e rede de rádio cognitiva (CR) [46].

Comunicações de onda milimétrica (mmWave)

Garantem uma largura de banda grande e uma alta produção, que pode ser atrativa para as comunicações V2V entre veículos muito próximos, como por exemplo, para apoiar a deteção cooperativa em um pelotão de alta consistência e comunicações V2I para transferência de dados em massa (por exemplo, para deteção e reconhecimento de objetos, mapas de alta-definição em tempo real) em um curto espaço de tempo. O ambiente hostil de propagação pode, no entanto, dificultar tais benefícios. Alguns desafios surgem, devido à sobrecarga para a formação de feixes em alta mobilidade e ao efeito de bloqueio por, por exemplo, as entidades pedonais [46].

Acesso múltiplo não ortogonal (NOMA)

A NOMA é outro método com potencial para ser usado em 5G NR, segundo B. Di [54] em seu artigo, os autores dizem que a NOMA permite que vários utilizadores partilhem o mesmo recurso de tempo e frequência por multiplexação de domínio de potência ou de domínio de código, dando as comunicações V2X o recurso de cancelamento de interferência, proporcionando melhorias na eficiência do espetro e redução da latência em ambientes móveis mais densos.

Massive MIMO

Massive MIMO, nasce como uma tecnologia que combina as perspetivas da enorme largura de banda mmWave disponível por um lado, e os ganhos esperados das enormes matrizes de antena MIMO por outro [55]. Esta tecnologia pode garantir a segurança das comunicações veiculares em grande parte. Como os tamanhos das antenas são pequenos, é possível estabelecer várias antenas na estação base separadamente. Uma antena de múltiplas entradas e saídas (MIMO) permite que os feixes concentrados sejam direcionados aos utilizadores que são individuais por natureza. Ao utilizar o rastreamento do feixe, bem como o treinamento do feixe, um feixe pode fornecer aos utilizadores uma configuração de comunicação ininterrupta por meio de *links* idênticos com eficiência [55].

Rede de radio cognitiva (CR)

Desenvolvida para aumentar o desempenho do espetro do rádio, a CR é responsável por fazer de ponto de ligação entre os utilizadores licenciados e não licenciados para que eles possam existir em simultâneo usando vários espetros [56] [57].

Por outro lado, os utilizadores não licenciados tornam-se secundários, isto significa que, apenas conseguem transmissão quando os utilizadores licenciados deixam uma lacuna no espetro. O rádio definido pelo *software*, fornece uma alternativa para se alcançar o sensor do espetro, isso faz com que a mesma possua uma melhoria na sua capacidade e na sua taxa de transferência, o que torna a operação desta tecnologia complexa, levando a vulnerabilidades e propiciando ataques voltados a disponibilidade da rede e a confidencialidade[58].

Existem soluções que foram propostas para dar resposta a estas vulnerabilidades, como a utilização da solução para protocolos de transmissão em redes CR (CRN). Devido a ligação dos utilizadores licenciados e não licenciados na mesma largura de banda, há um alto risco de um utilizador não licenciado espiar um utilizador licenciado [59]. Os autores do artigo que fala sobre, a segurança primária da camada física [57], propuseram adicionar ruído artificial ao sinal original através de codificação sobreposta, que causa interferência a um potencial invasor. O ruído é gerado com uma sequência aleatória conhecida pelo emissor e recetor, mas não pelo intruso, neste contexto a questão de privacidade seria resolvida [57].

6.8.1 Coexistência de LTE V2X e 5NR V2X

Espera-se que os veículos equipados com LTE V2X estejam em breve nas estradas o que levará a uma coexistência com o NR V2X [53]. NR V2X não é compatível com LTE V2X,

isto deve-se em parte ao facto de NR V2X utilizar esquemas de numeração múltipla. Os dispositivos LTE V2X que operam na gama de portadoras de 15 kHz não conseguem descodificar as mensagens transmitidas a 30 ou 60 kHz. Assim, os novos veículos serão equipados com ambas as tecnologias modulares, ou seja, LTE V2X e NR V2X, o que exigirá o desenvolvimento de mecanismos de coexistência eficazes [60].

O pacote de trabalho NR V2X sobre coexistência de LTE V2X e NR V2X [37] aborda um cenário em que LTE V2X e NR V2X coexistem em canais diferentes. Para este fim, podem ser utilizadas duas abordagens sem canais coexistentes [61]: Multiplexação por Divisão de Frequência (FDM) ou Multiplexação por Divisão de Tempo (TDM).

- **Abordagem FDM à coexistência:** Nesta abordagem, as transmissões de dois RATs podem sobrepor-se no tempo. A vantagem desta abordagem é que não é propriamente necessária uma sincronização temporal rigorosa entre dispositivos. Para os módulos LTE V2X e NR V2X, mesmo que sejam utilizados dois rádios diferentes, caso os canais não estiverem suficientemente afastados, a receção na outra rádio será afetada por fugas de informação devido a emissões fora da banda. Além disso, se dois rádios operarem na mesma banda de frequência a potência transmitida pelo veículo pode ser limitada por restrições regulamentares e a potência pode ter de ser partilhada entre os dois RAT, o que pode afetar os requisitos de QoS das aplicações V2X. A prioridade do pacote pode ser tida em conta ao regular a potência de transmissão entre dois RAT [61]. Por exemplo, se os pacotes NR-V2X tiverem maior prioridade, a potência de transmissão LTE-V2X pode ser reduzida para manter a potência total de transmissão dentro dos limites regulamentares;
- **Abordagem de coexistência da TDM:** Nesta abordagem, os dois RATs são transmitidos em canais e momentos diferentes. Assim sendo, apenas uma interface transmite num determinado momento, a taxa máxima de transmissão admissível pode ser utilizada por ambas as tecnologias. Também não há fugas de informação entre canais. No entanto, o TDM não é vantajoso para casos de uso crítico de atraso, uma vez que a interface NR-V2X precisa de ser bloqueada no veículo ao gerar pacotes sensíveis ao atraso. Além disso, a sincronização temporal entre LTE-V2X e NR-V2X na abordagem TDM está sujeita a severas limitações [62]. Na abordagem TDM, se um RAT estiver a transmitir o canal LTE-V2X e outro RAT estiver a transmitir (NR-V2X), o segundo RAT NR-V2X, não conseguirá detetar que o RAT

LTE-V2X está a transmitir devido ao problema de *half-duplex*, que afeta o desempenho do algoritmo de reserva de recursos baseado na deteção (LTE-V2X). Mensagens diferentes enviadas usando a NR V2X na mesma UE podem exigir outros requisitos de QoS. A titulo de exemplo, uma UE precisa de enviar mensagens difundidas, difundidas em grupo e *unicast*. No entanto, algumas destas mensagens podem ser intermitentes e algumas podem ser descontínuas. No entanto, outras classes de tráfego (por exemplo, tráfego *unicast* intermitente) podem utilizar outros mecanismos de transmissão. Uma forma de resolver a coexistência de diferentes tipos de tráfego é usar a preempção [60].

- **Avaliação do desempenho:** O desenvolvimento dos mecanismos que compõem o NR V2X ainda não está completo, mas alguns membros realizaram testes iniciais de desempenho. Os resultados de [63] mostram que é possível obter um grande ganho de desempenho com um espaçamento portador de 60 KHz; o LTE V2X utiliza 15 KHz. Este benefício é ainda mais pronunciado a velocidades relativas mais elevadas (280 500 km/h). Para cobrir longas distâncias, é necessário um prefixo cíclico alargado de 60 KHz, o que aumenta a sobrecarga de comunicação. O NR V2X pode superar consideravelmente o LTE V2X aproveitando a maior distância de sub-interferência proporcionada pela utilização de sub-interferência flexível NR. O maior desempenho do NR V2X ao nível da ligação resulta num maior desempenho ao nível do sistema, tal como demonstrado em [64]. Num cenário em que a distância de interligação é de 60 KHz e o canal é de 20 MHz, o percentual de entrega de pacotes (PDR) foi cerca de 99,7 % para todos os tipos de mensagem e comunicação. A NR V2X pode, pelo menos, satisfazer aproximadamente alguns requisitos de desempenho num cenário de autoestrada. No entanto, em ambientes urbanos, normalmente caracterizados por maiores densidades de veículos e elevadas perdas de tráfego, o desempenho do NR V2X varia entre 93 e 97%, indicando que são necessárias mais melhorias para assegurar uma comunicação fiável em ambientes urbanos. O desempenho do NR V2X em ambientes difíceis e aplicações mais exigentes continua por investigar [64]-[65]-[63].

A rede celular omnipresente (LTE V2X) é um espectro de comunicação que permite uma maior segurança rodoviária e uma condução autónoma [66]. Estas redes utilizam um modo de transmissão direta denominado LTE V2X e proporcionam um maior alcance de comunicação e uma maior fiabilidade para ligar veículos, objetos e pessoas. As soluções de *chipset* LTE V2X

serão compatíveis com sensores 5G e sistemas avançados de assistência ao condutor (AAS) como o LTE V2X de comunicação direta [67].

Estudos demonstraram que DSRC e LTE V2X podem apoiar de forma fiável aplicações de segurança que requerem um atraso de 100 milissegundos (msec), desde que a densidade de veículos não seja demasiado elevada [68]. Contudo, como os requisitos de qualidade de serviço (QoS) se tornam mais rigorosos nas aplicações V2X, como em muitas aplicações V2X avançadas [19], os dois RATs V2X existentes já não podem fornecer o desempenho requerido.

No entanto, os utilizadores de LTE V2X enviam mensagens de controlo para além dos símbolos de dados. O sinal de referência desmodulado (DMRS) é um dos sinais utilizados para a estimativa do canal. Nos símbolos LTE, o DMRS é adicionado aos símbolos do OFDM [34].

Uma vez que o LTE V2X pode operar tanto em banda larga como fora de banda, assim como também opera em interfaces aéreas LTE tradicionais e interfaces de derivação. Passo a descrever as interfaces no paragrafo seguinte:

- **V2X sobre interface aérea LTE**: LTE é a tradicional interface aérea entre o eNodeB e o *User Equipment* (UE). Através da interface LTE, cada UE tem de enviar as suas mensagens para o eNodeB através da ligação ascendente e o eNodeB tem de as reencaminhar para a UE de destino através da ligação descendente. Usando a interface LTE, os UEs podem enviar pacotes para o eNodeBs através do *uplink*. Os mesmos ou diferentes eNodeBs reencaminham estes pacotes para UEs remotas usando *downlink* unidirecional ou mensagem multimédia unidirecional melhorada (eMBMS). Por conseguinte, a principal vantagem da interface LTE é aumentar o raio de propagação, o que pode ser conseguido através da exploração das seguintes características do núcleo da célula. O desenvolvimento do LTE V2X é tipicamente realizado em camadas superiores (rede e acima) e ao nível da arquitetura do sistema. Em LTE V2X, eMBMS *unicast* para *downlink* refere-se à transmissão de dados a todas as UEs, em oposição a eMBMS unicast para *downlink*, onde os dados são transmitidos uma vez e simultaneamente a todas as UEs. Isto é benéfico para aplicações V2X, uma vez que a maioria dos transcetores LTE V2X pretendidos estão próximos uns dos outros e são suscetíveis de serem servidos pelo mesmo eNodeB. Para além das características acima referidas, os eNodeBs podem também implementar uma programação quase estável utilizando a interface LTE, onde os recursos eNodeB podem ser utilizados por dispositivos móveis não só para uma

próxima transmissão, mas também para múltiplas transmissões seguintes. A programação semi-estacionária é útil para reduzir a sobrecarga de programação das transmissões V2X na ligação ascendente. Tal mecanismo de programação é benéfico para V2X, uma vez que a maioria do tráfego contém pacotes descontínuos e de tamanho semelhante [69].

