



**Universidade de Brasília
Faculdade de Tecnologia**

**Modelagem e Simulação de Jamming
em Comunicação V2X**

Davi Salomão Soares Corrêa

PROJETO FINAL DE CURSO
ENGENHARIA DE CONTROLE E AUTOMAÇÃO

Brasília
2023

**Universidade de Brasília
Faculdade de Tecnologia**

Modelagem e Simulação de Jamming em Comunicação V2X

Davi Salomão Soares Corrêa

Projeto Final de Curso submetido como requisito parcial para obtenção do grau de Engenheiro de Controle e Automação

Orientador: Prof. Dr. Fernando William Cruz
Coorientador: Prof. Dr. Giovanni Almeida Santos

Brasília
2023

S676m Soares Corrêa, Davi Salomão.
Modelagem e Simulação de Jamming em Comunicação V2X /
Davi Salomão Soares Corrêa; orientador Fernando William
Cruz; coorientador Giovanni Almeida Santos. -- Brasília, 2023.
64 p.

Projeto Final de Curso (Engenharia de Controle e Automação)
-- Universidade de Brasília, 2023.

1. Veículos autônomos. 2. Rede de veículos. 3. Simu5G. 4.
Jamming. I. Cruz, Fernando William, orient. II. Santos, Giovanni
Almeida, coorient. III. Título

**Universidade de Brasília
Faculdade de Tecnologia**

Modelagem e Simulação de Jamming em Comunicação V2X

Davi Salomão Soares Corrêa

Projeto Final de Curso submetido como requisito parcial para obtenção do grau de Engenheiro de Controle e Automação

Trabalho aprovado. Brasília, 20 de dezembro de 2023:

Prof. Dr. Fernando William Cruz
UnB/FGA
Orientador

Prof. Dr. Giovanni Almeida Santos
UnB/FGA
Coorientador

Prof. Dr. José Alfredo Ruiz Vargas
UnB/FT/ENE
Examinador interno

Me. Antonio Arlis Santos da Silva
KIT/AIFB
Examinador externo

Brasília
2023

*Dedico este trabalho à minha mãe, Sandra, cujo apoio foi fundamental em minha jornada.
Sua inspiração me impulsionou a superar desafios e atingir meus objetivos.
Com amor, confiança e incentivo, você fortaleceu meu caminho.
Esta conquista também pertence a você.*

Agradecimentos

Gostaria de expressar meus agradecimentos ao meu orientador, Fernando William Cruz, por sua orientação e influência em meu progresso. Também sou grato ao meu coorientador, Giovanni Almeida Santos, por seu conhecimento, dedicação e comprometimento, os quais foram fundamentais para o sucesso deste trabalho.

Agradeço à minha mãe Sandra, às minhas irmãs Natália e Sabrina, e ao meu sobrinho Gabriel. Suas demonstrações de amor, apoio e compreensão foram inestimáveis para meu equilíbrio emocional durante todo o meu percurso acadêmico. Sou muito grato pelo incentivo e pelo suporte que recebi de vocês.

Não posso deixar de agradecer aos meus amigos Kayo, Isabella e Francisco. Sua amizade, encorajamento e apoio mútuo foram de extrema importância ao longo da minha jornada acadêmica. Obrigado por estarem sempre presentes e por compartilharem momentos de descontração e motivação.

A todos aqueles mencionados e a todos os que, de alguma forma, contribuíram para a realização deste trabalho, expressei meu agradecimento. Sem a colaboração e o apoio de cada um de vocês, esta conquista não teria sido possível. Sou grato por fazer parte de uma rede de pessoas tão especiais e inspiradoras.

“Even the smallest person can change the course of the future.”
(J. R. R. Tolkien)

Resumo

Veículos autônomos representam uma inovação promissora. Eles não apenas percebem e interpretam o ambiente ao redor, mas também são capazes de planejar rotas e gerenciar seus próprios movimentos. A evolução dessa tecnologia tem um impacto significativo tanto no trânsito quanto no avanço científico, destacando sua importância. Embora cada veículo perceba o meio localmente, a complexidade e as variações do ambiente limitam o desenvolvimento de um veículo totalmente autônomo. No entanto, com a evolução dos veículos em rede, é possível compensar os atrasos dos sensores, melhorar a percepção local do ambiente e estender para uma visão global. Tal avanço aproxima o desenvolvimento dessa tecnologia ao seu mais alto grau de autonomia. Para avaliar esse tema, foram realizadas simulações no Simu5G, permitindo o teste de cenários sem custos adicionais. Essas simulações abordaram especificamente os casos de uso *Do Not Pass Warning* (DNPW) e *Intersection Movement Assist* (IMA), que são definidos no *3rd Generation Partnership Project* (3GPP). Esses casos de uso foram então adaptados para incluir cenários de ataque *jamming* na comunicação 5G. Os resultados foram comparados com base em parâmetros como a qualidade de sinal, a taxa de perda de pacotes, a distância entre veículos e a potência de saída do *jammer*. Observou-se que a interferência do *jammer* prejudica as comunicações, afetando negativamente a qualidade de sinal e aumentando a taxa de perda de pacotes, o que aumenta o risco de colisões.

Palavras-chave: Veículos autônomos. Rede de veículos. Simu5G. *Jamming*.

Abstract

Autonomous vehicles represent a promising innovation. They not only perceive and interpret the surrounding environment, but are also able to plan routes and manage their own movements. The evolution of this technology has a significant impact on both traffic and scientific advancement, highlighting its importance. Although each vehicle perceives the environment locally, the complexity and variations of the environment limit the development of a fully autonomous vehicle. However, with the evolution of networked vehicles, it is possible to compensate for sensor delays, improve local perception of the environment and extend to a global view. This advance brings the development of this technology closer to its highest degree of autonomy. To evaluate this topic, simulations were carried out in Simu5G, allowing the testing of scenarios without additional costs. These simulations specifically addressed the Do Not Pass Warning (DNPW) and Intersection Movement Assist (IMA) use cases, which are defined in the 3rd Generation Partnership Project (3GPP). These use cases were then adapted to include jamming attack scenarios in 5G communication. The results were compared based on parameters such as signal quality, packet loss rate, distance between vehicles and jammer output power. Jammer interference has been observed to impair communications, negatively affecting signal quality and increasing the rate of packet loss, which increases the risk of collisions.

Keywords: Autonomous vehicles. Vehicle network. Simu5G. Jamming.

Lista de figuras

Figura 2.1	Arquitetura modular das ferramentas de simulação	30
Figura 3.1	Esquemático do caso de uso DNPW.	34
Figura 3.2	Cenário DNPW com ênfase no ataque <i>jamming</i>	35
Figura 3.3	Esquemático do caso de uso IMA.	36
Figura 3.4	Cenário IMA com ênfase no ataque <i>jamming</i>	36
Figura 3.5	Diagrama de blocos da camada física no Simu5G	40
Figura 4.1	Realização do ataque no cenário DNPW	42
Figura 4.2	Parâmetros no cenário DNPW entre o transmissor car[0] e o receptor car[2]	43
Figura 4.3	Parâmetros no cenário DNPW entre o transmissor car[1] e o receptor car[2]	44
Figura 4.4	Variação da taxa de perda de pacotes entre car[0] e car[2] no DNPW	45
Figura 4.5	Variação da qualidade de sinal entre car[0] e car[2] no DNPW	46
Figura 4.6	Variação da taxa de perda de pacotes entre car[1] e car[2] no DNPW	46
Figura 4.7	Variação da qualidade de sinal entre car[1] e car[2] no DNPW	47
Figura 4.8	Realização do ataque no cenário IMA	48
Figura 4.9	Parâmetros no cenário IMA entre o transmissor car[0] e o receptor car[2]	49
Figura 4.10	Parâmetros no cenário IMA entre o transmissor car[1] e o receptor car[2]	50
Figura 4.11	Variação da taxa de perda de pacotes entre car[0] e car[2] no IMA	51
Figura 4.12	Variação da qualidade de sinal entre car[0] e car[2] no IMA	52
Figura 4.13	Variação da taxa de perda de pacotes entre car[1] e car[2] no IMA	52
Figura 4.14	Variação da qualidade de sinal entre car[1] e car[2] no IMA	53
Figura A.1	Cenário DNPW no SUMO	62
Figura A.2	Etapa final do ataque no cenário DNPW	62
Figura A.3	Cenário IMA no SUMO	63
Figura A.4	Etapa final do cenário IMA	63

Lista de tabelas

Tabela 2.1	Parâmetros V2X na literatura	28
Tabela 3.1	Parâmetros V2X configurados na simulação	37
Tabela 3.2	Parâmetros de ataque <i>jamming</i> configurados na simulação	39
Tabela A.1	Mecanismos de ataque <i>jamming</i>	59
Tabela B.1	Cronograma de atividades do TG	64

Lista de abreviaturas e siglas

3GPP	<i>3rd Generation Partnership Project</i>	24
ARES	<i>Anti-jamming Reinforcement System</i>	21
BS	<i>Base Station</i>	21
BSM	<i>Basic Safety Message</i>	22
C-GDBN	<i>Coupled Generalized Dynamic Bayesian Network</i>	25
C-V2X	<i>Cellular Vehicle to Everything</i>	18
CBR	<i>Constant Bit Rate</i>	37
CV	<i>Connected Vehicles</i>	25
D2D	<i>Device-to-Device</i>	40
dBm	<i>decibéis-miliWatt</i>	32
DKF	<i>Distributed Kalman Filtering</i>	20
DNPW	<i>Do Not Pass Warning</i>	34
DQN	<i>Deep Q-Network</i>	19
DRL	<i>Deep Reinforcement Learning</i>	20
DSRC	<i>Dedicated Short-Range Communications</i>	18
ETA	<i>Estimated Time of Arrival</i>	26
FCC	<i>Federal Communications Commission</i>	18
FDD	<i>Frequency Division Duplex</i>	29
GDBNs	<i>Generalized Dynamic Bayesian Networks</i>	21
GNSS	<i>Global Navigation Satellite System</i>	24
GPS	<i>Global Positioning System</i>	22
I-SIG	<i>Intelligent Signal</i>	26
IMA	<i>Intersection Movement Assist</i>	34
IMU	<i>Inertial Measurement Unit</i>	24
ITS	<i>Intelligent Transportation System</i>	18
M-MJPF	<i>Modified Markov Jump Particle Filter</i>	21
MAC	<i>Media Access Control</i>	22
MSF	<i>Multi-Sensor Fusion</i>	27
mW	<i>miliWatt</i>	32
OSI	<i>Open Systems Interconnection</i>	39
PHY	<i>Physical Layer</i>	22
PLR	<i>Packet Loss Ratio</i>	33
RAN	<i>Radio Access Network</i>	39
RF	<i>Radio Frequency</i>	24
ROC	<i>Receiver Operating Characteristic</i>	22
RSSI	<i>Received Signal Strength Indicator</i>	25

RSU	<i>Road Side Unit</i>	25
SINR	<i>Signal-to-Interference-plus-Noise Ratio</i>	19
SNR	<i>Signal-to-Noise Ratio</i>	22
SPS	<i>Semi-Persistent Scheduling</i>	22
TDD	<i>Time Division Duplex</i>	29
TDOA	<i>Time Difference of Arrival</i>	25
TG	<i>Trabalho de Graduação</i>	64
TraCI	<i>Traffic Control Interface</i>	30
TSC	<i>Traffic Signal Control</i>	25
UDP	<i>User Datagram Protocol</i>	21
UE	<i>User Equipment</i>	29
UMa	<i>Urban Macrocellular</i>	24
UMi OS	<i>Urban Microcellular Open Square</i>	24
UMi SC	<i>Urban Microcellular Street Canyon</i>	24
USRP	<i>Universal Software Radio Peripheral</i>	24
V2I	<i>Vehicle to Infrastructure</i>	18
V2N	<i>Vehicle to Network</i>	19
V2P	<i>Vehicle to Pedestrian</i>	19
V2V	<i>Vehicle to Vehicle</i>	18
V2X	<i>Vehicle to Everything</i>	16
VoD	<i>Video on demand</i>	37
VoIP	<i>Voice over IP</i>	37
WAVE	<i>Wireless Access in Vehicular Environments</i>	18
WLAN	<i>Wireless Local Area Network</i>	18

Lista de símbolos

Δf	<i>Bandwidth</i>	32
k_B	Constante de Boltzmann	32
N^{rx}	Número total de pacotes recebidos	33
N^{tx}	Número total de pacotes transmitidos	33
P_i	Potência da interferência	31
P_j	Potência do <i>jammer</i>	32
P_n	Potência do ruído	31
P_s	Potência do sinal	31
P_T	Potência do ruído térmico	32
T	Temperatura	32

Sumário

1	Introdução	15
1.1	Objetivos	16
1.2	Estruturação do trabalho	17
2	Referencial teórico	18
2.1	Contextualização	18
2.2	Revisão bibliográfica	19
2.3	Estado da arte de parâmetros V2X	28
2.4	Ferramentas de simulação	29
2.5	Modelagem do ataque <i>jamming</i>	31
3	Metodologia	34
3.1	Ataque <i>jamming</i> no cenário DNPW	34
3.2	Ataque <i>jamming</i> no cenário IMA	35
3.3	Implementação dos cenários V2X no Simu5G	37
3.4	Implementação do ataque <i>jamming</i> no Simu5G	38
4	Resultados	42
4.1	Simulação do cenário DNPW	42
4.2	Parâmetros analisados no cenário DNPW	43
4.3	Parâmetros afetados pelo ataque no cenário DNPW	44
4.4	Simulação do cenário IMA	47
4.5	Parâmetros analisados no cenário IMA	48
4.6	Parâmetros afetados pelo ataque no cenário IMA	50
5	Conclusões	54
	Referências	55
	Apêndices	58
	Apêndice A Tipos de ataque <i>jamming</i>	59
	Apêndice B Códigos de programação	60
	Anexos	61
	Anexo A Figuras dos cenários	62
	Anexo B Cronograma de atividades	64

1 Introdução

Os veículos autônomos representam uma inovação promissora no universo da tecnologia automotiva. Tais veículos possuem a capacidade de interpretar o ambiente ao redor, traçar rotas e gerenciar seu próprio movimento, enquanto mantêm uma interação contínua com os motoristas (Kato *et al.*, 2015).

Nesse sentido, a exploração cuidadosa e o entendimento profundo dessa tecnologia tornam-se fundamentais no setor automotivo, visto que sinalizam o início de uma transformação revolucionária no sistema de transporte, com capacidade para influenciar positivamente vários segmentos da sociedade.

Os meios de mobilidade autônoma detêm um potencial imenso de oferecer uma gama de benefícios significativos. Tais tecnologias emergentes possuem a capacidade de melhorar a mobilidade, minimizar o consumo de energia e as emissões de gases de efeito estufa, reduzir o tempo de deslocamento e ainda podem levar a uma diminuição na necessidade de cada indivíduo ter um veículo pessoal (Othman, 2021).

Os veículos autônomos, com sua crescente complexidade e necessidades de processamento, estão se tornando mais dependentes das redes de *edge computing*. Tal dependência destaca a importância da infraestrutura de computação robusta e confiável para garantir uma operação segura e eficiente nas estradas e rodovias do mundo real (Seredynski, 2021).

Segundo (Tong *et al.*, 2019), o progresso notável nas comunicações, nos sistemas de transporte inteligentes e nos sistemas computacionais tem desbravado novos caminhos para soluções inovadoras de segurança, conforto e eficiência no trânsito. Tais avanços estão redefinindo a paisagem do transporte moderno.

No contexto dos veículos autônomos, a rede intra-veicular é vital, pois conecta os componentes eletrônicos embarcados, sendo indispensável para a condução autônoma (Tong *et al.*, 2019). Ela coordena os sistemas do veículo, garantindo respostas adequadas às condições de trânsito e contribuindo para uma experiência de condução confiável.