- **V2X com interface aérea PC5:** A interface aérea PC5 permite a comunicação direta entre UEs. Os UEs podem utilizar a interface PC5 na presença ou ausência de um eNodeB. Os pacotes transmitidos através da interface PC5 consistem em elementos de dados e informação de controlo lateral (SCI) [69]. O SCI contém informações para descodificar uma determinada transmissão de dados, por exemplo, o esquema de modulação e codificação utilizado, recursos ocupados pelas atuais e futuras transmissões. O canal utilizado para a transmissão do SCI chama-se Canal de Controlo de Ligação Física Lateral (PSCCH) e o elemento de dados chama-se Canal Partilhado de Ligação Física Lateral (PSSCH). O PSCCH e PSSCH são transmitidos por multiplexação de frequência, quer isto dizer, ambos são transmitidos em diferentes recursos de frequência dentro do mesmo *subframe* [16]. A condução autónoma é o futuro da mobilidade [70][71]. Os automóveis podem ser considerados como robôs que interagem com o seu ambiente através de sensores e dispositivos de comunicação fazendo o uso da inteligência artificial para a toma de decisões. Estas comunicações de quinta geração (5G) desempenham um papel fundamental na condução autónoma através de comunicações altamente fiáveis de baixa latência (URLLC) [72]. Espera-se que o URLLC suporte novos serviços que sejam sensíveis a atrasos e exijam taxas de erro de bit muito baixas (os erros são quase inaceitáveis), tais como tráfego de longa distância ou veículos autónomos. A comunicação 5G não suporta a comunicação veículo-veículo (V2V) sobre as estações de base. A comunicação ponto-a-ponto é um serviço adicional de 5G. A figura 4 ilustra a V2X sobre interface baseada em LTE e PC5.

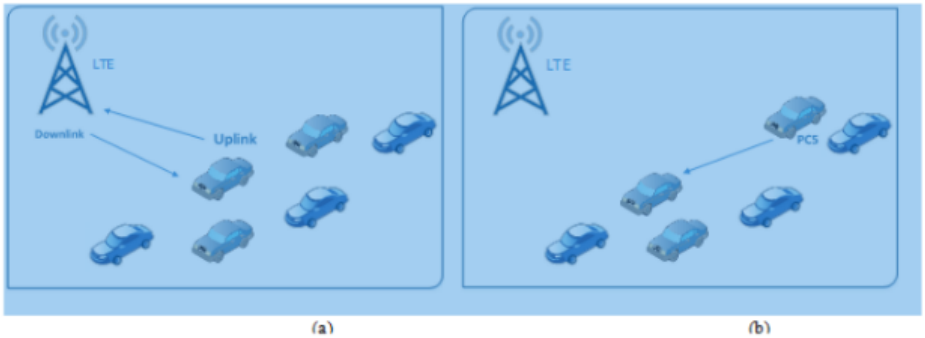

Figura 4: Interfaces de comunicação LTE-V2X (a) baseada em Uu (b) baseada em PC5. Imagem retirada em [73]

6.9 5G em comunicações V2X

Segundo A. Molinaro [46] os sistemas 5G cobrem capacidades de comunicação, *networking* e computação, tanto na rede de acesso a rádio (RAN) como nos segmentos principais da rede. E apresenta algumas das principais áreas de Investigação e melhoria 5G relacionadas com o V2X [46].

Segundo o artigo "*5G Vehicle-to-Everything Services: Gearing up for Security and Privacy"* [50] aos autores dizem que a arquitetura do 5G em comunicações V2X consiste em quatro camadas de rede, que são: rede de acesso 5G, rede de borda, rede central 5G e rede de dados. A rede de acesso 5G é constituída por uma rede de acesso a rádio de próxima geração (NG-RAN) e a rede de acesso 5G-3GPP que liga equipamentos de rede 5G e de suporte de energia, como veículos, infraestruturas e telemóveis transportados por peões.

As comunicações V2X 5G incluem duas operações PC5 e LTE-Uu [26][50]. Com base na proximidade da descoberta de serviço são usadas pelas comunicações V2X para apoiar os equipamentos dos utilizadores em rede [50]. Os autores do artigo [50] afirmam que o 5G NR é uma chave complementar do sistema LTE V2X.

5G Americas whitepaper [74] diz que o V2X foi introduzido com o padrão 802.11p e apoiou um conjunto limitado de serviços básicos de segurança. Com o lançamento de *3GPP 14*, a comunicação V2X poderia expandir-se para suportar uma gama de serviços muito mais ampla e rica, desde a segurança de aplicações com baixa largura de banda, até às aplicações de alta largura de banda, tais como informações de passageiros. A *3GPP* lançou as versões 15 e 16 que permitiram ainda mais serviços V2X, fornecendo uma maior gama, maior consistência, alta produção e segurança, um posicionamento muito preciso e latência ultrabaixa [74].

O *5G American* [74] apresenta uma descrição do 5G nomeando a sua interface de Novo Rádio 5G (NR), indicando que esta interface deverá suportar vários recursos avançados, como multiplexação ortogonal por divisão de frequência (OFDM) escalável e muitas outras.

O 5G tem evoluído para uma infraestrutura ponta-ponta, usando rádio 5G e redes fixas, tecnologias como o *Software Defined Networking (SDN)* são introduzidas, permitindo boa flexibilidade e partilha de recursos de forma virtual [74]. Sobre comunicações veiculares o *5G American* [74] diz ainda que independentemente da rápida evolução, a tecnologia é compatível com as versões anteriores, isto significa que uma rede 5G e um dispositivo LTE são capazes de comunicar um com o outro usando comunicações diretas V2V.

M. Garcia [26], em seu jornal introduz as comunicações NR V2X SL como base para apoiar comunicações V2X universais. O jornal fornece um tutorial abrangente e de referência que apresenta os principais desenvolvimentos do padrão 3GPP essenciais para entender como novo rádio (NR) funciona. O V2X 5G NR suporta casos de utilização avançados e níveis de automatização mais elevados, os autores apresentam ainda alguns casos de uso e requisitos aplicados em comunicações V2X elaborados pela 3GPP, e pela 5GAA[26].

Para os casos de uso elaborados pela 3GPP, distinguem-se diferentes graus de automação variando de 0 a 5, divididos em quatro grupos: pelotão de veículos, direção avançada, sensores estendidos e direção remota. Já os casos de uso 5GAA, os autores [26] dizem que o 5GAA combina casos de uso definidos por 3GPP e define sete grupos: segurança, gestão de operações de veículos, conveniência, direção autónoma, pelotão, a eficiência do trânsito e compatibilidade ambiental, sociedade e a comunidade, o *Journal* de M. Garcia [26], centra-se principalmente em pontos de sidelink que não foram desenvolvidos até a data da sua publicação, onde a interface de ar 5G NR foi introduzida pela primeira vez.

6.9.1 Tipos de Comunicações 5G-V2X

As comunicações 5G-V2X estão divididas em 4 tipos, nomeadamente: comunicação veículo para veículo (V2V), veículo por infraestrutura (V2I), veículo por pedestre (V2P), veículo a rede (V2N)[50].

- **V2V-** Quando dois veículos que estão nas proximidades, podem comunicar diretamente um com o outro, visa melhorar principalmente a segurança rodoviária, a título de exemplo, a colisão de automóveis, sendo que é necessária uma baixa latência e alta segurança para as comunicações V2V;

- **V2I:** Quando um veículo entra na gama de rádio da unidade, pode trocar e partilhar algumas informações que não são sensíveis ao atraso, por exemplo, dados recolhidos para monitorização do trânsito em grande escala na ligação e possíveis dados de informação e entretenimento na ligação;
- **V2P:** Quando um veículo se aproxima de peões que atravessam uma estrada ou um cruzamento, as comunicações diretas V2P são utilizadas para a troca de informações de posição, velocidade e direção, que serão utilizadas para prever uma possibilidade de colisão e alertar tanto os condutores como os peões para evitar potenciais acidentes de viação;
- **V2N:** Como um tipo de comunicações dispositivo-rede, a V2N permite que os veículos comuniquem com os servidores para vários serviços, por exemplo, informação do trânsito tempo real e navegação personalizada.

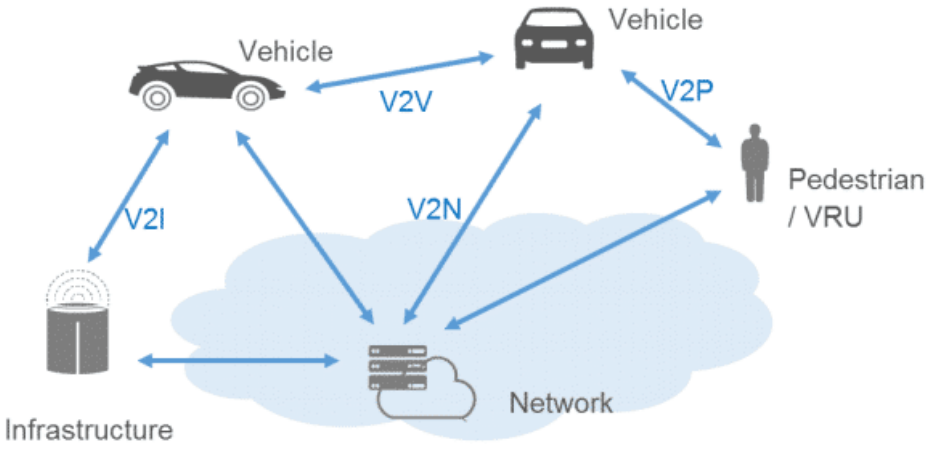

Figura 5: Tipos de comunicações V2X. Imagem retira em [75]

6.9.2 Casos de uso para 5G V2X

Os casos de uso V2X focam-se na segurança, eficiência do trânsito e serviços de informação e entretenimento. Segundo M. Boban [76] a tecnologia 5G-V2X pode ser dividida nas categorias a serem mencionadas em seguida: consciência cooperativa, sensor de cooperação, manobras cooperativas, consciência do utilizador vulnerável na estrada, melhorando a eficiência do trânsito, condução tele-operada.

Consciência cooperativa: tem como objetivo apoiar os veículos a fornecer conhecimento sobre o ambiente e tem como base informações de intercâmbio habilitadas por comunicações V2V/V2I [50].

Sensor de cooperação: tem como objetivo melhorar a qualidade e segurança das deteções individuais e aumentar a perceção ambiental dos veículos, os dados dos sensores e o objetivo da informação dos radares, câmaras e outros sensores que será trocada entre veículos vizinhos. Este caso de uso baseia-se também nas comunicações V2V/V2I, que é uma característica essencial na cooperativa condução autónoma [50].

Manobra cooperativa: este caso de uso permite que um grupo de veículos autónomos conduza coordenadamente de acordo com uma estratégia comum de tomada de decisão centralizada ou descentralizada [50].

Consciência dos utilizadores vulneráveis na estrada: são encaminhados para os utentes da estrada que têm uma elevada taxa de baixas e devem ter atenção especial para a estrada, como as notificações de pedestres, ciclistas [76].

Melhorando a eficiência do trânsito: este caso de uso permite atualizações de rotas e atualizações dinâmicas do mapa digital; como por exemplo, fases de sinal e tempo, aviso de sinal verde [76].

Condução tele-operada: utiliza a comunicação V2N para controlar remotamente um veículo em condições normais de trânsito. São fornecidas informações sobre o ambiente de um veículo, incluindo posições de GPS no mapa, e as condições meteorológicas atuais. Os autores [50] consideram este caso de uso como sendo uma solução em fase de transição, uma vez que ainda está em fase de testes.

6.9.3 Evolução do Celular V2X (C-V2X)

Devido a alta cobertura, segurança e serviços móveis de alta capacidade a tecnologia celular tem sido uma forte candidata para apoiar as comunicações veiculares [77]. O artigo de Abdel Hakeem, menciona que o avanço do C-V2X passou por três estágios, para este trabalho vale ressaltar apenas o terceiro em que as tecnologias C-V2X começaram a ser desenvolvidas para soluções 5G com o propósito de dar algumas respostas na questão de segurança rodoviária e carros conectados, pela *5GAA (5G Automotive Association)* [77].

Abdel Hakeem, [77] Diz que, os serviços exigidos pelos aplicações V2X devem incluir transferências de mensagens, uma frequência de transferência de mensagens que esteja no intervalo (10-50) Hz e, um longo alcance de comunicação para dar mais tempo de resposta. A comunicação V2X deve ser apoiada e, fora da área de cobertura de rede, com transmissão de latência inferior a 100 ms também deve ser apoiada em alguns casos.

S. Chen, et al [78] propõem uma nova estrutura de gestão e mecanismos unificados de identificação e autenticação de segurança numerados para equipamentos C-V2X com base na análise das questões de segurança do sistema C-V2X e regimes de proteção de segurança existentes. Este artigo aborda vários desafios relacionados com a segurança que o C-V2X enfrenta devido aos meios de transmissão de informação sem fios, que pode ser copiada, modificada e até eliminada por potências invasoras. A arquitetura de segurança proposta por este artigo faz a implementação de uma central de registo *VID (Vehicle Identification)* no sistema C-V2X, incorpora um *VIM (Vehicle Identity Module)* e implementa uma unidade de autenticação AAA, responsável por autenticar o VID e gerar certificados. A VID atribui um número único de VID para cada equipamento C-V2X, um VIM é construído no equipamento em módulos de segurança para armazenar VID e executar o processo de autenticação e identificação do equipamento, estas entidades devem trabalhar em conjunto com as entidades existentes no sistema C-V2X, quando o equipamento precisa de aceder ao certificado de comunicação de uma determinada entidade, primeiramente envia uma solicitação ao *AAA* e o processo só continua de se a autenticação for bem-sucedida [78].

6.10 Aspetos de segurança sobre 5G em comunicações V2X

A conexão de veículos prevista para o 5G exige mecanismos de segurança fortes e privacidade para que se consiga impedir o acesso não autorizado a veículos e dados pessoais e para evitar o mau funcionamento de aplicações críticas e dos futuros sistemas e serviços automatizados de condução [46]. M. Muhammad, [79] em seu artigo diz que é necessário reduzir a sobrecarga introduzida pelas funcionalidades de segurança como, a anulação de certificados e, como deve ser assegurada a pontualidade da gestão de autenticação pela contabilidade para as novas implicações de segurança de sensibilização em comunicações V2X.

O artigo de Bian [80] esclarece alguns aspetos de segurança em relação as comunicações V2X, propuseram-se diferentes desafios que não podiam ser atendidos por padrões de dados já propostos pela *ITS e 3GPP*, que adicionam uma subcamada de segurança ao sistema para fornecer mecanismos de segurança baseados em criptografia. Os autores deste artigo *"Toward Secure Crowd Sensing in Vehicle-to-Everything Networks"* [80] apresentam algumas limitações a esses métodos como, o custo elevado para criptografar todas as mensagens na rede e os ataques que não podem ser detetados com base em segurança baseada na criptografia, como

ataque de interrupção que foi encontrado com base em pacotes antigos e ataques de falsificação de dados fornecendo imagens ou vídeos falsos.

O mesmo artigo [80] diz ainda que é difícil encontrar os ataques por interferência e, estes desafios encontrados podem ser superados com a implementação de mecanismos de segurança baseados em segurança não criptografada, desenvolvido a princípio para dar respostas a ameaças de segurança em sistemas de redes móveis sem fio analisando características do canal. Em comunicações V2X o veículo recetor efetua a coleta de dados dos sensores de outros veículos que estejam no mesmo pelotão e com base nestes dados o veículo recetor detém a capacidade de determinar se o conteúdo da mensagem enviada é consistente com o funcionamento do próximo passo de todo pelotão. Os principais desafios do mecanismo de segurança não criptografada consistem no atraso da detenção da ameaça, levam alguns segundos para se concluir o processo e determinar se o conteúdo da mensagem recebida é confiável ou não, o que pode levar a uma tomada de decisão errada em um curto espaço de tempo e levar a uma série de acidentes [80].

Estudos recentes investigam a introdução do *blockchain* para a segurança das comunicações V2X [23], [24]. Vislumbra-se um protocolo de partilha de mensagens entre veículos seguro, baseado numa arquitetura de validação descentralizada usando *blockchain*, que é usado para validação rápida das mensagens trocadas dentro de um determinado pelotão aplicando regras de autenticação, esta autenticação é baseada numa assinatura de anel, que é responsável por validar a identidade dos veículos que acedem a rede de pelotão. Este sistema foi proposto para ser um candidato perfeito para a segurança das comunicações V2X, pelo facto de se basear numa arquitetura descentralizada o que constitui uma vantagem na sua implementação, assim como os valores que são previamente aceites após autenticação que não podem ser modificados [81].

Existe uma estrutura de segurança para partilha de informação eficiente baseada em *blockchain*, que é uma estrutura apoiada na aprendizagem distribuída e é utilizada para aumentar a eficiência da partilha de conhecimento e, um sistema de *acyclic graph (DAG)* direcionado. Para atender à grande exigência das redes veiculares altamente dinâmicas, foi projetado um *DAG* leve para reduzir a latência da operação em termos de permissão e autenticação rápida. Além disso, para aumentar ainda mais a precisão deste modelo, assim como para se minimizar o consumo de largura de banda, os autores propuseram um esquema baseado em aprendizagem distribuída assíncrona adaptativa (ADL) para *upload* e *download* dos

modelos. Os resultados da experiência mostram que a estrutura baseada em DAG é leve e segura, o que reduz tanto o atraso escolhido quanto a confirmação, bem como a resistência a ataques maliciosos. Além disso, o esquema de adaptação ADL proposto por este artigo, melhora o desempenho associado à segurança da condução em comparação com vários algoritmos existentes [82].

7 Metodologias

"O passo inicial para a construção efetiva de um protocolo de investigação é a pesquisa bibliográfica, quer isto dizer, após a escolha de um assunto é necessário fazer uma revisão bibliográfica do tema proposto. Essa pesquisa auxilia na escolha de um método mais apropriado, assim como, no conhecimento das variáveis e na autenticidade da pesquisa" [83].

Para elaborar a presente dissertação realizamos uma pesquisa profunda de diversos artigos científicos e dissertações que abordam o tema a fim de conhecer o estado da arte até ao momento, em bases de dados bibliográficas como a B- On, IEEE, Google Académico e sites da 3GPP, 5GAAA, organizações responsáveis pela gestão do 5G. A pesquisa bibliográfica será feita com base no método descritivo. Baseamo-nos no trabalho de R. Zaragatzky [28] para a escolha da maioria dos capítulos a serem estudados, os demais subcapítulos com abordagem a redes veiculares, condução autónoma e sobre a coexistência entre as tecnologias LTE e 5NR para V2X, baseamo-nos no trabalho de referencia [4], apôs a pesquisa de varias constatou-se os conceitos essências sobre comunicações veiculares, teve-se este trabalho como referência a para a descrição de determinadas definições, conceitos teóricos por apresentarem concordâncias nas definições com as demais bibliografias referenciadas. Sobre redes veiculares, sistemas de transportes inteligentes, os artigos e documentos a investigar são datados de 2006-2021.

A respeito das comunicações veiculares em 5G a pesquisa começa a partir do surgimento e implementação da tecnologia 5G, 2015-2021. Por ser um tema bastante complexo foram excluídos artigos que não estivessem diretamente ligados aos objetivos específicos. As palavras-chaves usadas são: 5G, comunicações veiculares, comunicações veículo-para-todos (V2X), sistema de transportes inteligentes, condução autónoma, New ratio 5G, segurança. A fim de dar resposta ao nosso problema principal, sobre o estado da segurança das comunicações veículos-para-todos (V2X) em ambientes 5G, iniciamos a pesquisa com a análise do estado da arte da condução autónoma, comunicações V2X, entrando em sistemas de transportes inteligentes, teve-se como referência vários autores citados ao longo do trabalho.

Com base nesta pesquisa foram descritos e analisados diferentes métodos que garantem a segurança das comunicações V2X, os principais problemas levantados, as soluções implementadas e sugestões impostas.

8 Análise

No capítulo introdutório, foram explanadas algumas linhas teóricas de interrogação, a partir dos quais se iria construir a nossa investigação. Desta forma, a inserção da tecnologia de 5G nas comunicações V2X infere numa afetação de segurança dos padrões coevos. Neste seguimento, o saber e o conhecimento conseguido com a fundamentação teórica e estado da arte, é aplicado para responder às questões de pesquisa que foram traçadas no início deste trabalho.