Cada veículo autônomo pode ser equipado com unidades de controle eletrônico, que estão interligadas através de uma série de redes intra-veiculares, formando uma malha de comunicação (Hbaieb; Rhaiem; Chaari, 2018). Tal configuração permite uma coordenação entre os sistemas do veículo, desde o controle de motor até os sistemas de segurança.

A rede intra-veicular não apenas permite a comunicação eficiente entre os diversos componentes do veículo, mas também facilita o controle coordenado e a resposta rápida aos comandos. Ela é o elemento central que permite a operação sincronizada das funções do veículo, garantindo uma condução robusta.

Em contrapartida, a rede inter-veicular estabelece o canal de interação entre os veículos e as informações externas (Tong *et al.*, 2019). Tais redes, além de conectarem os componentes eletrônicos embarcados, habilitam os veículos a compartilhar e transmitir informações sincronicamente, promovendo uma comunicação eficaz tanto entre os veículos e com o entorno.

A implementação da rede inter-veicular aperfeiçoa a percepção ambiental do veículo autônomo e enriquece os dados fornecidos pelos sensores. Contudo, à medida que os veículos evoluem para um estado de maior conectividade, torna-se essencial reconhecer que tal expansão da conectividade carrega consigo um risco ampliado de exposição a ataques cibernéticos (Guan *et al.*, 2022).

De acordo com (Silva *et al.*, 2023), *jamming* em *Vehicle to Everything* (V2X) é um ataque de cibersegurança, que envolve a geração intencional de interferência eletromagnética, o que pode resultar em comprometimento da comunicação. A gravidade desse tipo de ataque reside na sua capacidade de comprometer a troca de informações entre veículos e infraestruturas, o que pode levar a situações perigosas no trânsito.

Diante disso, a segurança cibernética é um aspecto fundamental na implementação de sistemas V2X. A compreensão e a mitigação de ataques como o *jamming* são, portanto, fundamentais para garantir a segurança desses sistemas. Este trabalho visa contribuir para esse campo, explorando simulação de cenários de ataque de *jamming* em V2X.

1.1 Objetivos

O objetivo principal deste trabalho é modelar e simular cenários em uma rede de veículos autônomos, utilizando a estrutura de rede V2X em comunicação 5G NR. Para atingir tal propósito, busca-se alcançar os seguintes objetivos específicos:

- Explorar as funcionalidades e aplicações do simulador Simu5G em cenários V2X.
- Modelar e simular cenários de caso de uso V2X no Simu5G, incluindo adaptação de cenários com ataque *jamming*.
- Implementar o nó *jammer* para dar suporte a simulações de casos de uso com ataques.
- Demonstrar a influência do ataque *jamming* no canal de comunicação, em particular, nos parâmetros qualidade de sinal e taxa de perda de pacotes.

1.2 Estruturação do trabalho

- Introdução

O [Capítulo 1](#) apresenta a motivação para o estudo de redes de veículos autônomos e explora os desafios associados aos ataques cibernéticos em tais redes. Ademais, também estabelece os objetivos gerais e específicos que orientam o restante do trabalho.

- Referencial teórico

O [Capítulo 2](#) realiza uma revisão bibliográfica, apresentando definições essenciais associadas ao ataque de *jamming*. Além disso, aborda os aspectos técnicos e as ferramentas de simulação empregadas na pesquisa.

- Metodologia

O [Capítulo 3](#) descreve a modelagem do ataque *jamming* em uma rede de veículos, abordando os métodos de simulação implementados no Simu5G. Ademais, discute os cenários selecionados para análise, explicando sua relevância para o estudo.

- Resultados

O [Capítulo 4](#) destaca observações e inferências derivadas dos resultados obtidos. Este capítulo apresenta uma análise detalhada, comparando parâmetros como qualidade de sinal, taxa de perda de pacotes, distância entre veículos e potência de saída do *jammer* durante o ataque, em relação aos cenários típicos de casos de uso em V2X.

- Conclusão

Por fim, o [Capítulo 5](#) oferece um resumo dos principais resultados e suas implicações, além das considerações finais sobre a modelagem do ataque de *jamming* em uma rede de veículos autônomos. Além disso, explora-se possíveis linhas de pesquisa e perspectivas futuras relacionadas ao tema.

2 Referencial teórico

Neste capítulo, é apresentado o modelo de rede de comunicação V2X, com uma discussão sobre as aplicações em redes de veículos autônomos e suas vulnerabilidades. Realiza-se uma revisão bibliográfica para elucidar as definições fundamentais para o entendimento do tema. Além disso, o capítulo aborda o estado da arte de parâmetros V2X, a modelagem do *jamming* e as ferramentas de simulação utilizadas na pesquisa.

2.1 Contextualização

V2X é reconhecido como uma tecnologia emergente que possui a capacidade de melhorar a eficiência e a mobilidade do tráfego urbano, além de aumentar a segurança dos motoristas. No entanto, ainda se enfrentam desafios relacionados à privacidade e segurança nas implementações de V2X. (Yang *et al.*, 2022b).

Conforme indicado em (Harounabadi *et al.*, 2021), a rede móvel 5G emerge como uma tecnologia promissora para redes veiculares, abrangendo a tecnologia de comunicação veicular denominada *Cellular Vehicle to Everything* (C-V2X). Essa tecnologia, com sua capacidade de alta velocidade e baixa latência, promete transformar a maneira como os veículos se comunicam entre si e com a infraestrutura ao redor.

Existem pesquisas em andamento para empregar padrões baseados na IEEE, como *Dedicated Short-Range Communications* (DSRC) no padrão IEEE 802.11p. Contudo, a comunicação C-V2X se mostra mais apropriada, em razão de suas características inovadoras e à capacidade de suportar uma diversidade de casos de uso.

No ano de 1999, a *Federal Communications Commission* (FCC) destinou 75 MHz do espectro de DSRC na frequência de 5.9 GHz para uso exclusivo em comunicações de *Vehicle to Vehicle* (V2V) e *Vehicle to Infrastructure* (V2I) (Moradi-Pari *et al.*, 2023). Essa destinação propiciou o desenvolvimento e a implementação de tecnologias de comunicação veicular, resultando em progressos significativos na segurança dos meios de transporte.

O DSRC é um protocolo de comunicação fundamentado em WLAN que facilita a conexão de veículos em aplicações de *Intelligent Transportation System* (ITS). Este protocolo funciona com base no padrão IEEE 802.11p, integrante do protocolo WAVE nos Estados Unidos (Jiang; Delgrossi, 2008).

O NR-V2X é apresentado com 5G NR e coexistirá com o LTE-V2X para dar suporte a aplicações avançadas, tais como comboio de veículos, condução autônoma, condução remota e sensores estendidos, entre outras (Chen *et al.*, 2020). Essa coexistência possibilitará que os sistemas de transporte inteligentes maximizem as vantagens de ambas as tecnologias, proporcionando uma experiência de condução mais confiável.

C-V2X emprega e aprimora as redes celulares já existentes para possibilitar comunicações ágeis e seguras entre diversos nós em redes veiculares, abrangendo V2V, *Vehicle to Pedestrian* (V2P), V2I, *Vehicle to Network* (V2N), entre outras topologias de redes (Chen *et al.*, 2017). Assim sendo, este trabalho dá ênfase ao NR-V2X, explorando suas potencialidades e contribuições para a evolução de comunicações veiculares.

2.2 Revisão bibliográfica

O estudo descrito em (Yao *et al.*, 2023) desenvolve uma abordagem ativa *anti-jamming*. A proposta identifica o sinal invasor e utiliza técnicas baseadas em *Deep Q-Network* (DQN) para selecionar dinamicamente os canais e a intensidade do sinal. Esta abordagem inovadora abre novas possibilidades para aprimorar a segurança das redes veiculares.

O ataque em questão é realizado por um *eavesdropper*, responsável por monitorar as comunicações, enquanto outros quatro *jammers* emitem sinais disruptivos na camada física do sistema. Este cenário complexo enfatiza a necessidade de soluções robustas e adaptáveis para garantir a integridade das comunicações veiculares.

Neste cenário, destaca-se a presença de dois tipos distintos de ataques. O primeiro é um *eavesdropper* especializado em monitorar as comunicações V2V, introduzindo riscos significativos à segurança do sistema. O segundo tipo de *jammer* foca na emissão de sinais de interferência com o objetivo de degradar a qualidade da transmissão.

A ação combinada desses dois tipos de ataques resulta na deterioração da relação de qualidade do sinal *Signal-to-Interference-plus-Noise Ratio* (SINR) para os usuários da rede de veículos. Tal ataque não apenas afeta a qualidade da comunicação, mas também causa uma série de complicações adicionais. Estas complicações podem variar desde atrasos na transmissão de dados até falhas completas na comunicação, impactando negativamente a segurança do sistema de transporte.

O objetivo central deste estudo é propor uma contramedida capaz de mitigar os efeitos desses ataques de *jamming*. Para isso, é introduzida uma abordagem baseada em técnicas de aprendizado de máquina. Tal abordagem visa melhorar substancialmente a segurança das comunicações V2V.

Assim sendo, a proposta de solução está na otimização da taxa de sigilo do sistema, garantindo simultaneamente a qualidade da comunicação. Sendo esses resultados alcançáveis mesmo sob a constante ameaça de possíveis tentativas de espionagem e interferência nos sinais de comunicação.

Durante a fase de simulação, uma série de parâmetros cruciais são definidos. Estes incluem um limiar necessário para SINR de 3 dB, bem como diferentes potências de transmissão V2V, variando entre 16, 19, 21 e 22 dBm. Assim como, os parâmetros específicos da camada física, como *carrier frequency* de 5,9 GHz e *bandwidth* de 10 MHz.

Na análise dos resultados, torna-se evidente que os ataques de *jamming* têm um impacto significativo. A interferência introduzida compromete diretamente o desempenho dos veículos conectados, afetando a precisão da estimativa de localização. Este comprometimento é particularmente preocupante, pois a localização precisa é crucial para a operação segura dos veículos autônomos.

À medida que a interferência aumenta, isso se desdobra em um cenário onde a SINR diminui, resultando em uma deterioração notável na qualidade da comunicação. Este declínio na qualidade não é apenas um inconveniente, mas uma ameaça direta à funcionalidade do sistema de transporte.

Conseqüentemente, a taxa de transmissão é reduzida, o que significa que os veículos não conseguem comunicar informações críticas de maneira oportuna. Além disso, a confiabilidade da comunicação é prejudicada, o que pode levar a erros de comunicação entre os veículos.

Esses efeitos combinados refletem substancialmente na taxa de sigilo, uma métrica crítica que mede a segurança das comunicações em redes de veículos. A redução na taxa de sigilo indica que as comunicações entre os veículos estão cada vez mais vulneráveis a ataques cibernéticos, colocando todo o sistema de transporte em risco.

O estudo apresenta contramedidas avançadas para enfrentar ataques intrincados. Ele emprega uma fusão de métodos, *Distributed Kalman Filtering* (DKF) para rastreamento e *Deep Reinforcement Learning* (DRL) para defesa. Além disso, adota uma estratégia hierárquica de DQN para otimizar a defesa. A combinação dessas estratégias melhora significativamente a segurança das comunicações entre veículos.

O artigo ([Pelechrinis et al., 2011](#)) explora a eficácia de duas funções cruciais da camada física, adaptação de taxa e controle de potência, para combater ataques de *jamming* em uma rede 802.11 interna. A adaptação de taxa envolve a seleção dinâmica da taxa de transmissão de dados ideal com base nas condições atuais do canal, enquanto o controle de potência ajusta a potência de transmissão para manter a qualidade do sinal desejada.

Quando um *jammer* realiza interferência, descobriu-se que o uso de algoritmos comuns de adaptação de taxa pode reduzir significativamente o desempenho da rede. No entanto, ajustando cuidadosamente o limiar de detecção de portadora, um nó de transmissão ainda pode enviar pacotes mesmo sob condições de *jamming*, permitindo que o receptor capture o sinal pretendido.

No cenário de ataque escolhido, um *random jamming* é analisado. Este tipo de ataque é caracterizado pela capacidade de transmitir sinais de forma não previsível. Esta natureza de ataque e a velocidade dessas transmissões tornam esse tipo de ataque particularmente desafiador, pois pode sobrecarregar os canais de comunicação de forma eficaz.

O *jammer* opera transmitindo tráfego de *User Datagram Protocol* (UDP) de transmissão, o que lhe permite adiar transmissões consecutivas. Ele alterna entre estados ativos e ociosos de maneira cíclica, transmitindo continuamente pacotes durante sua fase ativa antes de entrar em intervalos de economia de energia durante seu estado ocioso.

Os parâmetros de simulação foram definidos com cuidado para abranger elementos essenciais. Tais elementos incluem um limiar SINR crítico de 6 dB, uma faixa de potência de transmissão para comunicação V2V entre 1 e 18 dBm, uma frequência portadora de 5,9 GHz e uma largura de banda de 10 MHz.

Para combater ataques de *jamming*, foi concebido o *Anti-jamming Reinforcement System* (ARES). A contramedida ARES aprimora o desempenho em cenários de interferência ajustando os parâmetros de adaptação de taxa e controle de potência, garantindo operações contínuas na rede mesmo sob condições adversas.

Portanto, esta investigação apresenta o desenvolvimento, implementação e avaliação do ARES, um poderoso sistema *anti-jamming* projetado para redes 802.11p. ARES é mostrado como eficaz em três implantações diferentes, demonstrando sua adaptabilidade em vários contextos. Como complemento a outras técnicas de mitigação de *jamming*, ARES eleva o desempenho em ambientes afligidos por interferência de *jamming*.

A tecnologia V2X está revolucionando a maneira como pensamos sobre o transporte, melhorando a eficiência do tráfego, a segurança do trânsito e possibilitando a condução autônoma (Krayani *et al.*, 2022). Ela está transformando a infraestrutura de transporte existente em um ecossistema dinâmico e responsivo, onde os veículos podem se comunicar não apenas entre si, mas também com a infraestrutura e outros elementos ao seu redor.

No entanto, à medida que os veículos se tornam mais interconectados, eles também se tornam mais vulneráveis a ameaças de segurança, como ataques de *jamming*. Esses ataques podem interromper as comunicações vitais entre veículos e infraestruturas, colocando em risco a segurança dos passageiros e a eficiência do tráfego. Para abordar essa questão, foi proposto um *framework* para detectar *jammers* nas comunicações V2X.

O *framework* utiliza técnicas avançadas, como *Generalized Dynamic Bayesian Networks* (GDBNs) e *Modified Markov Jump Particle Filter* (M-MJPF), para rastreamento dos sinais no ambiente V2X e predizer sinais com precisão. Ao comparar os sinais observados com os previstos, o *framework* é capaz de detectar a presença de um *jammer* e melhorar a proteção e a eficiência geral das comunicações V2X.

Nas simulações, foi considerada uma rede veicular composta por vários veículos conectados trocando informações de coordenadas de posição com uma *Base Station* (BS). O ataque consiste em um veículo malicioso *jammer* que transmite sinais de interferência com a intenção de interromper as comunicações legítimas de V2I.

O método proposto empregou um modelo de comutação probabilística baseado em GDBN para aprender uma representação do ambiente de rádio V2X e identificar ataques de *jammer* nas comunicações veiculares entre BS e os veículos. Este modelo é particularmente eficaz na modelagem de ambientes de rádio dinâmicos e complexos.

Para simular as condições do canal, foram utilizados sinais 4G em cenários onde a qualidade do sinal sofre variações rápidas e de grande magnitude. Como métrica de avaliação, foram empregadas as curvas de desempenho de *Receiver Operating Characteristic* (ROC).

Os resultados mostraram que o método proposto é capaz de detectar ataques de *jamming* sob níveis razoáveis *Signal-to-Noise Ratio* (SNR). Trabalhos futuros visam testar o modelo em um cenário urbano com maior densidade de distribuição de veículos e lidar com *jammers* atacando com baixa potência. Estratégias *anti-jamming* de técnicas de aprendizagem de máquina para segurança também podem ser implementadas.

Em (Twardokus; Rahbari, 2023), investiga-se vulnerabilidades tanto na *Physical Layer* (PHY), quanto na *Media Access Control* (MAC) da comunicação 5G C-V2X. A pesquisa não apenas identificou as possíveis problemáticas, mas também projetou e conduziu experimentos para validar a gravidade de dois ataques.

O primeiro ataque consiste em interferência direcionada na ligação lateral, enquanto o segundo em exaustão de recursos da ligação lateral. Esses novos métodos de ataque foram especificamente criados para explorar as fraquezas inerentes à camada física baseada em intervalos de transmissão do C-V2X e no algoritmo *Semi-Persistent Scheduling* (SPS).

Em conjunto com a descrição desses ataques, a equipe forneceu recomendações perspicazes sobre como mitigar os efeitos adversos de tais explorações. O objetivo principal da equipe de pesquisa era simular ataques que pudessem avaliar com precisão as vulnerabilidades no sistema C-V2X existente.

A construção de um modelo de ameaça abrangente para ataques de interferência do C-V2X envolveu a definição de parâmetros críticos, incluindo elementos como o nível de potência C-V2X padronizado de 23dBm e a sincronização com os sinais do *Global Positioning System* (GPS). Além disso, a entidade de interferência deve aderir aos requisitos SPS estipulados, que abrangem a seleção periódica de recursos de comunicação.

O processo de interferência direcionada na ligação lateral consiste em seis etapas distintas: ouvir, gravar, antecipar, interferir, monitorar e atualizar. Em cada intervalo de tempo de transmissão, a entidade de interferência intercepta todas as *Basic Safety Messages* (BSMs) e as filtra para identificar mensagens do alvo.

Ao receber e reconhecer com sucesso um BSM do alvo, o dispositivo de ataque grava o intervalos de transmissão correspondentes e as informações de canal único que o alvo emprega para transmitir. Usando os dados gravados, o interferidor calcula os intervalos de tempo de transmissão para os próximos BSMs do alvo.

Nos intervalos de tempo de transmissão calculados, o dispositivo de ataque transmite um sinal de banda estreita, estrategicamente destinado a colidir com o campo canal do alvo. O objetivo é interromper o bloco de transmissão associado de uma maneira que o torne a recuperação difícil ou impossível.

Entre os intervalos de transmissão reservados para interferência, o dispositivo de ataque permanece atento a quaisquer BSMs potenciais do alvo, mesmo em intervalos imprevistos. Se a fase de monitoramento revelar qualquer nova seleção de recursos por parte do alvo, significando mudanças no intervalo de transmissão ou subcanais, o interferidor atualiza seu registro e retoma a interferência nos BSMs do alvo seguindo a estratégia anterior.

A estratégia de ataque de exaustão de recursos da ligação lateral tem duas variantes distintas. Na primeira variante, aleatorização de transmissões legítimas, os interferidores lançam ataques aos alvos sem preparação prévia. Embora a configuração do canal global seja predeterminada, o dispositivo de ataque tem a flexibilidade de definir aleatoriamente os tamanhos dos subcanais e manipular o conteúdo das mensagens.

Posteriormente, o interferidor envia um contador de seleção de recursos SPS, normalmente fixo para veículos comuns, alterando assim a alocação de recursos do veículo alvo para imitar uma transmissão normal. A introdução de perturbações no SPS também faz parte desta estratégia.

Na segunda variante, explorando o canal único de transmissão para abuso preditivo de SPS, os protocolos C-V2X incluem um campo crucial de reserva de recursos em cada mensagem do canal. Este campo reserva desempenha um papel fundamental durante a seleção de recursos.

Os veículos de ataque podem prever os recursos do veículo alvo ouvindo o canal por um breve período, um intervalo BSM de 100ms, gravando o valor de recursos de cada mensagem decodificada no canal. Os interferidores podem aplicar esta técnica para atingir vários veículos dentro do mesmo sistema.

Por fim, são sugeridas soluções para mitigar o dano potencial causado por esses ataques. Em relação à interferência direcionada na ligação lateral, sugere-se aproveitar o suporte do NR-V2X para transmissões aperiódicas. Além disso, para a exaustão de recursos da ligação lateral, é recomendado reduzir a duração do período de escuta do SPS, diminuindo assim a janela de vulnerabilidade.

A rede 5G C-V2X está emergindo como a tecnologia dominante para veículos conectados. Uma aplicação crítica do 5G C-V2X é a troca direta de mensagens de segurança entre veículos para prevenir acidentes (Yang *et al.*, 2022a). O desenvolvimento de aplicações de sistema ITS é significativamente impedido pela falta de soluções de segurança bem projetadas para comunicações C-V2X de mmWave.

O bloqueio e a estratégia de seleção de interferência baseada em potência são propostos no artigo (Yang *et al.*, 2022a) para abordar possíveis armadilhas de segurança em uma rede C-V2X mmWave. Os protocolos de segurança C-V2X atuais se preocupam apenas com as cargas úteis das mensagens. No entanto, o artigo expõe vulnerabilidades nos atributos da camada física e no algoritmo de agendamento descentralizado da camada MAC. Para explorar essas vulnerabilidades, foram desenvolvidos dois modelos de ataque *jamming*.

Esses ataques de baixo ciclo de trabalho degradam significativamente a disponibilidade de sinal no C-V2X. Tal situação aumenta a probabilidade de tempos de viagem prolongados e até mesmo acidentes de veículos. Para combater esses ataques, foram desenvolvidas técnicas de detecção e mitigação. Essas técnicas exploram, em parte, novos recursos do C-V2X no *3rd Generation Partnership Project (3GPP)*¹.

Os ataques e contramedidas foram avaliados experimentalmente em um banco de testes de *hardware*. Esse banco é composto por *Universal Software Radio Peripheral (USRPs)* e módulos C-V2X de última geração. Também foram realizadas extensas simulações de rede e estrada. Os resultados mostram que, em segundos após o início, os ataques podem reduzir a taxa de entrega de pacotes de um alvo em 90% ou a do canal C-V2X para menos de 25%.

Por fim, ainda foram avaliadas técnicas de detecção por aprendizado de máquina e de mitigação de baixo custo. Os resultados mostram que as técnicas de mitigação conseguem neutralizar completamente um ataque e reduzir o impacto do outro em 80%. Tais descobertas fornecem novas perspectivas para o desenvolvimento de sistemas 5G C-V2X mais robustos.

O artigo (Wyglinski *et al.*, 2023) descreve um ataque que utiliza a emissão de sinais de *Radio Frequency (RF)* na camada física. Os dados manipulados pelo ataque são interpretados como uma situação legítima de aplicação. O ataque é realizado através de um processo de localização de emissões de RF, onde um veículo não legítimo exibe leituras falsas dos sensores *Global Navigation Satellite System (GNSS)* e *Inertial Measurement Unit (IMU)* usando BSMs.

O principal objetivo deste ataque é fornecer uma prova de conceito para a detecção de ataques conhecidos como *phantom cars*. Para alcançar a realização deste ataque, é utilizado um complexo *framework* que integra estações móveis, um centro de fusão de dados e um modelo de emissão de RF. O modelo simulado é cuidadosamente desenvolvido e posteriormente testado em um ambiente real, embora em escala reduzida.

Durante o processo de simulação, são definidos parâmetros essenciais, incluindo uma potência de transmissão V2V de 23 dBm e *carrier frequency* C-V2X de 5,9 GHz para comunicação V2V e V2I. As faixas de frequência para C-V2X são 2 a 73,5 Hz para *Urban Microcellular Street Canyon (UMi SC)* e *Urban Macrocellular (UMa)*, e 2 a 60,0 Hz para *Urban Microcellular Open Square (UMi OS)*.

¹ Disponível em: <https://portal.3gpp.org/#/55936-specifications>. Acesso em: <1 de ago. de 2023>.

Na análise dos resultados, a trajetória simulada é comparada com o percurso teórico. Além disso, outros fatores críticos, que são alterados devido ao ataque, são examinados. Estes fatores abrangem mudanças de faixa, variações de velocidade e mudanças na dinâmica do veículo. Os atributos físicos dos sinais, incluindo a intensidade do sinal e os atrasos correspondentes, também são levados em conta ao longo desta análise abrangente.

Para mitigar os riscos impostos por esta classe de ataque, várias contramedidas são discutidas. Entre elas, o uso do *Received Signal Strength Indicator* (RSSI) e *Time Difference of Arrival* (TDOA) se destacam. Ademais, a abordagem híbrida que combina RSSI e TDOA demonstra um desempenho superior na detecção desses ataques complexos.

(Krayani *et al.*, 2023) discute um novo método para detectar interferências com altas probabilidades de detecção. O ponto essencial deste método é o modelo interativo *Coupled Generalized Dynamic Bayesian Network* C-GDBN, que pode detectar interferências conjuntas de GPS sob um cenário V2X. Uma *Road Side Unit* (RSU) equipada com este modelo pode estimar posições de veículos usando sinais de RF dinamicamente.

Para entender essa implementação, é necessário descrever brevemente o ambiente necessário para sua realização. A RSU recebe todos os sinais de RF de todos os carros no mesmo sistema de estrada e rastreia suas posições, geralmente referindo-se aos sinais de GPS, decodificando os sinais de RF.

Uma vez que este ambiente esteja configurado, a RSU aprende um único modelo GDBN para ambos os sinais de RF e GPS. Essa capacidade possibilita que a RSU faça suposições estáticas para prever sinais de RF. Após aprender o modelo base GDBN, a RSU passa para um modelo acoplado C-GDBN, que permite analisar a relação entre os sinais de GPS e RF e rastrear comportamentos anormais no sistema.

Nesta fase, a RSU ainda é incapaz de prever com precisão os sinais de RF. No entanto, ao usar um M-MJPF, a RSU pode fazer previsões temporais e hierárquicas. Este novo método é baseado em um modelo dinâmico interativo, que permite à RSU detectar efetivamente interferências em sistemas V2X.

A tecnologia de *Connected Vehicles* (CV) apresenta oportunidades e desafios para o sistema de *Traffic Signal Control* (TSC) (Feng *et al.*, 2022). Embora a segurança e o desempenho da mobilidade possam ser significativamente melhorados pela adoção de tecnologias de CV, a conectividade entre veículos e infraestrutura de transporte pode aumentar os riscos de ameaças cibernéticas.

Apesar de estudos relacionados à segurança cibernética nos sistemas TSC terem sido conduzidos nos últimos anos, ainda falta uma investigação sistemática que forneça um modelo de análise completo. A pesquisa (Feng *et al.*, 2022) tem por objetivo preencher essa lacuna, propondo um estrutura de análise abrangente para o problema de segurança cibernética do TSC no ambiente CV.

As ameaças potenciais para os principais componentes do sistema e seus impactos correspondentes na segurança e eficiência são analisados, sendo considerada a abordagem de ataque mais plausível e realista. Diferentes estratégias de ataque e soluções de defesa são discutidas, e um estudo de caso é apresentado para mostrar o impacto dos ataques em um sistema TSC selecionado baseado em CV e as contramedidas correspondentes.

Este estudo de caso é conduzido em uma plataforma de teste de segurança híbrida, com tráfego virtual e uma rede de comunicação V2X real. O artigo descreve um modelo de ataque seguindo a estrutura de avaliação de risco, onde se assume que o objetivo do veículo não legítimo é aumentar o atraso total do veículo. Também se assume que o ataque só pode comprometer um veículo de cada vez, aumentando a dificuldade de lançar ataques com consequências proeminentes.

Um cenário de ataque de duas etapas para o sistema de *Intelligent Signal (I-SIG)* é construído. Onde o veículo não legítimo primeiro tenta aprender a lógica de controle através de observações usando um modelo substituto, depois lança ataques de dados falsificados para influenciar os sistemas de controle a tomar decisões subótimas de controle.

O modelo I-SIG é encontrado para ser vulnerável a dois tipos de ataques: ataque de *Estimated Time of Arrival (ETA)* e de *phantom queue*. O ataque ETA aproveita o fato de que o I-SIG usa ETAs na tabela de chegada para avaliar o atraso, enquanto o ataque *phantom queue* utiliza o algoritmo de estimativa de estado de tráfego sob taxas de penetração CV menores.

Neste artigo, o problema de segurança cibernética do sistema TSC em um ambiente CV é sistematicamente investigado. Uma estrutura de análise de segurança cibernética é proposta, incluindo avaliação de risco, soluções de defesa e uma plataforma de teste implementada na infraestrutura de transporte do mundo real.

Por fim, um estudo de caso abrangente é apresentado para mostrar como o arcabouço é aplicado a um sistema TSC selecionado. Os resultados do experimento mostram o impacto dos ataques em aumentar o atraso do sistema e a eficácia dos modelos de defesa na detecção e filtragem de dados falsificados.

As tecnologias de CVs estão sendo implantadas em todo o mundo e em breve remodelarão os sistemas de transporte, trazendo benefícios para a mobilidade, segurança e meio ambiente (Shen *et al.*, 2023). No entanto, essas tecnologias tornam-se inevitavelmente alvos potenciais de ataques cibernéticos.

Trabalhos recentes mostraram que os sistemas de TSC inteligentes baseados em CV são vulneráveis a ataques, que podem causar efeitos severos de congestionamento nos cruzamentos. Em (Shen *et al.*, 2023), uma estratégia geral de detecção para aplicações de CV do lado da infraestrutura é explorada, estimando a confiabilidade dos CVs com base em sensores do lado da infraestrutura prontamente disponíveis.

No cenário, o detector é implementado para controle de sinal de trânsito baseado em CV e avaliado contra dois ataques de congestionamento representativos. A avaliação em um simulador de tráfego de grau industrial mostra que o detector pode detectar ataques com pelo menos 95% de taxas de verdadeiros positivos, mantendo a taxa de falsos positivos abaixo de 7%, sendo robusto a ruídos de sensores.

Uma solução geral de defesa contra ataques em aplicações de CV do lado da infraestrutura também é explorada. Com base no princípio geral de usar informações da camada física para validar cruzadamente as informações da camada cibernética, sensores do lado da infraestrutura prontamente disponíveis, como câmeras de trânsito, são usados para estimar os estados de CV da camada física.

No entanto, esses sensores sofrem de uma limitação fundamental, pois seu alcance de sensor é geralmente muito menor do que o alcance de comunicação do CV. Para resolver isso, modelos de tráfego são usados como invariantes para inferir estados de veículos que estão fora do alcance do sensor.

Neste estudo, o detector é implementado e submetido a uma avaliação rigorosa contra dois tipos específicos de ataques. Esses ataques têm como objetivo provocar congestionamentos em cruzamentos, explorando o sistema de controle de sinal de trânsito baseado em CV. Os resultados da avaliação revelam que o detector é capaz de identificar efetivamente o veículo não legítimo com um alto grau de precisão na detecção.

Além disso, o detector demonstrou robustez em relação aos ruídos dos sensores. Mesmo quando operando de forma contínua, a presença de ruído apenas degrada ligeiramente o desempenho da detecção, destacando a eficácia do detector em ambientes complexos.

Com base nas informações de (Yang *et al.*, 2023), uma nova abordagem é sugerida para identificar comportamentos irregulares em veículos. Este método se baseia em um modelo que utiliza GPS e IMU para fornecer informações precisas de posicionamento.