Em matéria de segurança nas comunicações V2X, os métodos e mecanismos que asseguram a fidúcia corporizam soluções criptográficas existentes para a segurança V2X e breve discussão sobre vários esforços de padronização. Concentramo-nos principalmente nos cenários de comunicação direta V2X em ambientes 5G, nomeadamente:

- Infraestrutura de Chave Pública: Para proteger as comunicações V2X (por exemplo, para assegurar a integridade e autenticidade da mensagem), a abordagem comum é utilizar criptografia assimétrica utilizando uma infraestrutura de chave pública (PKI) para a gestão das credenciais de segurança [84][85][86]. A PKI permite o intercâmbio seguro de mensagens através da rede. Cada veículo é fornecido com um par de chaves assimétricas e um certificado. O certificado contém a chave pública com atributos específicos V2X, tais como ID e é assinado pela autoridade emissora da chave - desta forma os veículos são registados como participantes válidos da V2X. PKI inclui os seguintes elementos-chave: (a) uma parte de confiança, por exemplo, a autoridade certificadora de raiz (RCA), que fornece serviços para autenticar a identidade das entidades; (b) uma autoridade de registo certificada por uma RCA que emite certificados para usos específicos permitidos pela RCA; (c) uma base de dados que armazena pedidos de certificados e emite/revoca certificados e (d) um armazenamento de certificados no veículo - para guardar os certificados emitidos e chaves privadas [87]. O nó de comunicação (por exemplo, veículo e RSU) é uma entidade final do sistema que solicita certificados ao PKI e comunica com outras entidades finais. A RCA é a raiz da confiança para todos os certificados. Ela entrega certificados às entidades de autorização para emitir certificados para os nós de comunicação. O centro de distribuição fornece informação de confiança atualizada necessária para validar a informação recebida obtida de uma autoridade

PKI legítima e autorizada. O operador regista os nós de comunicação e atualiza a informação necessária nas entidades de autorização;

- Esforços de padronização para a segurança da V2X: Nos Estados Unidos, as principais organizações de desenvolvimento de normalização (SDO) ativas no domínio V2X são IEEE e SAE (*Society of Automotive Engineers*). Na Europa, as SDO relevantes são ETSI (*European Telecommunications Standards Institute*) e CEN (Comité Europeu de Normalização). Grupos de trabalho dedicados dentro de organizações de normalização e fabricantes de veículos estão a trabalhar na resolução de questões de segurança e privacidade para sistemas V2X, a saber, o grupo de trabalho IEEE 1609.2, comité técnico SAE DSRC, consórcio CAMP-VSC (parceria para evitar colisões - comunicações de segurança automóvel) nos Estados Unidos e o grupo de trabalho ETSI-TC-ITS-WG5 na Europa que trata de questões de segurança e privacidade para sistemas V2X [88],[89]. Os grupos de normalização na Europa e nos Estados Unidos estão a construir separadamente arquiteturas de segurança V2X baseadas em PKI [90]. As técnicas de deteção de comportamentos incorretos utilizam um sistema de gestão de credenciais de segurança (SCMS) e uma autoridade de comportamento incorreto (MA) para identificar veículos anómalos. Uma OBU pode enviar relatórios de mau comportamento (MBR) ao SCMS que se baseia em meta dados BSM, por exemplo: (a) a hora e localização onde o MBR foi criado; (b) o método LMBD que causou a criação do MBR e (c) alguma combinação da hora de início e paragem e localização do alegado mau comportamento (dependendo do Método LMBD). CAMP-VSC define "mau comportamento" como a transmissão intencional ou inadvertida de dados incorretos dentro da rede veicular e fornece mecanismos para detetar tais transmissões [91]. A equipa concebe cinco métodos locais de deteção de comportamentos incorretos (LMBD) (para identificar comportamentos incorretos dentro de uma rede V2V) e três métodos de deteção de comportamentos incorretos globais baseados em limiares (GMBD) (identificação de comportamentos incorretos ao nível do veículo utilizando algoritmos e processamento dentro do veículo). As técnicas de deteção de comportamentos incorretos utilizam um sistema de gestão de credenciais de segurança (SCMS) e uma autoridade de comportamento incorreto (MA) para identificar veículos anómalos. Uma OBU pode enviar relatórios de mau comportamento (MBR) ao SCMS que se baseia em metadados BSM, por exemplo: (a) a hora e localização onde o MBR foi

criado; (b) o método LMBD que causou a criação do MBR e (c) alguma combinação da hora de início e paragem e localização do alegado mau comportamento (dependendo do Método LMBD).

- 1) V2X Normas de Segurança: IEEE introduziu uma norma para comunicações V2X - WAVE (acesso sem fios em ambientes veiculares) [92]-[91]. Acima da pilha de protocolos, os requisitos de desempenho do V2X são especificados pela SAE (por exemplo, na norma SAE J2945/1 [72]) que é utilizada principalmente nos Estados Unidos. A norma SAE 2945/1 [72] utiliza um SCMS baseado em PKI [86] para segurança V2X. A norma também requer mecanismos para proteger a privacidade: o certificado é alterado após um período de tempo variável e as entradas nas mensagens BSM (que podem ser usadas para identificar/rastrear o veículo) são aleatórias sempre que um certificado é alterado. A segurança das mensagens V2X é uma queixa com a norma de serviço de segurança IEEE 1609.2 [93] que define estruturas de dados de segurança, formatos de mensagens seguras e o processamento dessas mensagens seguras dentro da plataforma WAVE. As principais características da norma IEEE 1609.2 incluem: (a) esquema de comunicação sem fios entre dispositivos V2X e PKI; (b) esquemas de validade e revogação de certificados e (c) preservação da privacidade (por exemplo, identidade do veículo/utilizador). Os serviços de segurança da norma IEEE 1609.2 apoiam os mecanismos tradicionais de criptografia. O serviço de autenticidade e integridade da mensagem baseia-se em assinaturas digitais. A assinatura e verificação são realizadas utilizando um algoritmo de assinatura digital de chave pública. Por exemplo, o remetente calcula uma assinatura utilizando o algoritmo de assinatura digital de curva elíptica (ECDSA) e o recetor verifica a assinatura utilizando o certificado associado. Para transportar chaves de cifragem simétrica, a norma utiliza um esquema de cifragem assimétrica baseado no esquema de cifragem integrada da curva elíptica (ECIES). A norma define também os tipos de autoridades certificadoras (AC), formatos dos certificados e listas de revogação de certificados (LCR). A distribuição de todos os certificados de segurança (incluindo as CRL) é efetuada pelo SCMS. O ETSI define arquiteturas que as aplicações podem utilizar para satisfazer os seus requisitos de segurança

[84]. Para ter acesso à infraestrutura e serviços de comunicação, um veículo contacta primeiro uma autoridade de inscrição (EA) e autentica-se a si próprio. A EA responde com um conjunto de certificados pseudónimos (para preservar a verdadeira identidade do veículo como medida de privacidade). Estes certificados validam que o veículo pode ser confiado para funcionar corretamente dentro da rede. Para pedir permissão de acesso a um serviço, o veículo contacta uma autoridade de autorização (AA) utilizando um dos certificados pseudónimos (que representa uma identidade temporária). O veículo recebe então um conjunto de certificados em resposta (um para cada serviço solicitado). Os veículos só podem aceder a um serviço se a AA o autorizar a utilizar esse serviço. O formato do certificado ETSI para comunicações V2X também se baseia atualmente no IEEE 1609.2. As normas de segurança ETSI-ITS foram divididas em vários relatórios/especificações técnicas que descrevem (a) a arquitetura e gestão de segurança, (b) modelos de confiança e privacidade, (c) vulnerabilidade de ameaças e análise de risco, (d) formatos de mensagens e certificados e, finalmente, (e) modelos PKI e mapeamento com IEEE 1609.2.

- 2) Esforços de harmonização: Havia dois grupos de trabalho de harmonização de normas (HTG) estabelecidos pelos Estados Unidos e grupo de trabalho de harmonização de normas internacionais europeias [94]: (a) HTG1 - para harmonizar normas de segurança (por exemplo, do CEN, ETSI e IEEE) e promover a interoperabilidade cooperativa V2X; e (b) HTG3 - para harmonizar protocolos de comunicações. O objetivo dos HTG foi fornecer feedback para as SDOs e identificar áreas onde as ações políticas e/ou reguladoras podem ajudar a melhorar a segurança V2X [88]. Os esforços de harmonização foram concluídos em 2013 [94] e os relatórios/recomendações estão disponíveis ao público em linha [94] [95].

Subjacentes a estes mecanismos, existem algumas ameaças à segurança em sistemas V2X, que se encontram dependentes das capacidades e métodos disponíveis do atacante para aceder ao alvo (por exemplo, veículo, RSU e canais de comunicação). Os incentivos para desestabilizar os sistemas V2X incluem [96]: (a) danos físicos/vandalismo (p. ex., negação de

serviço, causar um acidente, congestionamento indesejado da estrada por desvio de trânsito, etc.); (b) incentivos financeiros (p. ex., roubar informação privada do utilizador, extrair propriedades intelectuais OEM, fraude de seguros, etc.); e (c) não monetários (p. ex., melhoria das condições de trânsito dos atacantes, melhoria do agressor reputação, etc.).

Dentro destes ataques, existem algumas variantes, a serem nomeadas no paragrafo seguinte.

Primeiro enumeramos os modelos atacantes que são utilizados na literatura [97] ativos ou passivos - no caso de ataques ativos, o adversário interage ativamente com o sistema enquanto os atacantes passivos escutariam dados críticos (tais como chave privada, certificados, informação de sensores, etc.) sem interagir diretamente com o sistema e/ou perturbar o comportamento normal. Exemplos de ataques ativos incluem falso código/injeção de dados, negação de serviço (DoS), alteração de dados transmitidos (por exemplo, falsificação de GPS, adulteração de transmissão/transação [98]), etc. No contexto do V2X, os ataques passivos podem ameaçar a privacidade de um utilizador, uma vez que é possível ligar mensagens V2X e movimentos de veículos a indivíduos.

Os ataques podem ser realizados *offline*, por exemplo, quando o sistema não está operacional - estes tipos de ataques requerem frequentemente acesso físico ao dispositivo. Os ataques *online*, em contraste, podem ser executados explorando bugs de hardware/software/comunicação em tempo de execução. O atacante pode ser: (i) um membro autenticado da rede autorizado a comunicar com outros membros e/ou com acesso ao nível do sistema (interno) - estes atacantes comportam-se de acordo com o protocolo subjacente, mas enviam informações falsas/violentas ou (ii) podem não ter credenciais válidas/acesso ao sistema (externo) - bastante passivamente escutar a comunicação para inferir informação.