No entanto, essas tecnologias também podem ser mal utilizadas para causar acidentes. Para resolver este problema, a equipe propôs um modelo de ataque baseado em algoritmos de *Multi-Sensor Fusion* (MSF) para detectar vulnerabilidades nos sistemas V2X existentes.

As ferramentas de defesa tradicionais dependem da detecção de anomalias, que podem ser divididas em detecção centrada no nó e detecção centrada nos dados. No entanto, a nova estrutura de detecção da equipe é baseada em aprendizado demonstrativo que é projetada para detectar comportamentos irregulares em V2X.

A pesquisa propõe dois modelos de ataque: um voltado para veículos autônomos e outro para veículos conectados. No primeiro, o algoritmo *FusionRipper* é usado para interferir no GPS, podendo levar o veículo a situações de risco. No segundo, o sistema de integração aviônica modular é aplicado, com a manipulação do GPS para gerar BSMs falsos, resultando em alterações indesejadas na trajetória.

Para combater esses ataques, sugere-se treinar o sistema sem conexão à internet usando dados históricos de trajetória e empregar aprendizado demonstrativo para aprimorar as capacidades de geração de trajetória do sistema. Com um classificador de anomalias, torna-se possível diferenciar entre trajetórias típicas e inconsistentes.

2.3 Estado da arte de parâmetros V2X

Com base na revisão bibliográfica, foi montada uma tabela com os principais parâmetros para a modelagem de cenários V2X em 5G NR. Essa tabela serve como um guia para a configuração inicial das simulações, proporcionando uma aproximação mais precisa de cenários reais. Destaca-se que alguns parâmetros são específicos para determinados métodos de ataque, evidenciando a complexidade e a especificidade do contexto V2X. Os parâmetros efetivamente utilizados na simulação deste trabalho estão especificados ao longo do Capítulo 3.

Tabela 2.1 – Parâmetros típicos em simulações de aplicações V2X presentes na literatura.

Parâmetros	Valores
<i>Carrier frequency</i> ²	5,9 GHz
<i>Bandwidth</i> ³	10 MHz
Potência de transmissão V2V ⁴	16 a 23 dBm
Potência de transmissão V2I ⁵	20 a 30 dBm
Modelo de <i>multipath fading</i> ⁶	<i>Jakes e Rayleigh</i>
Modelo de <i>pathloss</i> ⁷	<i>Free Space, Two Ray Ground, Rayleigh, Nakagami, Rice, Log Normal Shadowing</i>
Limiar de SINR ⁸	0, 3 e 6 dBm

Fonte: Produzido pelo autor.

² Extraído das obras: (Yao *et al.*, 2023), (Pelechrinis *et al.*, 2011), (Wyglinski *et al.*, 2023).

³ Extraído das obras: (Yao *et al.*, 2023), (Pelechrinis *et al.*, 2011), (Twardokus; Rahbari, 2023).

⁴ Extraído das obras: (Yao *et al.*, 2023), (Pelechrinis *et al.*, 2011), (Krayani *et al.*, 2022), (Twardokus; Rahbari, 2023), (Yang *et al.*, 2022a), (Krayani *et al.*, 2023).

⁵ Extraído das obras: (Krayani *et al.*, 2022), (Yang *et al.*, 2022a), (Krayani *et al.*, 2023).

⁶ Disponível em: <https://github.com/Unipisa/Simu5G>. Acesso em: <8 de ago. de 2023>. Extraído da obra: (Nardini *et al.*, 2020).

⁷ Disponível em: <https://github.com/Unipisa/Simu5G>. Acesso em: <8 de ago. de 2023>. Extraído da obra: (Nardini *et al.*, 2020).

⁸ Extraído das obras: (Yao *et al.*, 2023), (Pelechrinis *et al.*, 2011).

2.4 Ferramentas de simulação

Este projeto foi desenvolvido com o auxílio das seguintes ferramentas de simulação: OMNeT++, INET *framework*, Simu5G, Veins e SUMO. A [Figura 2.1](#) mostra como essas ferramentas são encapsuladas e cooperam para criar simulações de redes de veículos. Cada um desses componentes desempenhou um papel essencial no projeto, e a seguir, serão fornecidas definições para compreender melhor suas contribuições.

OMNeT++⁹ é um simulador de eventos discretos, modular e orientado a objetos, amplamente utilizado para construir simuladores de rede. Ele permite criar modelos de simulação de redes de forma flexível e escalável, possibilitando a análise de diversos cenários e protocolos de comunicação.

INET *framework*¹⁰ é uma biblioteca no OMNeT++ que contém modelos dos principais protocolos de camada de rede e camada de enlace para redes com fio e sem fio. Além disso, também fornece suporte para mobilidade, protocolos MANET, DiffServ, MPLS com sinalização LDP e RSVP-TE e diversos modelos de aplicação.

Simu5G¹¹ é um simulador de rede 5G NR que se baseia na biblioteca SimuLTE e foi criada pelo mesmo grupo de pesquisa. Ele é construído sobre o *framework* de simulação OMNeT++ e oferece uma variedade de modelos com interfaces bem definidas.

Tais modelos podem ser instanciados e conectados para criar cenários de simulação de complexidade variável. Ademais, o Simu5G incorpora modelos da biblioteca INET, permitindo a simulação de redes TCP/IP genéricas.

O Simu5G permite a modelagem de comunicações em modos *Frequency Division Duplex* (FDD) e *Time Division Duplex* (TDD), com uma variedade de gNodeBs heterogêneos. Tal *software* também suporta comunicação via interface X2 para facilitar a transição e coordenação de interferência entre células.

Além disso, o Simu5G suporta vários modelos de mobilidade para *User Equipment* (UE). Ele permite a implementação de diferentes estratégias de alocação e gerenciamento de recursos, incluindo a seleção de quais UEs devem ser alvo de determinadas ações, a escolha do esquema de modulação, a coordenação para minimizar a interferência entre células e a seleção da faixa de frequência.

Veins¹² é um *framework* de simulação de rede de veículos de código aberto que vem com uma coleção de modelos de simulação de comunicação entre veículos. Esses modelos são projetados para interagir com um simulador de trânsito, como o SUMO, para fornecer uma simulação bidirecionalmente acoplada de tráfego rodoviário e rede.

⁹ Disponível em: <https://omnetpp.org>. Acesso em: <15 ago. de 2023>.

¹⁰ Disponível em: <https://inet.omnetpp.org>. Acesso em: <15 ago. de 2023>.

¹¹ Extraído da obra: (Nardini *et al.*, 2020).

¹² Extraído da obra: (Sommer; German; Dressler, 2011).

SUMO¹³ é um simulador de trânsito rodoviário de código aberto, detalhado e multimodal, que permite simular o movimento de veículos individuais em uma rede viária específica. As simulações são determinísticas por padrão, porém é possível introduzir aleatoriedade aos agentes da simulação.

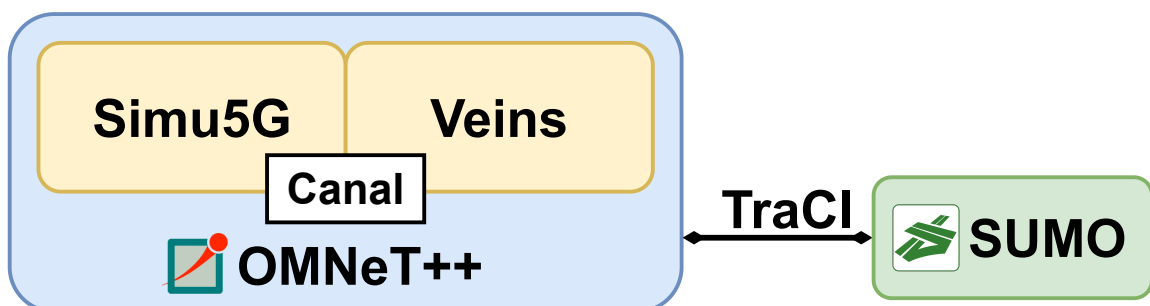
Depois de definir os simuladores utilizados, é crucial entender como esses módulos se integram, como mostrado na [Figura 2.1](#). O OMNeT++ atua como o controlador principal da simulação e também como o coletor de dados. Dentro do ambiente OMNeT++, o Simu5G é responsável por estabelecer a conectividade entre os nós da rede de veículos autônomos, simulando várias camadas e configurações em redes 5G.

Para permitir uma simulação da rede de veículos autônomos, o Veins e o Simu5G são conectados por meio de um canal de comunicação dentro do ambiente OMNeT++. A conexão permite que os dois simuladores troquem informações e colaborem para simular o comportamento da rede de veículos autônomos.

Com a conexão estabelecida entre o Veins e o Simu5G, o módulo *Mobility* do Veins desempenha um papel essencial. Ele facilita a integração entre o Simu5G e o SUMO, atualizando as informações de mobilidade do nó, como posição, velocidade e direção, com base no comportamento do veículo. A interconexão entre o OMNeT++ e o SUMO é estabelecida através de um soquete TCP, permitindo a comunicação por meio do protocolo *Traffic Control Interface* (TraCI).

Finalmente, vale ressaltar que a simulação de uma rede de veículos autônomos não se limita apenas à comunicação entre os nós. A mobilidade dos veículos, influenciada por vários fatores, como tráfego e condições da estrada, também é essencial. Esses aspectos são simulados pelo SUMO, que fornece um ambiente de simulação que permite que os veículos se movam de acordo com as condições de trânsito implementadas.

Figura 2.1 – Arquitetura modular das ferramentas de simulação



Fonte: Adaptado de (Pusapati *et al.*, 2022).

¹³ Extraído da obra: (Lopez *et al.*, 2018).

2.5 Modelagem do ataque *jamming*

Definição 2.1. Um ataque de *jamming* em V2X é um sinal físico emitido na mesma frequência do alvo com o objetivo de gerar interferência eletromagnética. Essa interferência pode degradar a qualidade das comunicações e resultar em perda de informações críticas, tornando o *jamming* uma ameaça às redes de comunicação.

Com base na [Definição 2.1](#), que estabelece uma relação entre a interferência na camada física e a qualidade do sinal recebido, e considerando a estrutura da camada física no simulador Simu5G que será detalhada no [Capítulo 3](#), torna-se importante definir a relação *Signal-to-Interference-plus-Noise Ratio* (SINR) para a modelagem do ataque *jamming*.

Definição 2.2. A razão SINR é uma métrica que quantifica a qualidade de um sinal em um canal de comunicação sem fio. É definida como a razão entre a potência do sinal de interesse e a soma da potência da interferência e do ruído. Matematicamente, é expressa em sua forma linear como:

$$SINR = \frac{P_s}{P_n + P_i} \quad (2.1)$$

Sejam P_s , P_n e P_i os parâmetros que representam, respectivamente, a potência do sinal de interesse, a potência do ruído no canal e a potência da interferência de sinais externos no mesmo canal.

Nos parâmetros da [Equação 2.1](#), P_s é calculado levando em consideração as potências, ganhos, perdas de caminho e atenuações definidas para os receptores, transmissores, *jammers* e na camada de acesso ao meio físico. Por outro lado, P_n representa a potência do ruído gerado pelo *hardware*.

Na modelagem de P_n , é comum considerar a contribuição de três tipos de ruído: *thermal noise*, *shot noise* e *flicker noise*. No entanto, no Simu5G apenas o *thermal noise* é implementado por padrão. Este tipo de ruído é comum em *hardware* e resulta da agitação térmica dos condutores.

É amplamente aceito na literatura que o ruído térmico possa representar adequadamente o comportamento geral do ruído, sendo definido pela [Equação 2.2](#). Além disso, foi definido um *figureNoise* de 7 dBm, que corresponde a um ganho aplicado em P_n .

Em telecomunicações, a modelagem do ruído térmico através da [Equação 2.3](#), que leva em consideração a largura de banda, é a abordagem mais conveniente e foi a adotada na simulação. A [Observação 2.1](#) descreve como a largura de banda é calculada no Simu5G. Além disso, P_i foi definido por métodos do Simu5G para computar interferência externa entre células D2D.

Definição 2.3. Potência do ruído térmico de Johnson–Nyquist.

$$P_T = k_B T \Delta f \quad (2.2)$$

Sejam k , T e Δf os parâmetros que representam, respectivamente, a constante de Boltzmann, a temperatura e a largura de banda.

Observação 2.1. Conforme o espectro, a largura de banda pode ser obtida por meio do parâmetro *numBands* do Simu5G:

$$\Delta f = \frac{\text{numBands}}{5}$$

Definição 2.4. Potência do ruído térmico.

$$P_T = -174 + 10 \cdot \log(\Delta f) \quad (2.3)$$

A interferência gerada pelo *jammer* foi obtida modificando a [Equação 2.1](#) para incluir a potência de saída do *jamming* P_j por banda de canal, que é similar em natureza ao P_i . Essa modificação resultou na [Equação 2.4](#).

$$SINR = \frac{P_s}{P_n + P_i + P_j} \quad (2.4)$$

Para diversificar os cenários, foram usados dois *jammers*, sendo um *jammer* portátil com 1W por canal e um *jammer* de alta potência com 30W por canal, que apresenta maior alcance. Esses modelos são padronizados para interferir em dispositivos de comunicação sem fio, incluindo 5G, e são adotados em indústrias de países onde o seu uso é regulamentado.

Além disso, o formato linear da razão SINR nas [Equações 2.1](#) e [2.4](#) é comumente expresso em telecomunicações na escala logarítmica, conforme a [Equação 2.5](#). Por padrão, no Simu5G, as potências são expressas em miliWatt (mW) e utilizou-se a referência de SINR em sua forma logarítmica em relação ao nível de 1mW na [Equação 2.6](#), que corresponde ao decibéis-miliWatt (dBm). A conversão inversa é obtida pela [Equação 2.7](#).

$$SINR_{dB} = 10 \cdot \log(SINR) \quad (2.5)$$

$$SINR_{dBm} = 10 \cdot \log(1000 \cdot SINR) \quad (2.6)$$

$$SINR = 10^{(SINR_{dBm} - 30)/10} \quad (2.7)$$

Por fim, para a análise de resultados, levou-se em consideração o cálculo das mensagens transmitidas e recebidas na camada de aplicação. Tal cálculo foi realizado por meio da *Packet Loss Ratio* (PLR), conforme indicado na [Observação 2.2](#).

Observação 2.2. PLR é uma métrica importante para validar o ataque *jamming*, que será analisada na [Capítulo 4](#). Matematicamente, é expressa como:

$$PLR = \frac{N^{tx} - N^{rx}}{N^{tx}} \cdot 100\%$$

Sejam N^{tx} e N^{rx} os parâmetros que representam, respectivamente, o número total de pacotes transmitidos e o número total de pacotes recebidos.

3 Metodologia

Neste capítulo, são abordadas simulações em redes de veículos autônomos com a consideração de ataques *jamming*. Os cenários *Do Not Pass Warning* (DNPW) e *Intersection Movement Assist* (IMA) são examinados, seguindo as especificações do 3GPP¹. As implementações desses cenários no Simu5G e suas adaptações para situações de ataque são detalhadas.

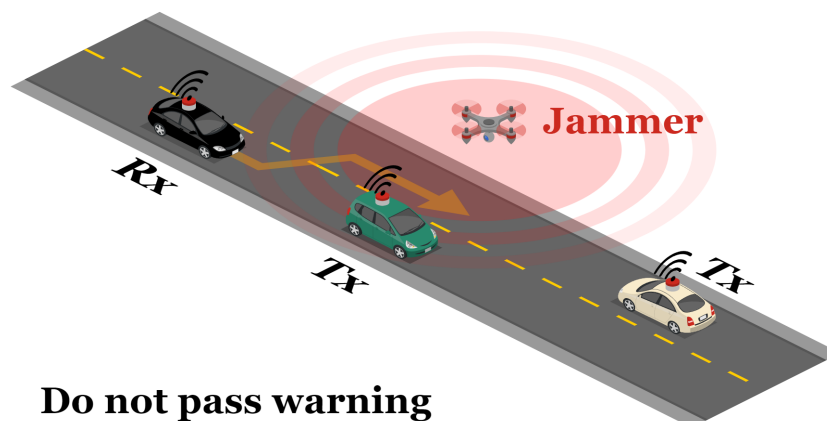
3.1 Ataque *jamming* no cenário DNPW

O caso de uso DNPW é um componente crucial em rede de veículos autônomos. Este processo atua como um sistema de alerta que notifica o veículo sobre a aproximação de outro veículo na direção contrária. Tal recurso é de extrema importância, pois pode prevenir situações de ultrapassagem perigosas.

O DNPW é uma ferramenta versátil para veículos autônomos, útil em estradas retilíneas e curvas. O veículo pode prever a aproximação de veículos na direção oposta, permitindo medidas preventivas. Sua eficácia é ainda mais essencial em estradas curvas, onde pode detectar veículos não imediatamente visíveis em pontos cegos devido à curvatura.

A [Figura 3.1](#) ilustra uma situação comum onde o DNPW é fundamental. Neste cenário específico, o veículo receptor (Rx) está com a intenção de ultrapassar o veículo transmissor (Tx) à sua frente. Contudo, um drone *jammer* está causando interferência na comunicação entre eles, agravando o risco de acidente.

Figura 3.1 – Esquemático do caso de uso DNPW.



Fonte: Produzido em colaboração com (Silva *et al.*, 2023).

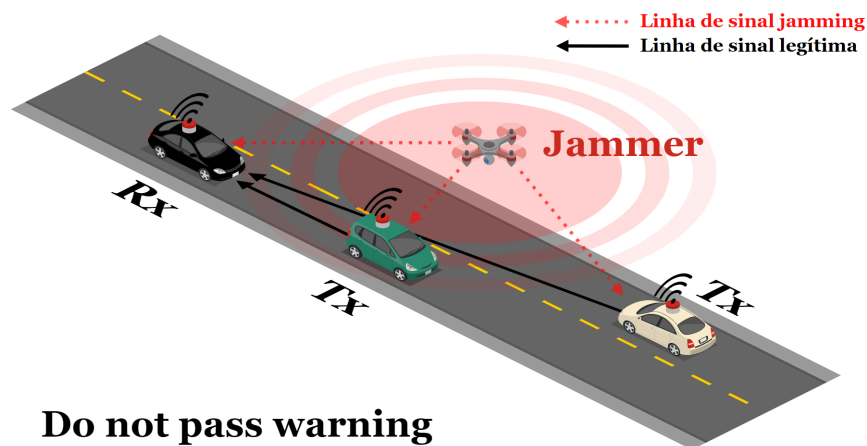
Nota: ©Icograms Designer

¹ Disponível em: <https://portal.3gpp.org/#/55936-specifications>. Acesso em: <12 de ago. de 2023>.

A comunicação V2X é fundamental para o funcionamento correto do DNPW. O comprometimento dessa comunicação pode levar a situações perigosas, visto que o veículo Rx não receberá o alerta do DNPW, tornando a ultrapassagem inevitável. Esta situação já é arriscada e pode se tornar ainda mais grave em condições climáticas adversas, como chuva, neblina ou neve, onde a visibilidade é reduzida.

Na [Figura 3.2](#), percebe-se que o veículo Rx é afetado pela interferência do drone *jammer*. A presença do drone impede que o veículo Rx receba os dados transmitidos pelos veículos Tx de maneira correta. Tal cenário pode resultar em falta de informações essenciais para a tomada de decisões seguras na condução autônoma, aumentando assim o risco de acidentes na estrada.

Figura 3.2 – Cenário DNPW com ênfase no ataque *jamming*



Fonte: Produzido em colaboração com (Silva *et al.*, 2023).

Nota: ©Icograms Designer

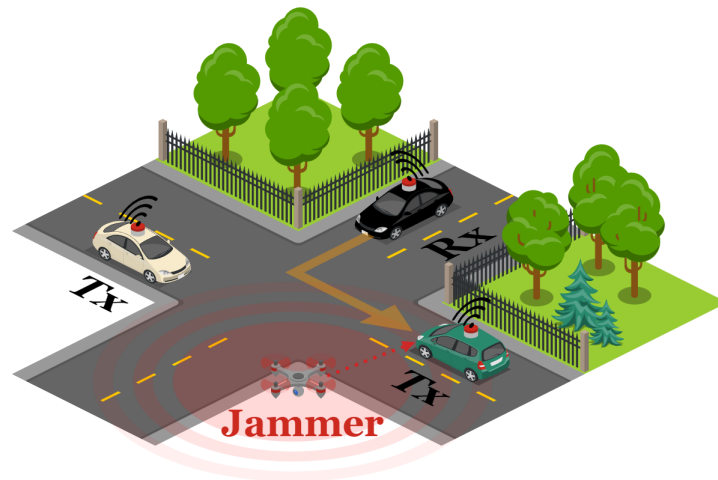
3.2 Ataque *jamming* no cenário IMA

IMA é cenário onde veículos autônomos auxiliam a realizar cruzamentos ou desvios nas direções desejadas, especialmente em locais onde não há semáforos para controlar o tráfego. Normalmente, o veículo recebe mensagens BSM do veículo transmissor e a unidade interna do veículo processa essas mensagens para prever a trajetória futura.

Se a análise desses dados sugerir a probabilidade de uma colisão, um alerta pode ser acionado para o motorista. A emissão de tal alerta desempenha um papel vital na prevenção de acidentes. Além disso, contribui para a manutenção da segurança na condução, permitindo que o motorista tome medidas preventivas com base no alerta recebido.

Na [Figura 2.1](#), apresenta-se um exemplo do cenário IMA. O veículo Rx pretende fazer uma curva à esquerda, enquanto os veículos Tx enviam alertas através de mensagens BSM. No entanto, a comunicação é comprometida devido à interferência de um drone *jammer*.

Figura 3.3 – Esquemático do caso de uso IMA.



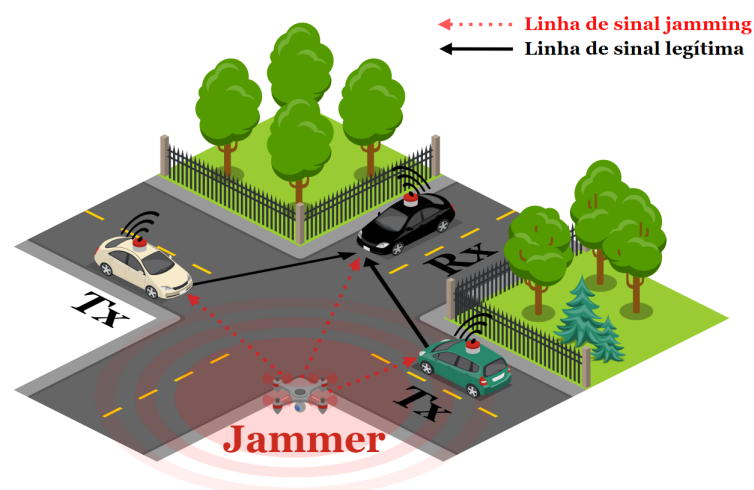
Intersection movement assist Left turn assist

Fonte: Produzido em colaboração com (Silva *et al.*, 2023).

Nota: ©Icograms Designer

Com visibilidade reduzida, a interrupção da comunicação pode causar colisões entre o Rx e os veículos Tx. Na Figura 3.4, a interferência do *jammer* afeta negativamente o Rx, dificultando a recepção aos dados dos veículos Tx. Tal situação aumenta a probabilidade de acidentes na estrada devido à falta de informações para decisões seguras ao dirigir.

Figura 3.4 – Cenário IMA com ênfase no ataque *jamming*



Intersection movement assist Left turn assist

Fonte: Produzido em colaboração com (Silva *et al.*, 2023).

Nota: ©Icograms Designer

3.3 Implementação dos cenários V2X no Simu5G

A revisão bibliográfica concisa, apresentada na [Tabela 2.1](#), destaca valores típicos encontrados em aplicações V2X. Com base nesses dados, a [Tabela 3.1](#) foi estabelecida. Esta tabela contém os parâmetros de configuração utilizados para a simulação dos cenários DNPW e IMA, proporcionando uma visão detalhada das condições de teste.

Os valores de *carrier frequency* e *bandwidth* estão de acordo com o 3GPP. Já em relação à potência de transmissão entre veículos, foi adotado o valor superior no intervalo da [Tabela 2.1](#), que é de 23 dBm. Tal escolha se deve ao fato de que foram consideradas perdas de potência no caminho, denominada *pathloss*, incluindo modelos de *fading* e *shadowing*.

Tabela 3.1 – Parâmetros típicos V2X configurados na simulação

Parâmetros	Valores
<i>Carrier frequency</i>	5,9 GHz
<i>Bandwidth</i>	10 MHz
Potência de transmissão V2V	23 dBm
Modelo de <i>multipath fading</i>	<i>Rayleigh</i>
Modelo de <i>pathloss</i>	<i>Log Normal Shadowing</i>

Fonte: Produzido pelo autor.

Com relação à simulação, o planejamento das rotas dos veículos e seus movimentos foram realizadas no SUMO^{2,3}, por meio da linguagem de marcação XML. A inicialização dos parâmetros V2X, da [Tabela 3.1](#), e as configurações das simulações foram realizadas nos arquivos *omnetpp.ini*^{4,5} e *Highway.ned*^{6,7} dentro do ambiente do Simu5G no OMNeT++.

A camada de aplicação do Simu5G comporta várias opções, tais como: *alert*, *burst*, *Constant Bit Rate* (CBR), *Video on demand* (VoD) e *Voice over IP* (VoIP). Entre os dispositivos Rx e Tx, foi adotado o tipo *alert*, que envia mensagens de alerta periódicas ao receptor, sendo escolhida por melhor se aproximar das aplicações definidas nos cenários DNPW e IMA.

² Rotas do cenário DNPW:

<https://github.com/devis6x7/V2X/blob/main/simu5G/simulations/NR/DNPW/heterogeneous.rou.xml>

³ Rotas do cenário IMA:

<https://github.com/devis6x7/V2X/blob/main/simu5G/simulations/NR/IMA/heterogeneous.rou.xml>

⁴ Inicialização de parâmetros e configurações do cenário DNPW:

<https://github.com/devis6x7/V2X/blob/main/simu5G/simulations/NR/DNPW/omnetpp.ini>

⁵ Inicialização de parâmetros e configurações do cenário IMA:

<https://github.com/devis6x7/V2X/blob/main/simu5G/simulations/NR/IMA/omnetpp.ini>

⁶ Configurações dos módulos no cenário DNPW:

<https://github.com/devis6x7/V2X/blob/main/simu5G/simulations/NR/DNPW/Highway.ned>

⁷ Configurações dos módulos no cenário IMA:

<https://github.com/devis6x7/V2X/blob/main/simu5G/simulations/NR/IMA/Highway.ned>

O Simu5G suporta a implementação de técnicas de transmissão de dados, incluindo *unicast*, *broadcast* e *multicast*. Neste trabalho, optou-se pela configuração de *multicast* entre veículos Rx e Tx, associando ao grupo um endereço IPV4. Nesses cenários, os dois veículos Tx foram configurados como *AlertSender* e o veículo Rx como *AlertReceiver*.

Para a modelagem dos agentes Rx, Tx e *jammer*, é imprescindível defini-los como dispositivos de comunicação de dados, permitindo assim a sua conexão em rede. O Simu5G estabelece classes associadas a esses dispositivos de comunicação, as quais incorporam protocolos específicos e são denominadas nós⁸.

Os nós que podem ser implementados no Simu5G incluem *Ue*, *Car*, *gNodeB*, *MEC* e *Upf*. Dentro desse escopo, os nós Rx e Tx, sendo usuários finais, são modelados por meio de herança de classe a partir do nó *Car*. Vale ressaltar que o nó *Car* é, por sua vez, uma extensão do nó *Ue* com mobilidade.

A herança de classe do nó *Car* permite que os nós Rx e Tx se movam dentro do ambiente de simulação, sendo fundamental para aproximar a simulação de um cenário real. Além disso, o nó *Car* também suporta a implementação de protocolos de comunicação específicos para veículos, o que contribui para uma simulação mais precisa e alinhada com as condições dos cenários DNPW e IMA.

3.4 Implementação do ataque *jamming* no Simu5G

A revisão bibliográfica objetiva, apresentada na [Tabela 2.1](#), destaca valores típicos encontrados em ataques V2X. Com base nesses dados, a [Tabela 3.2](#) foi estabelecida para fornecer uma estrutura da simulação. Esta tabela contém os parâmetros de configuração utilizados nos cenários DNPW, IMA e adaptados com ataque, proporcionando uma visão detalhada das condições de teste.

A potência de transmissão do *jammer* foi definida no limite superior da potência de transmissão V2I. Tal configuração se deve à natureza do nó *jammer* e às perdas de potência no caminho configuradas. Além disso, o limiar de SINR foi estabelecido em 0 dBm, já que valores inferiores resultariam em qualidade baixa e seriam considerados como desconexão das comunicações. Embora os valores de 3 e 6 dBm estejam presentes na [Tabela 2.1](#), eles servem apenas para fins comparativos e não foram aplicados neste trabalho.

Conforme o período de BSM estabelecido, o *jammer* realizará um *broadcast* a cada 100ms, introduzindo assim interferências na rede. Nos cenários DNPW e IMA, foram adotados modelos de ataque *jamming* periódico. Este tipo de ataque, que pode impactar significativamente a comunicação na rede, é detalhado no [Capítulo 4](#) e [Apêndice A](#).

⁸ Nós no Simu5G:
<https://github.com/Unipisa/Simu5G/tree/master/src/nodes>. Acesso em: <13 de out. de 2023>.

Tabela 3.2 – Parâmetros de ataque *jamming* configurados na simulação

Parâmetros	Valores
Potência de transmissão <i>jammer</i>	30 dBm
Limiar de SINR	0 dBm
Período de ataque <i>jamming</i>	100 ms
Potências do <i>jammer</i> por canal	1W e 30W

Fonte: Produzido pelo autor.

Na biblioteca padrão do Simu5G, o nó *jammer* não está predefinido. Assim, foi criado um nó personalizado que herda de *gNodeB*. Nesse contexto, o *jammer* atua como um drone equipado com uma antena que estabelece uma *Radio Access Network* (RAN). Ao mesmo tempo, pode introduzir interferências eletromagnéticas externas aos veículos e que afetam a comunicação da rede.

O *jammer* não foi estabelecido como nó *Car*, levando em consideração que os ataques são omnidirecionais. Em cenários envolvendo o nó *Car*, o *broadcast* pode ser efetuado por meio de *handover*, no entanto, necessita de um endereço IPV4, que está vinculado à camada de transporte conforme o modelo *Open Systems Interconnection* (OSI). Contudo, o *jamming* é uma perturbação do sinal originada da camada física.

O parâmetro de configuração *jamming*, inicializado no arquivo *omnet.ini*, foi estabelecido na camada física para validação do ataque. Este parâmetro *boolean* e a potência de saída do *jammer* determinam a presença de interferência. Se o *jamming* for verdadeiro, então haverá interferência, caso contrário, o cenário será um caso de uso típico em V2X.