Para se classificarem estes ataques aos sistemas V2X, em ambiente de 5G, principalmente os tipos de ataque DoS, Sybil e a injeção de dados falsos:

1. Ataques do DoS: Os ataques DoS podem acontecer em diferentes camadas da rede onde um adversário envia mais pedidos do que o sistema pode tratar. Por exemplo, um atacante pode tentar desligar/desativar a rede estabelecida pelas RSUs e parar a comunicação entre veículos e/ou RSUs [99]. Num ataque distribuído DoS (DDoS) [100], os nós maliciosos lançam ataques a partir de locais diferentes, tornando assim mais difícil a sua deteção. Na camada física, um tipo importante de ataque de DoS é o ataque de interferência [15] (consulte o trabalho relacionado [101] para uma

classificação detalhada) onde o atacante interrompe o canal de comunicação (por exemplo, por interferência eletromagnética) e pode filtrar/limitar as mensagens recebidas. O encravamento funciona bem apenas em áreas geograficamente restritas, ou seja, digamos, dentro do alcance do(s) dispositivo(s) sem fios do atacante. A maioria dos ataques de interferência/DoS no nível PHY (IEEE 802.11p) ou nas bandas de cerca de 5,9 GHz são sempre restringidos pelo alcance do(s) atacante(s) e não têm impacto nas comunicações V2X em todo o lado. Os ataques de interferência não requerem qualquer conhecimento particular da semântica das mensagens trocadas [102]. Embora os ataques de interferência não sejam específicos dos sistemas V2X (ou seja, podem ser uma ameaça para qualquer rede sem fios), tais ataques podem aumentar a latência nas comunicações V2X e reduzir a fiabilidade da rede [103]. Na camada da rede, ataques DoS baseados no encaminhamento, tais como ataques *JellyFish* [104] exploram vulnerabilidades nos protocolos de controlo de congestionamento e o atacante atrasa ou (periodicamente) larga os pacotes (embora não viole as especificações do protocolo). A queda de pacotes é catastrófica para aplicações relacionadas com a segurança - por exemplo, um veículo envolvido num acidente de trânsito deveria propagar mensagens de aviso, mas outros veículos poderiam ser impedidos de receber estas mensagens de aviso por um atacante que desloque intencionalmente os pacotes. Outra variante é o ataque de batoteiro inteligente [99] em que um adversário obedece às especificações do protocolo de encaminhamento, mas se comporta de forma intermitente. Tais ataques requerem monitorização a longo prazo para deteção [104] que poderia ser impraticável para o cenário V2X devido à alta mobilidade. Ataques de inundação [99], tais como inundação de dados (por exemplo, onde um atacante cria falsos pacotes de dados e os envia para os seus vizinhos) podem tornar os recursos da rede (por exemplo, largura de banda, energia, etc.) indisponíveis aos utilizadores legítimos. Nós notar que estes ataques baseados em rotas só podem ser realizados para redes de comunicação multi-hop (p. ex., não de loja única direta comunicações como a radiodifusão BSM);

2. Ataques da Sybil: Este é um ataque nocivo bem conhecido em redes de veículos sem fios em que um veículo finge ter mais do que uma identificação (por exemplo, múltiplos pares de chaves certificadas) ao mesmo tempo ou em sucessão [105]. Os atacantes da Sybil podem também lançar ataques DoS, desperdiçar largura de banda

da rede, desestabilizar a rede global e constituir ameaças à segurança [99] [30]. Por exemplo, se um veículo malicioso alterar a sua identidade, pode usar múltiplos pseudónimos para aparecer como um veículo diferente em movimento ou fazer parecer que a estrada está congestionada (embora não esteja) e enviar informações incorretas sobre as condições da estrada para veículos/RSUs vizinhos. Um agressor Sybil pode também utilizar as pseudo-identidades para aumentar maliciosamente a pontuação de reputação/confiança (por exemplo, esse uso para medir o quanto os vizinhos podem confiar na informação enviada por um determinado veículo Vi), etc. de veículos específicos ou, inversamente, reduzir a pontuação de veículos legítimos [25].

3. Injeção de dados falsos: Um veículo desonesto pode gerar falsas mensagens de tráfego/segurança ou informação de estimativa de tráfego incorreta (que difere da informação do mundo real) e transmiti-la para a rede com a intenção de perturbar o tráfego rodoviário ou provocar uma colisão [99]- [106]. Os atacantes da Sybil podem reivindicar a sua existência em múltiplos locais e podem, assim, injetar informações falsas na rede. Ao falsificar o GPS, um atacante pode injetar informações falsas de posição utilizando simuladores de GPS e os veículos vítimas podem acabar por aceitar estes sinais gerados, falsos, (mas mais fortes do que os originais). Dados incorretos, tais como informação de localização falsificada, poderiam diminuir a eficiência da entrega de mensagens em até aproximadamente 90% [107]. Os investigadores demonstraram que o controlo cooperativo de cruzeiro adaptativo (CACC) - um importante caso de utilização de V2X - é especificamente vulnerável a falsos ataques de injeção de dados [108]-[109]. Outro tipo de falsa injeção de dados é a repetição de ataques onde um atacante retransmite mensagens para explorar as condições no momento em que a mensagem original foi enviada (por exemplo, o atacante armazena a informação do evento e reenviá-la-á mais tarde, mesmo que já não seja válida) [85]-[99]. Por exemplo, em ataques baseados em localização, o atacante regista uma mensagem autenticada num local Li, transmite-a rapidamente para um local Lj (e retransmite-a em Lj). Da mesma forma, em ataques de repetição baseados em tempo, um adversário regista uma mensagem válida no tempo t1 e volta a reproduzi-la mais tarde (no mesmo local) noutro tempo t2. Para proteção de repetição, existem mecanismos tais como:

a. Incluindo um carimbo de tempo em cada mensagem - digamos utilizando um sistema global de navegação por satélite (GNSS) [109];
b. Assinando digitalmente e incluindo números de sequência [110], etc.

As normas V2X [84]-[92] também fornecem mecanismos de proteção de repetição: o atraso máximo de transmissão de mensagens de um único ponto teria de ser verificado através da receção de estações e mensagens com um carimbo de data/hora desatualizado (ou um futuro *timestamp*) deve ser considerado como não plausível. Reproduzir os ataques em comunicação multi-linha V2X (ou seja, DENMs) são relacionados com o mau comportamento de encaminhamento (por exemplo, onde o agressor possa desviar-se do protocolo de encaminhamento e reencaminhar mensagens para veículos específicos e/ou mensagens de queda) [94], [105]. Enquanto os ataques de repetição (especialmente para comunicações multi-hop) podem afetar o rendimento da rede, apoio a infraestruturas tais como As RSUs (e estações de base para o C-V2X) podem reduzir o impacto de encaminhamento de comportamentos incorretos [106].

A aplicação destes sistemas de comunicação transportam consigo algumas vulnerabilidades. No entanto, as novas tecnologias introduzidas com a 5G NR têm vulnerabilidades que os analistas de segurança e os fabricantes de equipamento original devem conhecer e tratar em conformidade. No campo da privacidade, muitas das novas tecnologias da 5G NR apresentadas neste documento podem ter um impacto negativo na privacidade. As pequenas células introduzidas para permitir a mmWave tornam possível que um atacante tire conclusões sobre a localização de um utilizador a partir da sua escolha da estação base. Isto pode ser combatido adicionando alguma aleatoriedade à escolha da estação de base.

A tecnologia de formação do feixe pode trazer problemas de privacidade, porque o seguimento do feixe implica o seguimento de um utilizador. Também a NOMA pode introduzir problemas de privacidade se não for tratada corretamente, porque o recetor extrai o sinal mais forte de forma iterativa e, assim, extrai sinais com outros destinos. Para resolver isto, não deve ser possível a um recetor não leal traduzir um sinal para a mensagem enviada.

Em termos de disponibilidade, a rádio cognitiva pode introduzir problemas de disponibilidade, devido à sua natureza complexa. No entanto, existem alguns documentos que propõem métodos para assegurar implementações de rádio cognitivas. No plano da confidencialidade, a rádio cognitiva pode também introduzir problemas de confidencialidade. É por isso que vários artigos estudam diferentes soluções para a confidencialidade na rádio

cognitiva. Uma delas é a introdução de ruído a possíveis espiões, mantendo o canal entre o emissor e o recetor autorizado. Esta abordagem é muito semelhante à PLS.

8.1 Cronograma

Tabela 2: Cronograma de atividades. Fonte: Elaboração própria.

	Outubro				Novembro				Dezembro				Janeiro			
Atividades	sem1	sem2	sem3	sem4	sem1	sem2	sem3	sem4	sem1	sem2	sem3	sem4	sem1	sem2	sem3	sem4
Tarefas																
Inicio do projeto																
Reuniões com orientador																
Fase de Planeamento																
Leitura de artigos																
Determinação de objetivos																
Discussão teorica em função dos objetivos																
Fase de escrita do projeto																
Escrever sobre a pesquisa																
Desenvolvimento de conteudo																
Analisar metodologias																
Resumo do projeto																
Apresentação do projeto																

Tabela 3: Cronograma de atividades. Fonte: «Idem»

	Fevereiro				Março				Abril				Maio			
Atividades	sem1	sem2	sem3	sem4	sem1	sem2	sem3	sem4	sem1	sem2	sem3	sem4	sem1	sem2	sem3	sem4
Tarefas																
Inicio do projeto																
Reuniões com orientador																
Fase de Planeamento																
Leitura de artigos																
Determinação de objetivos																
Discussão teorica em função dos objetivos																
Fase de escrita do projeto																
Escrever sobre a pesquisa																
Desenvolvimento de conteudo																
Analisar metodologias																
Resumo do projeto																
Apresentação do projeto																

Conclusão

NR V2X considera uma maior fiabilidade e menor latência na arquitetura da Rede, Segurança, Camada Física e Protocolo. Melhorias adicionais para NR V2X na Versão 17 estão definidas para estudar o desenho da camada física mm-Wave, suporte para múltiplas portadoras *sidelink* como agregação de portadoras, duplicação de pacotes, programação RSU/UE outra UE, formação de feixe, gestão de feixe para ligação *unicast* e Entrada Múltipla Saída Múltipla (MIMO) com classificação superior.

O próprio 5G é um fenómeno recente neste mundo e está sempre a fazer o seu caminho para melhorar a vida das pessoas. Além disso, a comunicação V2X já existe há algum tempo para proteger o segredo de milhares e tem sido um dos modos de comunicação de confiança. Este documento contém o estudo sobre o efeito da segurança 5G centrado particularmente no veículo para tudo na rede, o que pode ter muito impacto na medição da segurança das comunicações V2X. Foram recolhidos estudos literários e respostas dos participantes, a fim de analisar o impacto das comunicações V2X sobre a introdução da tecnologia 5G.

No início, foi adotado um modelo, nomeadamente o modelo ITS ETSI, com vista a descrever o estado atual, bem como as normas para as comunicações V2X. O procedimento de segurança e as perspetivas foram retratados na sua totalidade.

Mais tarde, as soluções dos problemas de segurança foram discutidas em relação ao modelo 5G. A parte de análise deste relatório descreve os requisitos de segurança em vários casos de utilização. Além disso, houve soluções correspondentes que foram dadas com base nos requisitos.