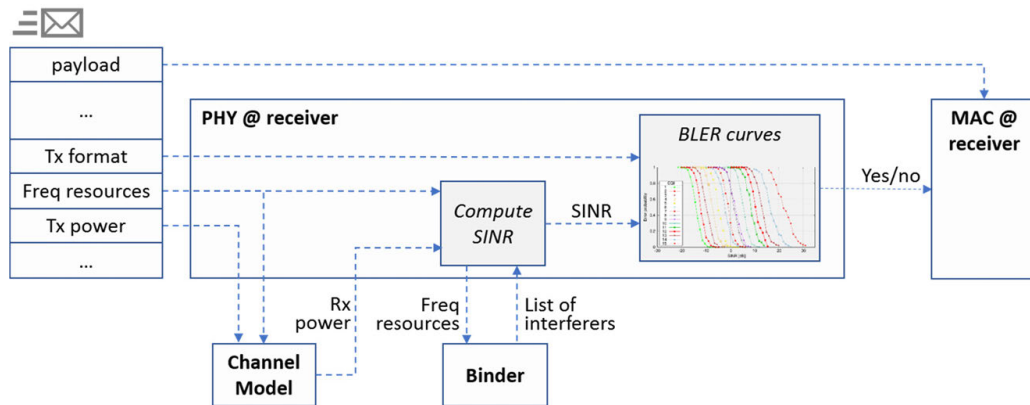
Após definir do nó *jammer*, o próximo passo foi estabelecer o local de configuração da interferência *jamming*. Segundo (Nardini *et al.*, 2020), as potências dos transmissores são recebidas no *Channel Model* através do *payload*. Esse canal interage com a camada física para computar as perdas de potência e gerar interferência, como ilustrado na Figura 3.5.

O artigo destacada que a interação entre o *Channel Model*⁹ e a camada física é uma parte essencial do processo de comunicação entre veículos, sendo realizada através dos métodos *getSinr()* e *error()*. Tais métodos, são implementados dentro do *Channel Model* no módulo *Realistic Channel Model*¹⁰.

⁹ *Channel Model* no Simu5G:
<https://github.com/Unipisa/Simu5G/tree/master/src/stack/phy/ChannelModel>.
 Acesso em: <21 de out. de 2023>.

¹⁰ Módulo *Realistic Channel Model* do *Channel Model* no Simu5G:
<https://github.com/Unipisa/Simu5G/blob/master/src/stack/phy/ChannelModel/LteRealisticChannelModel.cc>. Acesso em: <21 de out. de 2023>.

Figura 3.5 – Diagrama de blocos da camada física no Simu5G



Fonte: (Nardini *et al.*, 2020).

O método *getSinr()* desempenha um papel essencial na implementação do *jamming*, sendo através dele que as interferências externas em relação aos nós da rede são computadas e permite a manipulação das características do sinal. Já o método *error()* é usado para verificar se o sinal foi decodificado corretamente.

O módulo *Realistic Channel Model* apresenta polimorfismos para o método *getSinr()*, onde são computadas a interferência entre os nós *gNodeB* e *Ue*. Entretanto não afeta diretamente a aplicação *alert*, assim investigou-se outro método de polimorfismo denominado *getSinr()_d2d*.

No método *getSinr()_d2d*¹¹, utilizado para *multicast* entre células *Device-to-Device* (D2D), é possível calcular a interferência externa que afeta a aplicação *alert*. Portanto, o método *getSinr()_d2d*¹² foi modificado para computar a interferência externa originada do *jammer*. Tais implementações alteram a qualidade do sinal SINR e geram perda de dados e pacotes no receptor.

O **Algoritmo 3.1** descreve a razão SINR modificada em dois cenários distintos: comunicações legítimas e situações de *jamming*. A inicialização do sistema envolve a definição de várias variáveis, incluindo um indicador de *jamming*, os tempos de início e fim do *jamming*, o número de bandas e as potências de ruído, *jamming* e interferência.

No cenário de ataque, quando o indicador de *jamming* está habilitado e o momento atual se encontra dentro do intervalo de *jamming*, o ruído total (*totN*) é calculado. Este cálculo compreende a soma das potências de ruído e *jamming*, a qual é convertida para uma escala linear conforme a **Equação 2.7**.

¹¹ Método *getSinr()_d2d* para D2D *multicast*:
<https://github.com/Unipisa/Simu5G/blob/master/src/stack/phy/ChannelModel/LteRealisticChannelModel.cc#L1559>. Acesso em: <6 de nov. de 2023>.

¹² Método modificado de *getSinr()_d2d* para D2D *multicast*:
<https://github.com/devis6x7/V2X/blob/main/simu5G/src/stack/phy/ChannelModel/LteRealisticChannelModel.cc#L1572>

É importante observar que o *jamming*, apesar de ser uma forma de interferência externa, é computado juntamente com o ruído total. Esse método de cálculo é adotado porque tanto o ruído total quanto a interferência do *jamming* são definidos na mesma unidade de potência.

Posteriormente, para cada banda, o denominador (*den*) é calculado como a soma das potências de interferência e do ruído total, convertida para dBm de acordo com a [Equação 2.6](#). A atualização da qualidade SINR para cada banda é realizada subtraindo o denominador do valor atual, resultando em um vetor de SINR (*sinrVector*).

Cada elemento do *sinrVector* representa a qualidade do sinal em uma parte específica do espectro de frequências, fornecendo assim uma medida abrangente da qualidade da comunicação em todas as bandas. Por fim, caso *jamming* não esteja habilitado, então a interferência do *jamming* não é considerada na razão SINR.

Algoritmo 3.1 Pseudocódigo para avaliação de SINR em comunicações legítimas e *jamming*

```

1: Inicialização do sistema: ‘jamming’, ‘startJamming’, ‘endJamming’, ‘numBands’,
   ‘Pn’, ‘Pj’, ‘Pi’
2: if ‘jamming’ e ‘now >= startJamming’ e ‘now <= endJamming’ then
3:   Calcular ‘totN = dBmToLinear(Pn + Pj)’
4:   for cada banda ‘i’ em ‘numBands’ do
5:     Calcular ‘den = linearToDBm(Pi + totN)’
6:     Atualizar ‘sinrVector[i] = den’
7:   end for
8: else
9:   Calcular ‘totN = dBmToLinear(Pn)’
10:  for cada banda ‘i’ em ‘numBands’ do
11:    Calcular ‘den = linearToDBm(Pi + totN)’
12:    Atualizar ‘sinrVector[i] = den’
13:  end for
14: end if

```

4 Resultados

Neste capítulo, apresentam-se os resultados das simulações e análises dos cenários DNPW e IMA. Tais cenários são inicialmente simulados no Simu5G como casos de uso em V2X e, posteriormente, adaptados para ataques *jamming*. Analisam-se a qualidade de sinal e a taxa de perda de pacotes entre os veículos receptor e transmissor, levando em consideração a distância e a interferência entre as células D2D.

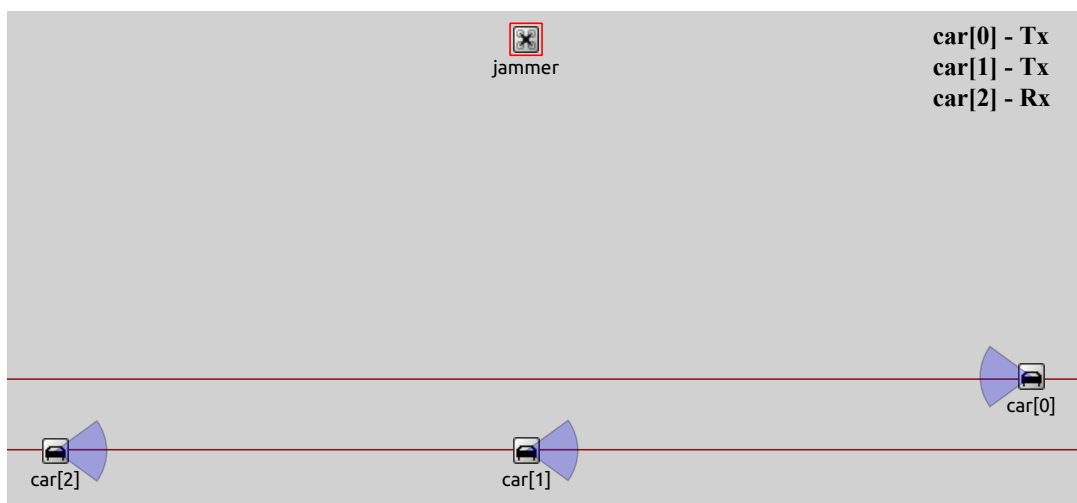
4.1 Simulação do cenário DNPW

Na realização do cenário DNPW, implementado no simulador Simu5G e ilustrado na [Figura 4.1](#), as possíveis trajetórias são destacadas por linhas vermelhas. A [Figura A.1](#) exibe o cenário no SUMO e a [Figura A.2](#) representa o instante final da simulação no Simu5G.

Os elementos do cenário incluem o primeiro carro transmissor (car[1]) e o segundo carro transmissor (car[0]), que se move na direção oposta ao car[1]. Além disso, o cenário conta com o carro receptor (car[2]), que segue no mesmo sentido de car[1]. O veículo car[2] está em uma situação crítica, visto que a possibilidade iminente de mudança de faixa pode levar a um acidente.

Outro componente importante é o *jammer*, estrategicamente localizado a uma distância na ordem de dezenas de metros dos três veículos. Sua principal função é causar interferência eletromagnética, podendo afetar negativamente o recebimento dos pacotes no car[2] e causar falhas na comunicação entre os veículos, que aumentam significativamente o risco de acidentes.

Figura 4.1 – Realização do ataque no cenário DNPW



Fonte: Produzido pelo autor.

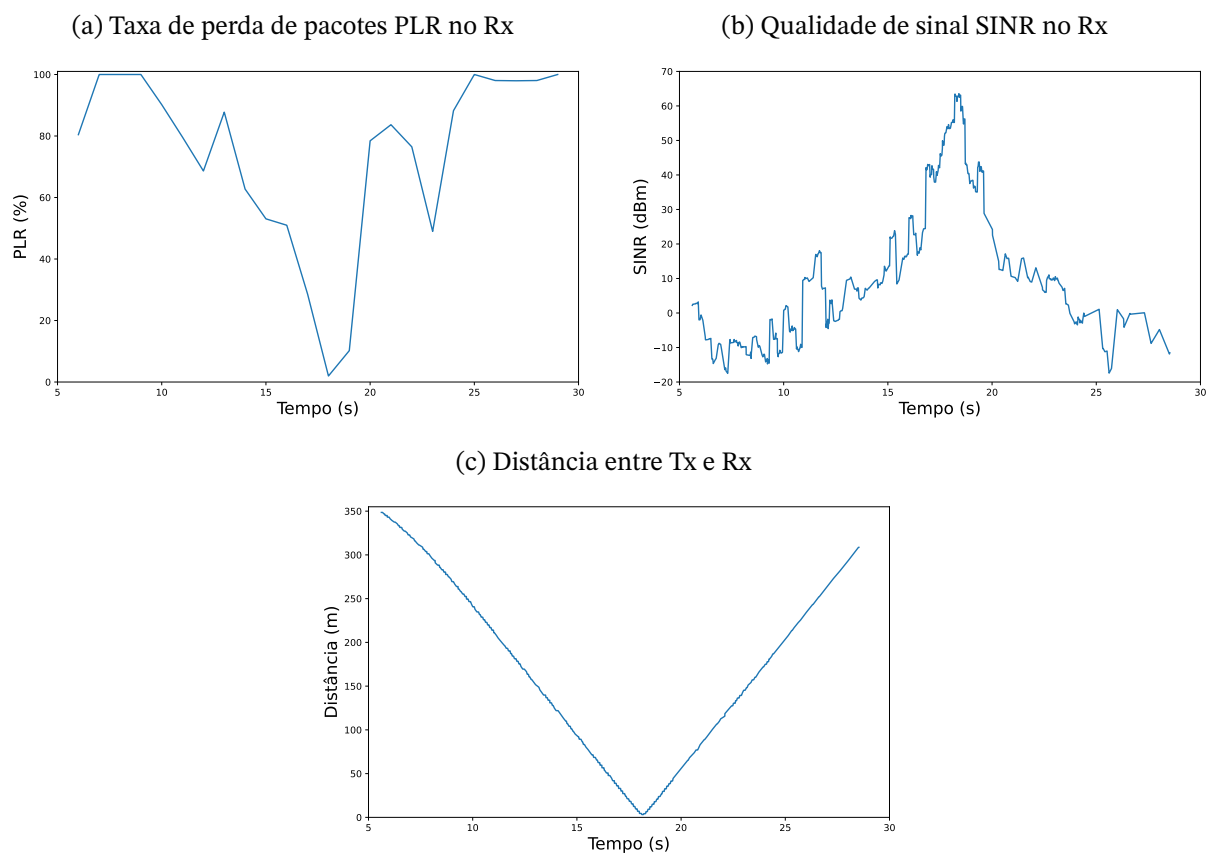
4.2 Parâmetros analisados no cenário DNPW

Os parâmetros no cenário DNPW sem ataque, medidos entre os nós car[0] e car[2], são ilustrados nas figuras a seguir. A [Figura 4.2a](#) apresenta a taxa de perda de pacotes ao longo do tempo, conforme definido na [Observação 2.2](#). A [Figura 4.2b](#) exibe a razão SINR, que representa a qualidade do sinal recebido no canal em relação a ruídos e interferências, como especificado na [Equação 2.1](#).

Além disso, a [Figura 4.2c](#) representa a distância entre os nós ao longo do tempo, fornecendo mais contexto para a análise. No início da simulação, a distância significativa na ordem de centenas de metros entre o car[0] e car[2] leva a uma alta taxa de perda de pacotes, evidenciada pela baixa qualidade com valores de SINR inferiores do limiar de 0 dBm.

Conforme os veículos gradualmente se aproximam, a qualidade melhora e a taxa de perda de pacotes começa a diminuir. O pico de qualidade ocorre quando a distância é mínima. Posteriormente, à medida que os veículos se afastam, a qualidade diminui e a taxa de perda de pacotes aumenta.

Figura 4.2 – Parâmetros no cenário DNPW entre o transmissor car[0] e o receptor car[2]

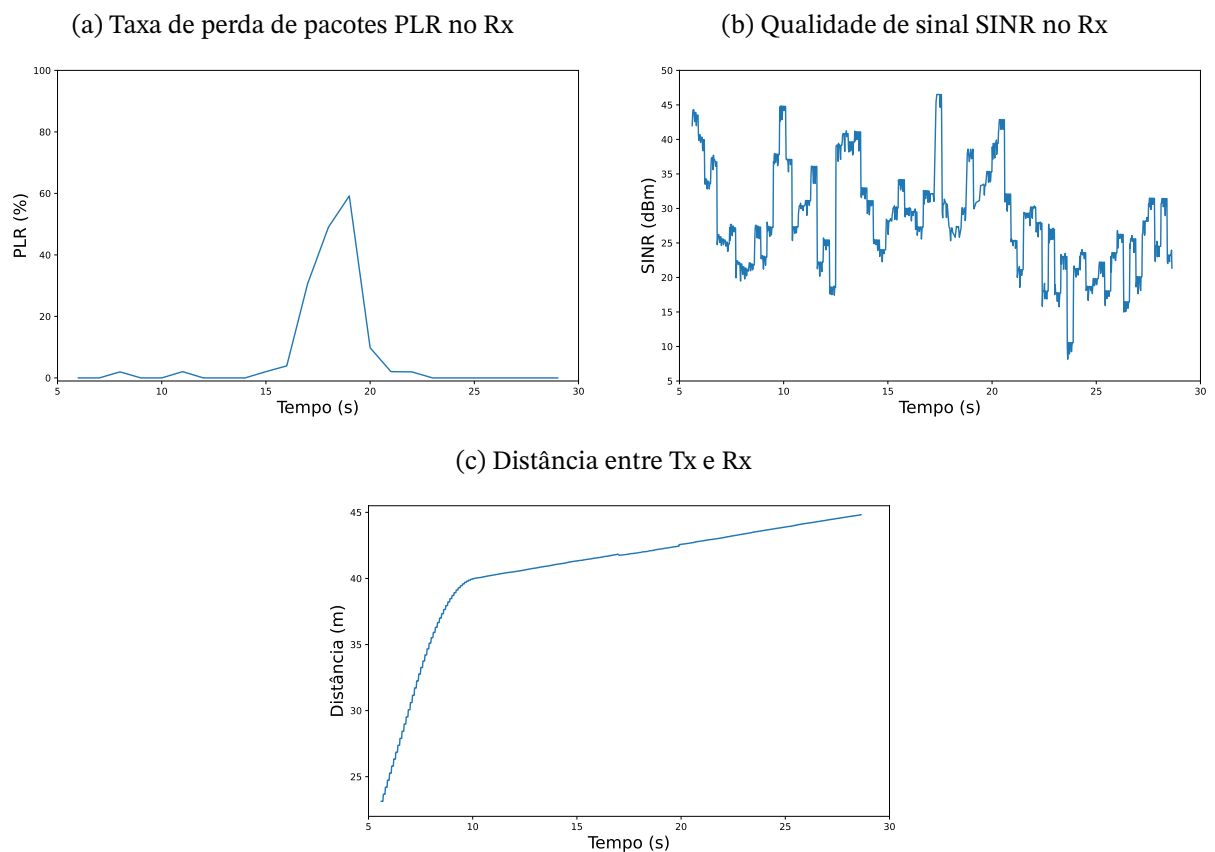


Fonte: Produzido pelo autor.

Os parâmetros no DNPW sem ataque, medidos entre os veículos car[1] e car[2], são apresentados nas figuras a seguir. No início da simulação, conforme a [Figura 4.3c](#), os veículos estão próximos, o que resulta em uma baixa perda de pacotes na [Figura 4.3a](#) e uma alta qualidade de recepção do sinal na [Figura 4.3b](#).

À medida que os veículos se distanciam, ocorre um aumento da taxa de perda de pacotes e a qualidade oscila, mas tende a diminuir conforme o aumento da distância. É importante notar que o pico na taxa de pacotes, que é influenciado pela proximidade com o car[0], acontece entre 15s e 20s. Durante esse intervalo de tempo, o car[0] passa por car[1] e car[2], induzindo uma interferência de célula na comunicação entre eles.

Figura 4.3 – Parâmetros no cenário DNPW entre o transmissor car[1] e o receptor car[2]



Fonte: Produzido pelo autor.

4.3 Parâmetros afetados pelo ataque no cenário DNPW

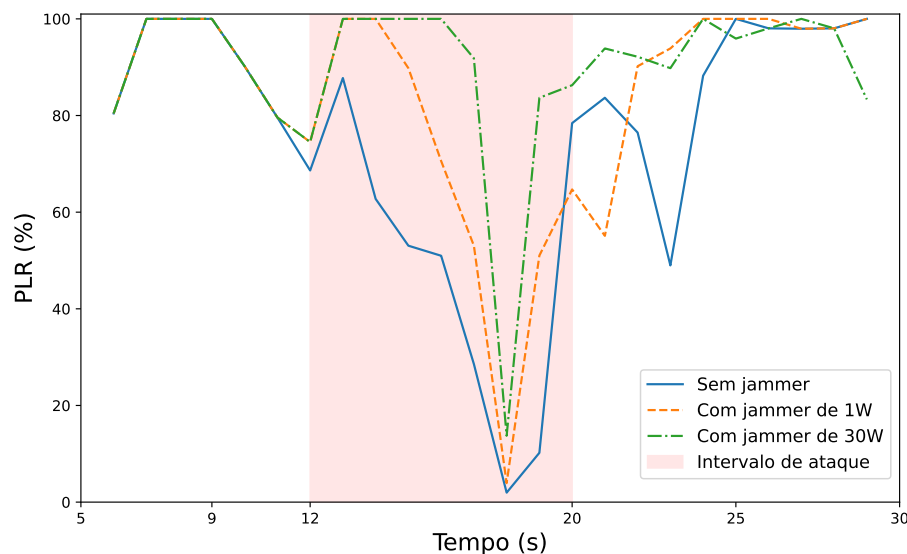
O *jamming* periódico foi selecionado no DNPW entre os tipos de ataque descritos no [Apêndice A](#). Esta escolha é eficiente em termos de energia e *hardware*, já que a interferência induzida pelo *jammer* ocorre em intervalos regulares, alternando entre períodos de ataque e períodos de inatividade, o que reduz o consumo de recursos. Além disso, a programação de ciclos de trabalho em momentos oportunos, como no DNPW, aumenta a eficácia do ataque.

O ataque *jamming* foi implementado no intervalo de tempo entre 12s e 20s, coincidindo com o momento oportuno de aproximação entre os veículos, como evidenciado na [Figura 4.2c](#). Durante este período de ataque, sinais de interferência foram enviados a cada 100ms com o objetivo de prejudicar o recebimento e o processamento dos pacotes de dados no veículo *car[2]*.

A [Figura 4.4](#) mostra a taxa de perda de pacotes entre os nós *car[0]* e *car[2]*, enfatizando o intervalo de ataque representado pela área vermelha. Os dados dos cenários sem interferência *jamming* são representados em azul. Já os casos com ataque, que apresentam *jammer* de potência de saída de 1W e 30W para cada banda, são representados em laranja e verde, respectivamente.

A taxa de perda de pacotes aumenta durante o ataque no intervalo especificado. No cenário sem *jammer*, a taxa de perda é menor. Quando se utiliza um *jammer* com potência de saída de 1W por banda, a taxa de perda se intensifica e se torna ainda maior com o *jammer* de 30W por banda. Após o intervalo de ataque, as taxas não diminuem imediatamente devido à discrepância gerada pelo ataque entre o número de pacotes transferidos e recebidos.

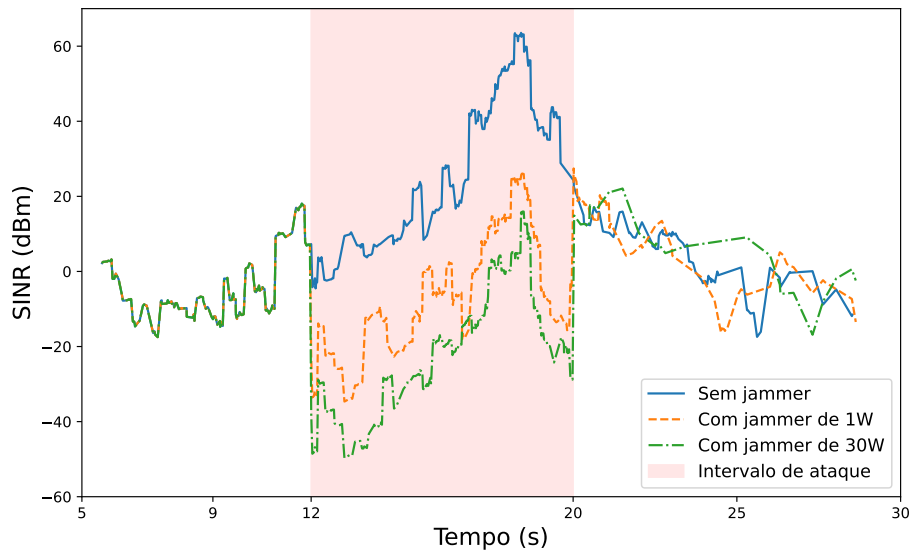
Figura 4.4 – Variação da taxa de perda de pacotes entre *car[0]* e *car[2]* no DNPW



Fonte: Produzido pelo autor.

Em termos de qualidade de sinal, a [Figura 4.5](#) representa a variação do SINR entre os veículos *car[0]* e *car[2]*. Inicialmente, a qualidade varia em torno do limiar de 0 dBm devido à distância significativa entre os nós. No intervalo entre 12s e 20s, devido à proximidade entre os veículos, o sinal sem *jammer* resulta em uma qualidade muito acima do limiar. Por outro lado, nos cenários de ataque com *jammer* de 1W, a qualidade está abaixo do limiar e, no caso de 30W, a qualidade diminui consideravelmente. Após o intervalo de ataque, os veículos se distanciam e a razão SINR nos cenários oscila.

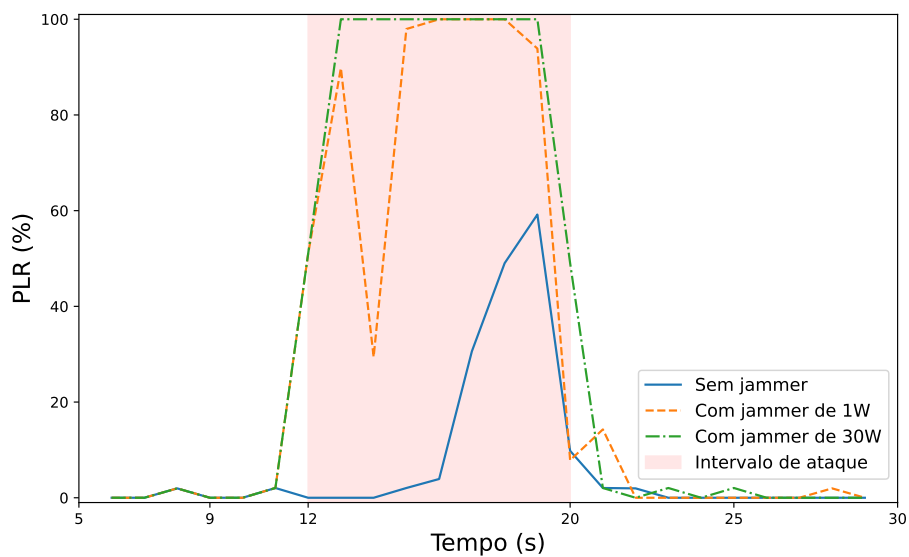
Figura 4.5 – Variação da qualidade de sinal entre car[0] e car[2] no DNPW



Fonte: Produzido pelo autor.

A taxa de perda de pacotes entre os veículos car[1] e car[2] é apresentada na [Figura 4.6](#), com a distância entre os nós sendo relativamente próxima, conforme a [Figura 4.3c](#). Nesse sentido, a perda de pacotes no cenário sem ataque *jamming* é mínima. Entretanto, no intervalo de ataque destacado em vermelho, a perda de pacotes é significativa no caso com *jammer* em laranja e ainda maior no caso em verde, que possui maior potência de saída. Logo após o ataque, as perdas de pacotes nos casos em verde e em laranja tendem a diminuir, mas não imediatamente, devido aos efeitos do ataque.

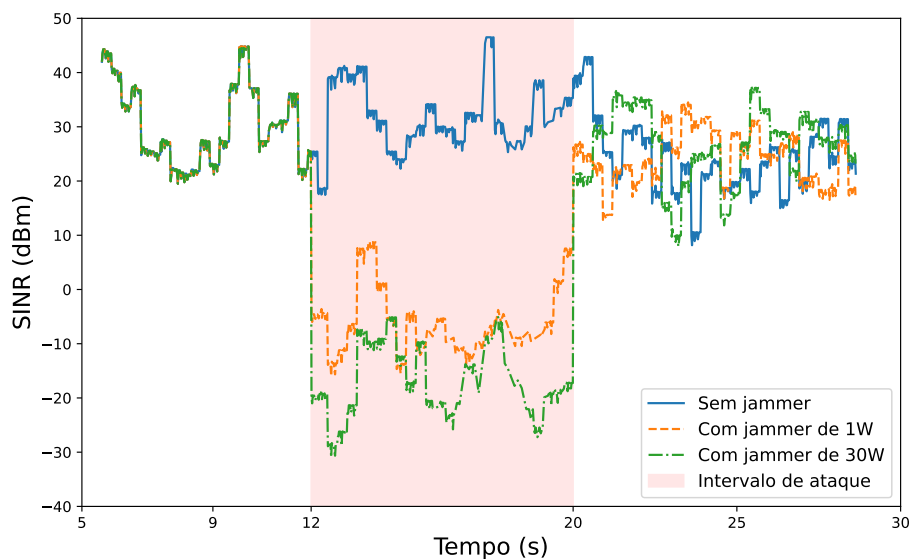
Figura 4.6 – Variação da taxa de perda de pacotes entre car[1] e car[2] no DNPW



Fonte: Produzido pelo autor.

Em termos de qualidade de sinal entre os nós car[1] e car[2], a [Figura 4.7](#) evidencia que a proximidade entre os veículos, no caso sem interferência *jammer*, resulta em uma qualidade significativamente acima do limiar de SINR de 0 dBm. Essa qualidade reflete uma maior transferência de dados e confiabilidade nas comunicações entre os veículos conectados. Entretanto, a razão SINR foi comprometida no intervalo de ataque, no caso em laranja, e foi ainda mais reduzida no caso em verde, com maior potência de saída do *jammer*.

Figura 4.7 – Variação da qualidade de sinal entre car[1] e car[2] no DNPW



Fonte: Produzido pelo autor.

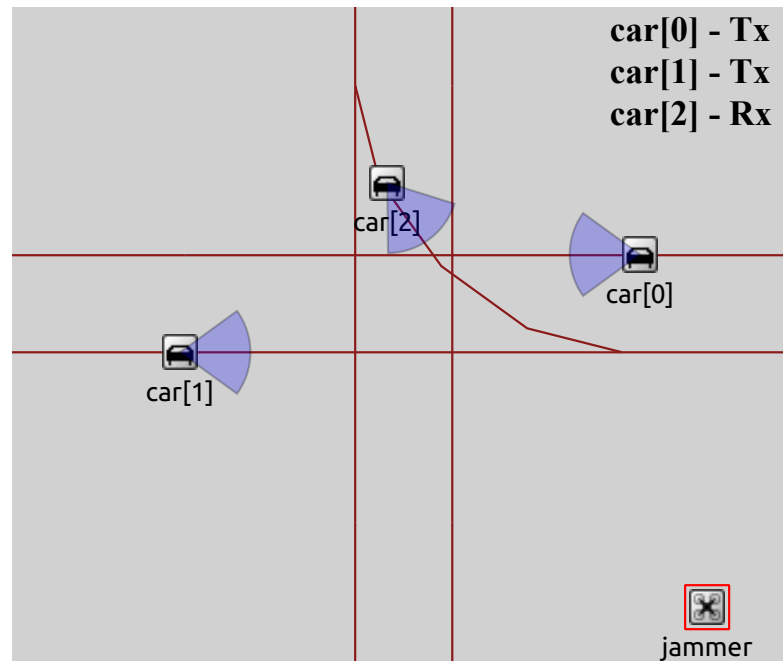
4.4 Simulação do cenário IMA

A representação do cenário IMA, realizada no Simu5G, é ilustrada na [Figura 4.8](#), com as trajetórias possíveis destacadas em linhas vermelhas. A [Figura A.4](#) mostra o instante final da simulação no Simu5G, enquanto a [Figura A.3](#) apresenta o cenário no SUMO.

Os componentes do cenário incluem os carros transmissores car[1] e car[0], sendo este último movendo-se na direção oposta ao primeiro. Além disso, o cenário conta com o carro receptor, car[2], que se move de cima para baixo com a intenção de virar à esquerda no cruzamento. Todos os veículos estão em uma situação de risco, pois car[0], car[1] e car[2] podem estar em rotas de colisão.

Um componente importante é o *jammer*, estrategicamente posicionado e distante na ordem de dezenas de metros dos três veículos. Sua principal função é gerar interferência eletromagnética, que pode comprometer a recepção de pacotes pelo car[2]. Este cenário apresenta um risco significativo, visto que a interferência pode causar falhas na comunicação entre os veículos, aumentando a probabilidade de colisões.