A investigação sobre os aspetos de segurança teve a inclusão de diferentes variáveis que se prendem com a autenticação, privacidade, confidencialidade, disponibilidade e integridade do sistema. Na investigação, descobriu-se que o protocolo 5G-AKA, bem como a autenticação na camada física, deveria ter lugar através da substituição de algoritmos criptográficos pesados no ITS, uma vez que o protocolo 5G-AKA está provado ser mais eficiente do que este último.

É necessário adaptar o IBC para as comunicações V2X e depois, será sensato remover a infraestrutura do certificado do modelo ITS. No final, as perspetivas e orientações futuras têm sido discutidas e pertinentes a este campo de investigação. A existência das comunicações V2X veio muito antes do início do 5G. Nessa altura, os mecanismos de segurança, bem como a pilha de protocolos, tinham sido feitos para a padronização com a ajuda de tecnologia de ponta.

No entanto, não se pode negar que 5G está a possuir padrões modernos para tornar a vida mais fácil, confortável, e segura para os cidadãos do mundo. Uma vez que 5G possui avanços tecnológicos, muitos investigadores acreditam que 5G terá um enorme domínio sobre as comunicações V2X. No entanto, é desnecessário dizer que a segurança de 5G deve ser analisada minuciosamente e é necessário encontrar uma forma eficiente de ter integração com o modelo ITS existente.

Através de um Sistema de Gestão de Credenciais de Segurança (SCMS) para comunicações V2X, com especial ênfase na comunicação de aplicações de segurança V2V. Este desenho SCMS é um dos principais candidatos ao desenho do *backend* de segurança V2X nos EUA. Um dos desafios restantes é definir políticas que equilibrem a segurança, a privacidade e a eficiência que apoiarão o estabelecimento de um sistema de âmbito nacional.

A solução proposta utiliza cinco tipos de certificados para cobrir todas as categorias de aplicação V2X identificadas. Este texto centrou-se na segurança das comunicações de segurança V2V e no ciclo de vida dos certificados de pseudónimos da OBE, uma vez que este tipo de certificado requer maior consideração em termos de proteção da privacidade e complexidade.

O SCMS foi concebido para ser dimensionado em função do número de dispositivos e para proteger a privacidade dos utilizadores finais contra-atacantes internos e externos, através da separação de funções. Os próximos passos para a implementação de um SCMS são os seguintes:

- Definir uma difusão eficaz do LCR com base no conceito de Distribuição Colaborativa;
- Implementação de testes em larga escala de uma prova de conceito de SCMS;
- Desenvolvimento de algoritmos de deteção de comportamentos incorretos, implementação e teste de comunicação de comportamentos incorretos, investigação e deteção numa prova de implementação de conceito.

Algumas das limitações desta comunicação entre mecanismos V2X, em ambiente de 5G, supõem determinadas particularidades, nomeadamente:

- É importante ter encontrado a latência que está limitada a 1 milissegundo no nível máximo quando as situações de emergência têm lugar. Além disso, o piloto

automático neste caso é muito importante, o que é necessário para estar no dedo do pé para ajudar o condutor o mais rápido possível;

- É importante considerar o sistema de comunicação ultra fiável no que respeita ao veículo e à segurança para o público em geral. Embora tenham sido feitas tantas pesquisas neste sector, a ligação entre a Internet das Coisas (IoT) e os dispositivos conectados irá certamente tornar a questão complicada;
- Para além disso, é vital ter a investigação sobre a identificação de diferentes tipos de lacunas que possam revelar-se vulneráveis para o sistema de comunicação. Assim, é obrigatório ter um enorme trabalho a ser colocado na camada física para que a identificação seja mais fácil para os dados e equipamento. Outro desafio de investigação pode ser a utilização de técnicas ML que possam analisar eficazmente o comportamento anormal dos atacantes;
- No caso de operações de UAV, os principais fatores são a fiabilidade e a latência e estes fatores são necessários para serem aplicados na operação, para que a assistência da salvaguarda possa ser fornecida ao sistema de operação. Além disso, é importante que haja uma ligação constante entre a estação terrestre e o UAV para a transmissão ininterrupta de vídeo;
- Na comunicação do UAV, existem múltiplos problemas relacionados com a privacidade, bem como com a segurança, que são necessários para serem resolvidos. Os problemas estão relacionados com a falsificação, interferência e espionagem. A fim de proporcionar solução para os problemas, é essencial seguir soluções de IA e técnicas leves. Outros desafios relacionados com a comunicação de UAV podem ser a prevenção da colisão, bem como o apoio rápido e móvel que tem o potencial de ser pesquisado pelos investigadores;
- Uma ligação fiável juntamente com a rede de alta velocidade é necessária para os processos de monitorização. Caso contrário, os investigadores não serão capazes de possuir dados exatos e em tempo real para tomar decisões úteis. Contudo, a obtenção de alta velocidade e uma ligação segura é um problema que é necessário ser recuperado pelos investigadores;
- É necessário fornecer apoio aos protocolos de segurança do 3GPP SA3 e ter um compromisso com o sistema. Num determinado período de tempo, é importante tornar-se realista e pragmático, não se esperando que se perca nenhuma oportunidade de conceber coisas novas para a melhoria bem-sucedida de 5G;

- É obrigatório fornecer incentivos para apoiar a segurança da SDN/NFV. Além disso, são necessários estímulos para os produtos que possam dar apoio às funcionalidades sensíveis em diferentes tipos de ambientes visualizados;
- É também aconselhável ter uma comunicação adequada com as comunidades de código aberto e também, é necessário ter a defesa de que traria mais proteção ao código aberto;
- A garantia da segurança por defeito foi construída nos desenvolvimentos de 5G/ É também sugerido pelo relatório da FCCG que a segurança será necessária para ter demonstração como parte do programa de desenvolvimento. A investigação futura deverá também ter em conta o envolvimento dos programadores na conceção de 5G para que haja o estabelecimento de segurança e proteção na fase inicial.

Num futuro próximo, espera-se que a tecnologia de comunicação V2X revolucione o moderno sistema de transporte terrestre. Com o surgimento desta tecnologia moderna, as aplicações V2X serão potencialmente visadas pelas entidades maliciosas (como é evidente pelos recentes ataques do mundo real aos sistemas automóveis [43], [98]-[102]) e existe um requisito de mecanismo de defesa em camadas para melhorar a resiliência de tais sistemas.

Neste estudo, fornecemos uma visão geral das atuais normas de segurança V2X, potenciais ameaças à segurança e diferentes abordagens de deteção. Enquanto neste artigo o nosso enfoque principal na tecnologia V2X, os novos mecanismos de segurança desenvolvidos para aplicações V2X podem ser utilizados para melhorar a segurança de domínios cibernéticos de segurança mais vastos [100], [111]. Acreditamos que esta investigação será tangencial e valiosa para os investigadores académicos/indústria, desenvolvedores, engenheiros de sistemas e agências de normalização que trabalham em segurança de sistemas.

A arquitetura da camada do sistema 5G desempenhará um papel fundamental na entrega de comunicações C-V2X capazes de fornecer e sustentar QoS adaptadas a aplicações veiculares avançadas. Em particular, um conjunto de características notáveis é destacado em 5GCAR como crítico para as comunicações V2X. Neste documento, fornecemos uma visão geral do *design* da arquitetura 5GCAR, juntamente com conhecimentos sobre componentes selecionados, que argumentamos serem importantes para a implementação do V2X.

A negociação de serviços V2X e o agendamento consciente da localização fornecem à rede conhecimentos sobre o padrão de mobilidade e os requisitos de aplicação das UEs veiculares, permitindo à rede otimizar a prestação de serviços no espaço e no tempo, com repercussões positivas na eficiência da utilização dos recursos e, portanto, da disponibilidade e da escalabilidade das aplicações automóveis. A evolução da comunicação baseada em infraestruturas para tráfego V2X localizado trata da exigência de que o tráfego crítico de segurança seja tratado no mais curto espaço de tempo possível, reduzindo ao mínimo.

A comunicação veículo-veículo permite que os veículos trabalhem em conjunto para melhorar a segurança rodoviária, a gestão do tráfego e reduzir o impacto ambiental. Sendo uma tecnologia mais espectralmente eficiente, a 5G tem características atrativas tais como flexibilidade, fiabilidade e escalabilidade. A análise neste estudo revela que NR V2X supera LTE V2X em termos de latência e taxa de dados.

Numa configuração com uma largura de banda de canal de 10 MHz e espaçamento de subportadora (SCS) de 15 kHz, a taxa de dados para o protocolo NR V2X varia e o melhor desempenho é alcançado na configuração de 64-QAM com uma taxa máxima de 83,2 Mbps.

Os resultados desta análise mostram que o atraso da transmissão NR V2X proporciona um melhor desempenho. A taxa de dados LTE V2X é mais baixa para a configuração 64-QAM com um valor de 32,64 Mbps quando a configuração tem uma largura de banda de canal de 10 MHz e um espaçamento de subportadora (SCS) de 15 kHz, mas melhor em termos de taxa de dados com um valor de 64,8 Mbps quando a configuração tem uma largura de banda de canal de 20 MHz e um espaçamento de subportadora (SCS) de 30 kHz. A análise mostra os requisitos de segurança e soluções relacionadas para diferentes casos de utilização.

Os aspetos de segurança considerados são a confidencialidade, a integridade, a disponibilidade, a privacidade e a autenticação. Relativamente à autenticação, verificou-se que os algoritmos de encriptação que requerem ITS podem ser substituídos por protocolos AKA 5G (se estes se revelarem mais eficientes) e autenticação em camada física. Além disso, se o IBC for adaptado à comunicação V2X, a infraestrutura de autenticação no modelo ITS pode ser completamente eliminada. Finalmente, são descritas algumas sugestões para trabalhos futuros nesta área.

A comunicação V2X tem sido estudada muito antes do desenvolvimento da 5G. A pilha de protocolos ETSI ITS e os mecanismos de segurança foram normalizados de acordo com o nível técnico da altura.

Contudo, o desenvolvimento de 5G está a progredir rapidamente e já estão a ser publicadas novas normas e propostas no momento da redação do presente documento. Com a nova velocidade e outras inovações na tecnologia 5G, muitos investigadores e representantes da indústria preveem que 5G é a tecnologia do futuro para a comunicação V2X. Por conseguinte, é importante realizar uma análise exaustiva da segurança de 5G e de como esta pode ser integrada no modelo ITS existente. Esta é uma área muito ampla que oferece muitas novas direções para a investigação futura.

Bibliografia

[1] A. F. LEITE, *Redes de computadores*. 2020.

[2] K. Ganesan, P. B. Mallick, J. Lohr, D. Karampatsis, and A. Kunz, "5G V2X Architecture and Radio Aspects," *2019 IEEE Conf. Stand. Commun. Networking, CSCN 2019*, no. October, 2019, doi: 10.1109/CSCN.2019.8931319.

[3] Y. Z. A. Essaili, T. Lohmar, T. Nylander, "Cellular V2X: What can we expect on the road ahead?," *Cellular V2X: What can we expect on the road ahead?* ?", https://www.ericsson.com/en/blog/2019/10/cellular-v2x-the-road-ahead-c-its-adas.

[4] I. Mabiala, "COMUNICAÇÕES SEM FIO PARA CONDUÇÃO AUTÓNOMA." .

[5] M. M. Silva, "Os desafios da 4 Revolucao Industrial na Empregabilidade e no apoio as Pessoas Vulneraveis," *Auton. TechLab*, p. 4, 2019.

[6] "(PDF) Redes Veiculares: Princípios, Aplicações e Desafios." https://www.researchgate.net/publication/320595628_Redes_Veiculares_Principios_Aplicacoes_e_Desafios (accessed Aug. 30, 2022).

[7] B. M. Wangham, M. Nogueira, P. C. Fernandes, O. Paviani, and B. F. da Silva, "Capítulo 4: Segurança em Redes Veiculares: Inovações e Direções Futuras," *Minicursos do XIV Simpósio Bras. em Segurança da Informação e Sist. Comput.*

[8] Anritsu Ltd, "Intelligent Transportation Systems and IEEE 802.11p," *Anritsu Ltd*, 2016.

[9] V. Jindal, and P. Bedi, "Vehicular Ad-Hoc Networks: Introduction, Standards, Routing Protocols and Challenges," *IJCSI Int. J. Comput. Sci. Issues*, vol. 13, no. 2, pp. 44–55, 2016.

[10] V. Jindal and P. Bedi, "Vehicular Ad-Hoc Networks- Introduction, Standards, Routing Protocols and Challenges," *Int. J. Comput. Sci. Issues, IJCSI*, vol. 13, pp. 44–55, Mar. 2016, doi: 10.20943/01201602.4455.

[11] F. Yang, J. Li, T. Lei, and S. Wang, "Architecture and Key Technologies for Internet of Vehicles: A Survey," *J. Commun. Inf. Networks*, vol. 2, no. 2, pp. 1–17, 2017, doi: 10.1007/s41650-017-0018-6.

[12] K. and S. M. R. O. Singh, "Efficient and secure message transfer in VANET," *Inven. Comput. Technol. (ICICT), 2016 Int. Conf.*, 2016.

[13] R. C. Storck and D. F. Figueiredo, “5G V2X ecosystem providing Entertainment on board using mm wave communications,” *Proc. IEEE10th Latin-Amer. Conf. Commun. (LATINCOM*, pp. 1–6, 2018.

[14] R. Hoefel, “IEEE 802.11ac: A Performance Assessment of Single-User Transmit Beamforming and Multi User MIMO Transceiver Architectures,” *n ISWCS 2013; Tenth Int. Symp. Wirel. Commun. Syst.*, pp. 1–5, 2013.

[15] et al. S., Chen, “tecnologias, padrões e aplicações de LTE-V2X para redes veiculares,” *ciência das telecomunicações*, 2018.

[16] M. R. Masegosa and J. Gozalvez, “LTE-V para comunicações veiculares sidelink 5G V2X: Uma nova tecnologia 5G para comunicações de curto alcance veículo-para-tudo,” *IEEE Veh. Technol. Mag.*, vol. 12, no. 4, pp. 30–39, 2017.

[17] Janet Fleetwood, “Public Health, Ethics, and Autonomous Vehicles,” *Am. J. Public Health*, pp. 1–6, 2016.

[18] “Evoluído Universal Terrestrial Radio Access (E-UTRA),” *Control. Recur. rádio (RRC); Especificação do Protoc.*, vol. 14.12.0 Ve, 2019.

[19] “Evoluído Universal Terrestrial Radio Access (E-UTRA),” *Procedimentos de Camada Física*, vol. 14.3.0, 2017.

[20] “Especificação da camada de acesso para ITS Usando comunicação LTE-V2X,” 2018.

[21] K. . et al K. Zheng, “Reliable and efficient autonomous driving: the need for heterogeneous Vehicular networks,” *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 72–79, 2015.

[22] E. N. Elnozahy and J. S. Plank, “Checkpointing for Peta-scale systems: A look into the future of practical rollback-recovery,” *IEEE Trans. Dependable Secur. Comput.*, vol. 1, no. 2, pp. 97–108, 2004, doi: 10.1109/TDSC.2004.15.

[23] K. . et al K. Zheng, “Reliable and efficient autonomous driving: the need for heterogeneous Vehicular networks,” *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 72–79, 2015.

[24] U. C. Davis and U. C. Davis, *--University of California — --University of California —* , no. December 2013. 2014.

[25] C. De Gualtar, “Instituto Superior de Engenharia do Porto,” pp. 33940–33943, 2011.

[26] M. H. C. Garcia *et al.*, “A Tutorial on 5G NR V2X Communications,” *IEEE Commun. Surv. Tutorials*, vol. 23, no. 3, pp. 1972–2026, 2021, doi: 10.1109/COMST.2021.3057017.

[27] T. Specification, “Intelligent Transport Systems (ITS);,” vol. 1, pp. 1–48, 2021.

[28] R. Zaragatzky, “Security analysis of introducing 5G in V2X communications,” 2018, [Online]. Available: https://odr.chalmers.se/handle/20.500.12380/255942.

[29] R. Moalla, B. Lonc, H. Labiod, and N. Simoni, “How to secure ITS applications?,” *2012 11th Annu. Mediterr. Ad Hoc Netw. Work. Med-Hoc-Net 2012*, pp. 113–118, 2012, doi: 10.1109/MedHocNet.2012.6257110.

[30] ETSI, “ETSI TR 102 638 V1.1.1 (2009-06): Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions,” *ETSI, Sophia Antip. Cedex, Fr.*, vol. 1, pp. 1–81, 2009, [Online]. Available: http://scholar.google.com/scholar?hl=en%7B&%7DbtnG=Search%7B&%7Dq=intitle:Intelligent+Transport+Systems+(ITS);+Vehicular+Communicatons;+Basic+Set+of+Applications;+Definitions%7B#%7D1.

[31] “V2X Cellular Solutions,” *5G Am. Bellevue*, 2016.

[32] and X. G. X. Wang, S. Mao, “Uma visão geral dos padrões 3GPP de veículo para tudo,” *GetMobile Mob. Comput. Comuni.*, vol. 21, pp. 15–25, 2017.

[33] and A. T. A. Filippi, K. Moerman, V. Martinez, “White Paper: IEEE802.11p à frente do LTE-V2V, para aplicações de segurança,” 2017.

[34] J. Thompson, X. Ce, C. X. Wu, R. Irmer, G. Jiang, G. Fettweis, G. and A. Alamouti, “5G Wireless Communication Systems: Prospects and Challenges,” *IEEE Commun. Mag, o que está aqui?*, no. 52, pp. 62–64, 2014.

[35] G. and A. A. J. Thompson, X. Ce, C. X. Wu, R. Irmer, G. Jiang, G. Fettweis, “5G Wireless Communication Systems: Prospects and Challenges,” *IEEE Commun. Mag, o que está aqui?*, pp. 62–64, 2014.

[36] and J. C. Z. J. Andrews, G. Buzzi, S. Choi, W. Hanly, V. Lozano, S. A. E. A. C. K. Soong, “O que será o 5G?,” *IEEE J. Sel. Áreas Comunas.2014, 32, 1065-1082*, 2014.

[37] et al E. Dahlman, “5G Wireless Access: Requirements and Realization,” *IEEE Commun. Mag.*, vol. 52, pp. 42–47, 2014.

[38] “Evolução da Arquitetura de Redes Móveis Rumo ao 5G - PDF Download grátis.” https://docplayer.com.br/126833695-Evolucao-da-arquitetura-de-redes-moveis-rumo-ao-5g.html (accessed Aug. 30, 2022).

[39] A. Al-Fuqaha, “Internet of Things: A Survey On Enabling Technologies, Protocols, and Applications,” *IEEE Commun. Surv. Tutorials*, vol. 17, pp. 2347–2376, 2015.

[40] “ITU-R M.2410-0,” *R. Minim. Requir. Relat. to Tech. Perform. IMT-2020 Radio Interface(s)*, 2017.

[41] “Guidelines for Evaluation of Radio Interface Technologies for IMT-2020,” *ITU-R M.2412-0 Rep.*, 2017.

[42] and J. S. E. Dahlman, S. Parkvall, “5G NR: the next generation wireless access technology. Academic Press,” 2018.

[43] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, “Overview of 5G Security Challenges and Solutions,” *IEEE Commun. Stand. Mag.*, vol. 2, no. 1, pp. 36–43, 2018, doi: 10.1109/MCOMSTD.2018.1700063.

[44] S. Sullivan, A. Brighente, S. A. P. Kumar, and M. Conti, “5G Security Challenges and Solutions: A Review by OSI Layers,” *IEEE Access*, vol. 9, pp. 116294–116314, 2021, doi: 10.1109/ACCESS.2021.3105396.

[45] J. . et al Barrachina, “V2X-d: A vehicular density estimation system that combines V2V and V2I communications,” *Wirel. Days (WD), 2013 IFIP*, pp. 1–6, 2013.

[46] A. Molinaro and C. Campolo, “Contribution ‘ 5G for V2X ,’” pp. 2–6.

[47] “A caminhodos carros autónomos,” 2016. http://exameinformatica.sapo.pt/lifestyle/carros/23/02/2016-A caminho dos carros autónomos.

[48] “3GPP, Technical specification group services and system aspects; study on enhancement of 3GPP support for 5G V2X services,” *3rd Gener. Partnersh. Proj. (3GPP), Tech. Rep. 22.886*, 2018.

[49] 3GPP, “(E-UTRA), Evoluído Universal Terrestrial Radio Access; Controle de recursos de rádio (RRC).” p. 393, 2019, [Online]. Available: https://itecspec.com/archive/3gpp-

specification-ts-36-213/.

[50] R. Lu, L. Zhang, J. Ni, and Y. Fang, “5G Vehicle-to-Everything Services: Gearing up for Security and Privacy,” *Proc. IEEE*, vol. 108, no. 2, pp. 373–389, 2020, doi: 10.1109/JPROC.2019.2948302.

[51] “Proc. 3GPP Plenary Meeting,” *RP-181480 Novo SID Estud. sobre NR V2X*, vol. 80, pp. 1–10, 2018.

[52] D. Butler, “Como veículos falando e ouvindo poderiam tornar as estradas mais seguras cidades melhores,” 2019.

[53] “Avaliação da Alocação de Recursos NR V2X Mode 2,” 2019.

[54] B. Di, L. Song, Y. Li, and Z. Han, “V2X Meets NOMA : Non-Orthogonal Multiple Access for 5G Enabled Vehicular Networks,” no. May 2017, 2018, doi: 10.1109/MWC.2017.1600414.

[55] S. A. Busari *et al.*, “Millimeter-Wave Massive MIMO Communication for Future Wireless Systems : A Survey,” vol. 20, no. 2, pp. 836–869, 2018.

[56] R. De Janeiro, “Universidade Federal do Rio de Janeiro Núcleo de Computação Eletrônica Érico Asano de Mello RÁDIO COGNITIVO : Aspectos de segurança,” 2010.

[57] P. Xie, M. Zhang, G. Zhang, R. Zheng, L. Xing, and Q. Wu, “On physical-layer security for primary system in underlay cognitive radio networks,” pp. 68–73, 2018, doi: 10.1049/iet-net.2017.0138.

[58] J. Soliman, T. Mageed, and H. El-Hennawy, *Taxonomy of Security Attacks and Threats on Cognitive Radio Networks*. 2017.

[59] P. Rb and R. Universitario, “Politecnico di Torino Politecnico di Torino,” no. October, p. 87316161, 2020.

[60] “Esquemas de alocação de recursos para NR V2X Sidelink Communications,” 2018.

[61] “Resumo dos Aspectos da Convivência no Estudo NR-V2X,” 2018.

[62] “IMT Vision Framework and overall objectives of the future development of IMT for 2020 and beyond,” *Recomm. ITU-R M.2083*, 2015.

[63] and E. P. M. Kutila, P. Pyykonen, Q. Huang, W. Deng, W. Lei, “C-V2X supported automated driving,” *Proc. IEEE Int. Conf. Commun. Work. (ICC Work.*, pp. 1–5, 2019.

[64] “Discussão sobre a coexistência do sidelink LTE e do sidelink NR em NR V2X,” 2018.

[65] “Design para–NR V2X Groupcast Resource Allocation,” 2018.

[66] “Teste de benchmarking de tecnologia, V2X,” 2018.

[67] and J. G. M. R. Molina, “LTE-V para comunicações veiculares 5G V2X sidelink: Uma nova tecnologia 5G para comunicações de curto alcance veículo-para-tudo,” *IEEE Veh. Technol. Mag.*, vol. 12, no. 4, pp. 30–39, 2017.

[68] “Estudo sobre o Aprimoramento do Suporte 3GPP para serviços 5G V2X,” vol. 16.2.0 16, 2018.

[69] and A. J. M. Rajasekhar, “Veículos autónomos: O futuro dos automóveis,” *Process. da Conferência Int. Eletrificação Transp.*, 2015.

[70] and K. K. J. Sachs, G. Wikstrom, T. Dudda, R. Baldemair, “5G Radio Network Design for Ultra-Reliable Low-Latency Communications. IEEE 32,” pp. 24–31, 2018.

[71] SAE International, “SAE J2945/1: On-board system requirements for V2V safety communications.”

[72] and J. V. A. C. Serban, E. Poll, “A security analysis of the ETSI ITS vehicular communications,” *EWICS SAFECOMP*, pp. 365–373, 2018.

[73] S. A. Mohammed Ali and E. H. Al-Hemairy, “MINIMIZING E2E DELAY IN V2X OVER CELLULAR NETWORKS: REVIEW AND CHALLENGES,” *Iraqi J. Inf. Commun. Technol.*, vol. 2, no. 4, pp. 31–42, Feb. 2020, doi: 10.31987/IJICT.2.4.79.

[74] 5G American, “5G Americas White Paper: Cellular V2X Communications Towards 5G,” *Http://Www.5Gamericas.Org*, 2018.

[75] “Conhecendo o V2X - Conectando veículos para tudo - Embarcados.” https://embarcados.com.br/conhecendo-o-v2x/ (accessed Aug. 29, 2022).

[76] M. Boban, A. Kousaridas, K. Manolakis, J. Eichinger, and W. Xu, “Connected Roads of the Future,” *IEEE Veh. Technol. Mag.*, vol. 13, no. 3, pp. 110–123, 2018.

[77] S. A. Abdel Hakeem, A. A. Hady, and H. W. Kim, “5G-V2X: standardization, architecture, use cases, network-slicing, and edge-computing,” *Wirel. Networks*, vol. 26, no. 8, pp. 6015–6041, 2020, doi: 10.1007/s11276-020-02419-8.

[78] S. Chen, Q. Li, Y. Wang, H. Xu, and X. Jia, “C-V2X Gerenciamento de Identificação de

Equipamentos e Mecanismo de Autenticação," pp. 297–306, 2022.

[79] M. Muhammad and G. A. Safdar, "Survey on existing authentication issues for cellular-assisted V2X communication," *Veh. Commun.*, vol. 12, pp. 50–65, 2018, doi: 10.1016/j.vehcom.2018.01.008.

[80] K. Bian, G. Zhang, and L. Song, "Toward Secure Crowd Sensing in Vehicle-to-Everything Networks," *IEEE Netw.*, vol. 32, no. 2, pp. 126–131, 2018, doi: 10.1109/MNET.2017.1700098.

[81] J. A. L. Calvo and R. Mathar, "Secure Blockchain-Based Communication Scheme for Connected Vehicles," *2018 Eur. Conf. Networks Commun. EuCNC 2018*, pp. 347–351, 2018, doi: 10.1109/EuCNC.2018.8442848.

[82] H. Chai, S. Leng, F. Wu, and J. He, "Secure and Efficient Blockchain-Based Knowledge Sharing for Intelligent Connected Vehicles," *IEEE Trans. Intell. Transp. Syst.*, pp. 1–12, 2021, doi: 10.1109/tits.2021.3131240.

[83] Edemia, "Pesquisa Bibliográfica de Trabalhos Acadêmicos - saiba como." https://tccmonografiaseartigos.com.br/pesquisa-bibliografica-metodologia/.

[84] "V2X cellular solutions," *5G Am. Tech. Rep.*, 2016.

[85] and R. G. B. Brecht, D. Therriault, A. Weimerskirch, W. Whyte, V. Kumar, T. Hehn, "A security credential management system for V2X communications," *IEEE T-ITS*, vol. 19, no. 12, pp. 3850–3871, 2018.

[86] and B. L. F. Haidar, A. Kaiser, "On the performance evaluation of vehicular pki protocol for v2x communications security," *IEEE VTC-Fall. IEEE*, pp. 1–5, 2017.

[87] "Global harmonization of connected vehicle communication standards," *MDOT CAR Tech. Rep.*

[88] and A. L. H. Hasrouny, A. E. Samhat, C. Bassil, "VANET security challenges and solutions: A survey," *Veh. Commun.*, vol. 7, pp. 7–20, 2017.

[89] and A. L. H. Hasrouny, A. E. Samhat, C. Bassil, "VANet security challenges and solutions: A survey," *Elsevier Veh. Comm*, vol. 7, pp. 7–20, 2017.

[90] "Vehicle-to-vehicle communications misbehavior detection," *Veh. Saf. Commun. 6 Consortium, Tech. Rep.*

[91] "IEEE standard for wireless access in vehicular environments–security services for applications and management messages," *IEEE Std 1609.2-2016*, pp. 1–240, 2016.

[92] Y. J. Li, "An overview of the DSRC/WAVE technology," *EAI Qshine*, pp. 544–558, 2010.

[93] "ITS standards program: Development activities." https://www.standards.its.dot.gov/DevelopmentActivities/IntlHarmonization.

[94] and W. W. S. Cadzow, W. Hoefs, F. Kargl, R. Roy, S. Sill, "EUUS standards harmonization task group report: Feedback to standards development organizations–security," *Tech. Rep*, 2012.

[95] and C. S. J. P. Stotz, N. Bißmeyer, F. Kargl, S. Dietzel, P. Papadimitratos, "PRESERVE D1.1 security requirements of vehicle security architecture," *Preserv. Consort.*, 2011.

[96] " M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *IOS J. Comp. Sec.*, vol. 15 no. 1, pp. 39–68, 2007.

[97] C. Laurendeau and M. Barbeau, "Threats to security in DSRC/WAVE," *AdHoc-Now*, vol. 4104 LNCS, pp. 266–279, 2006, doi: 10.1007/11814764_22.

[98] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV," *Elsevier Ad Hoc Net*, pp. 33–50, 5153.

[99] and F. K. R. W. van der Heijden, S. Dietzel, T. Leinm¨uller, "Survey on misbehavior detection in cooperative intelligent transportation systems," *IEEE Commu. Sur. Tut*, 2018.

[100] and K. Z. A. Alipour-Fanid, M. Dabaghchian, H. Zhang, "String stability analysis of cooperative adaptive cruise control under jamming attacks," *String Stab. Anal. Coop. Adapt. cruise Control under jamming attacks*, pp. 157–162, 2017.

[101] and J. G. O. Punal, C. Pereira, A. Aguiar, "Experimental characterization and modeling of RF jamming attacks on VANETs," *IEEE TVT*, vol. 64, no. 2, pp. 524–540, 2015.

[102] and J. -l. B. A. I. A. Sumra, H. B. Hasbullah, "Effects of attackers and attacks on availability requirement in vehicular network: a survey," *IEEE ICCOINS*, pp. 1–6, 2014.

[103] and E. W. K. I. Aad, J.-P. Hubaux, "Denial of service resilience in ad hoc networks," *ACM MobiCom*, pp. 202–215, 2004.

[104] and B. X. B. Yu, C.-Z. Xu, “Detecting Sybil attacks in VANETs,” *J. Par. Dist. Comp.*, vol. 73, no. 6, pp. 746–756, 2013.

[105] and Y. C. M. Arshad, Z. Ullah, N. Ahmad, M. Khalid, H. Criuckshank, “A survey of local/cooperative-based malicious Information detection techniques in VANETs,” *EURASIP J. W. Comm. Net*, vol. 2018, no., p. 62, 2018.

[106] T. Leinm¨uller and E. Schoch, “Greedy routing in highway scenarios: The impact of position faking nodes,” *Proc. WIT*, 2006.

[107] and F. K. R. van der Heijden, T. Lukaseder, “Analyzing attacks on cooperative adaptive cruise control (CACC),” *IEEE VNC*, pp. 45–52, 2017.

[108] and K. L. M. Amoozadeh, A. Raghuramu, C. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, “Security vulnerabilities of connected vehicle streams and their impact on cooperative driving,” *IEEE Comm. Mag.*, vol. 53, no. 6, pp. 126–132, 2015.

[109] and M. R. D. Schmidt, K. Radke, S. Camtepe, E. Foo, “A survey and analysis of the GNSS spoofing threat and countermeasures,” *ACM CSUR*, vol. 48, no. 4, p. 64, 2016.

[110] V. Jindal and P. Bedi, “Vehicular Ad-Hoc Networks: Introduction, Standards, Routing Protocols and Challenges,” *Int. J. Comput. Sci. Issues*, vol. 13, no. 2, pp. 44–55, 2016, doi: 10.20943/01201602.4455.

[111] and J. G. O. Puñal, A. Aguiar, “In VANETs we trust? Characterizing RF jamming in vehicular networks,” *ACM VANET*, pp. 83–92, 2012.