Figura 4.8 – Realização do ataque no cenário IMA



Fonte: Produzido pelo autor.

4.5 Parâmetros analisados no cenário IMA

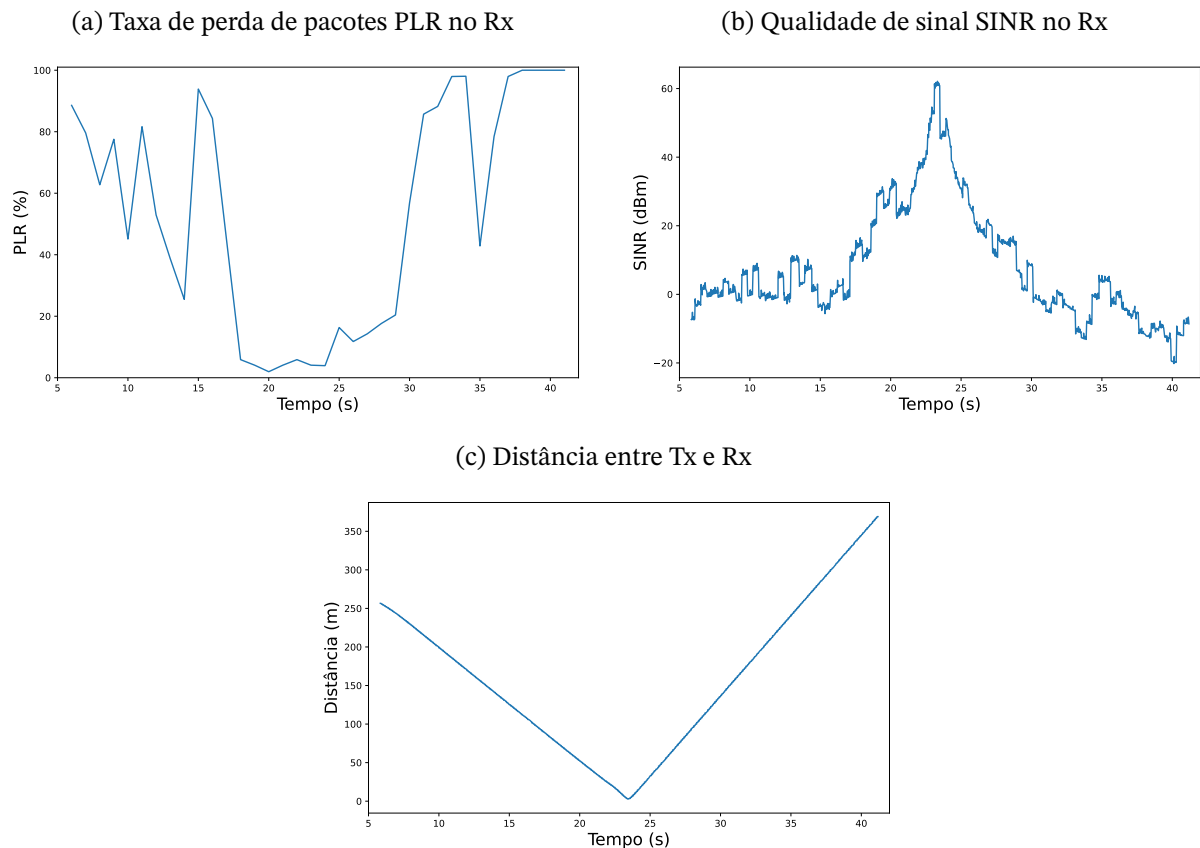
No caso de uso IMA, onde não ocorre o ataque *jamming*, os parâmetros de rede analisados entre os nós car[0] e car[2] são detalhados nas figuras subsequentes de forma sistemática. A [Figura 4.9a](#) ilustra a taxa de perda de pacotes ao longo do tempo, conforme estipulado na [Observação 2.2](#).

A [Figura 4.9b](#) exibe a razão SINR, que indica a qualidade do sinal recebido no canal em comparação com ruídos e interferências, conforme descrito na [Equação 2.1](#). Ademais, a [Figura 4.9c](#) demonstra a distância entre os nós ao longo do tempo, fornecendo um panorama complementar que elucida a análise.

No início da simulação, a distância considerável entre o car[1] e car[2] resulta em uma alta taxa de perda de pacotes, também refletida pela baixa qualidade com valores de SINR abaixo do limiar de 0 dBm. À medida que os veículos se aproximam, a qualidade do sinal melhora e a taxa de perda de pacotes começa a diminuir.

O ponto máximo de qualidade é alcançado quando a distância entre os veículos é mínima, indicando uma correlação entre a distância e a qualidade do sinal. No entanto, à medida que os veículos começam a se distanciar, a qualidade do sinal decai e a taxa de perda de pacotes volta a aumentar, reforçando a importância crucial da proximidade entre veículos para a eficácia da comunicação.

Figura 4.9 – Parâmetros no cenário IMA entre o transmissor car[0] e o receptor car[2]



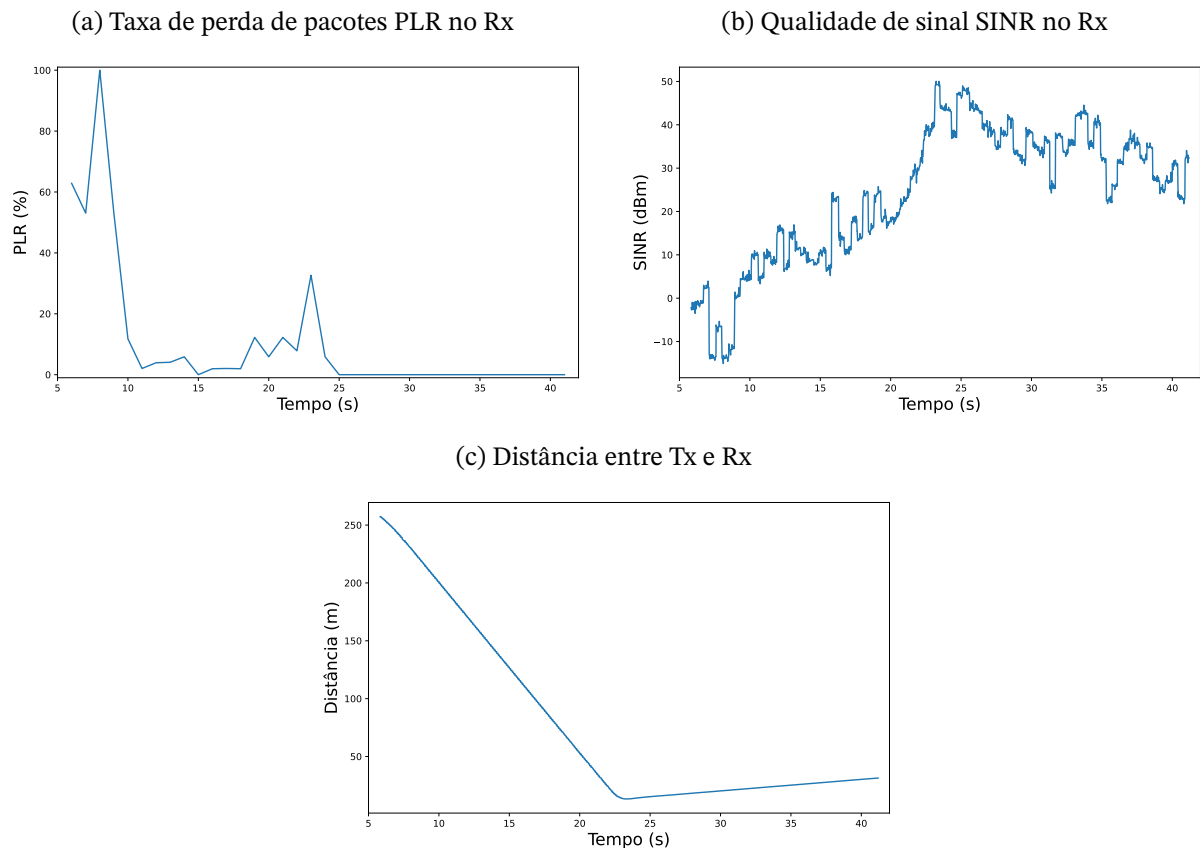
Fonte: Produzido pelo autor.

Os parâmetros no cenário IMA sem interferência *jamming*, determinado entre os veículos car[1] e car[2], são retratados nas figuras subsequentes. No começo da simulação, como visto na [Figura 4.10c](#), os veículos estão distantes na ordem de centenas de metros, resultando em uma alta taxa de perda de pacotes, conforme a [Figura 4.10a](#), e a uma qualidade de sinal baixa, como indicado na [Figura 4.10b](#).

À medida que os veículos se aproximam, a taxa de perda de pacotes, inicialmente alta, começa a diminuir na [Figura 4.10a](#). Paralelamente, a [Figura 4.10b](#) mostra que a qualidade do sinal é baixa no início devido à distância entre os veículos, mas começa a melhorar de forma significativa.

Por fim, quando os veículos car[1] e car[2] começam a seguir o mesmo sentido de deslocamento, a qualidade do sinal se mantém alta. A proximidade contínua entre os veículos facilita uma comunicação eficiente. Assim, manter os veículos próximos é um fator determinante para otimização da qualidade do sinal e da taxa de perda de pacotes.

Figura 4.10 – Parâmetros no cenário IMA entre o transmissor car[1] e o receptor car[2]



Fonte: Produzido pelo autor.

4.6 Parâmetros afetados pelo ataque no cenário IMA

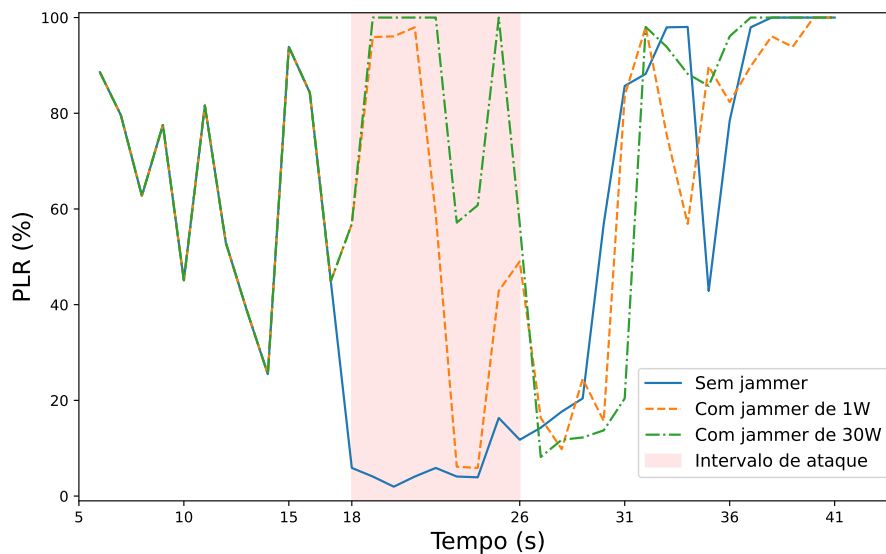
A opção de implementar o ataque de *jamming* periódico no IMA, dentre os ataques mencionados no [Apêndice A](#), foi feita considerando suas características. A interferência causada pelo *jammer* ocorre em intervalos fixos, alternando entre momentos de ataque e momentos de inatividade, o que pode potencialmente minimizar o uso de recursos. Além disso, a possibilidade de programar ciclos de trabalho em momentos estratégicos, como em situações de risco no IMA, pode aumentar a eficácia do ataque de *jamming*.

A implementação do ataque foi realizada no intervalo de tempo de 18s a 26s, que se alinhou com o momento de maior proximidade entre os veículos, conforme ilustrado na [Figura 4.9c](#). Durante esse período de ataque, sinais de interferência foram enviados a cada 100ms com o propósito de prejudicar a recepção dos pacotes de dados no veículo car[2].

A [Figura 4.11](#) exibe a taxa de perda de pacotes entre os nós car[0] e car[2], com ênfase no período de ataque indicado pela área em vermelho. Os dados dos cenários sem interferência *jamming* são apresentados em azul. Em contraste, nos cenários IMA que foram adaptados para incluir um ataque, as cores laranja e verde representam, respectivamente, um *jammer* de potência de saída de 1W e 30W para cada banda.

Durante o ataque no intervalo especificado, há um incremento na taxa de perda de pacotes. No cenário que não faz uso de um *jammer*, a taxa de perda é mais baixa. A implementação de um *jammer* com potência de saída de 1W por banda provoca um aumento expressivo na taxa de perda, que se amplifica ainda mais com o *jammer* de 30W por banda. Após o término do ataque, as taxas de perda não retornam imediatamente ao estado anterior devido à diferença causada pelo ataque entre o número de pacotes enviados e recebidos.

Figura 4.11 – Variação da taxa de perda de pacotes entre car[0] e car[2] no IMA



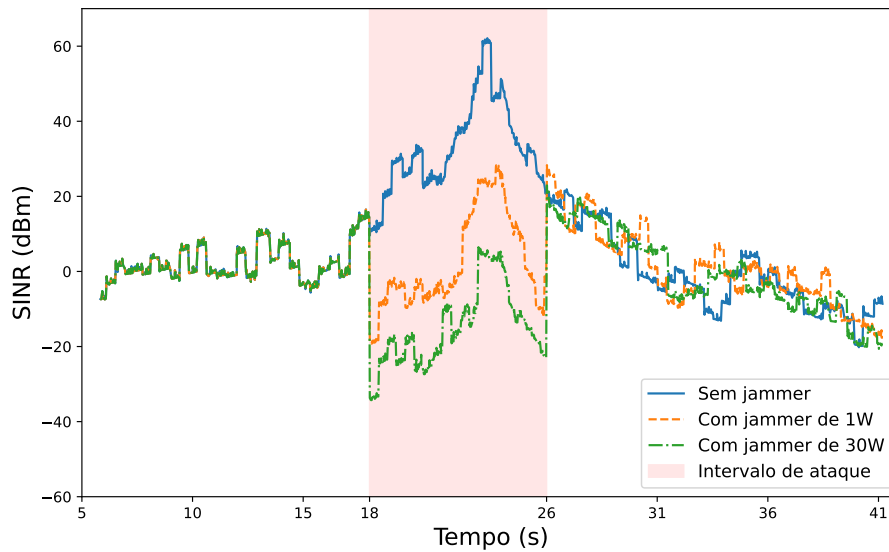
Fonte: Produzido pelo autor.

A [Figura 4.12](#) destaca a mudança da razão SINR entre os veículos car[0] e car[2], um parâmetro crucial para avaliar a qualidade do sinal em sistemas de comunicação de veículos conectados. No início da observação, a qualidade do sinal apresenta uma tendência de oscilação em torno do limiar de 0 dBm. Este comportamento é atribuído à distância considerável entre os nós.

Durante o intervalo de tempo de 18s a 26s, há uma mudança notável que é atribuída à proximidade entre os veículos. Neste cenário, na ausência de um *jammer*, a qualidade do sinal é superior ao limiar de 0 dBm. Este fato destaca que a proximidade entre os nós pode ter um impacto positivo na qualidade do sinal, facilitando uma comunicação mais efetiva entre os veículos.

Porém, nos cenários em que um ataque com um *jammer* de 1W ocorre, a qualidade do sinal fica, na maior parte do tempo, abaixo do limiar. Quando o *jammer* tem uma potência de saída de 30W, a qualidade do sinal diminui ainda mais. Após o fim do ataque, à medida que os veículos se afastam, a qualidade do sinal nos cenários começa a variar e mostra uma tendência de queda.

Figura 4.12 – Variação da qualidade de sinal entre car[0] e car[2] no IMA

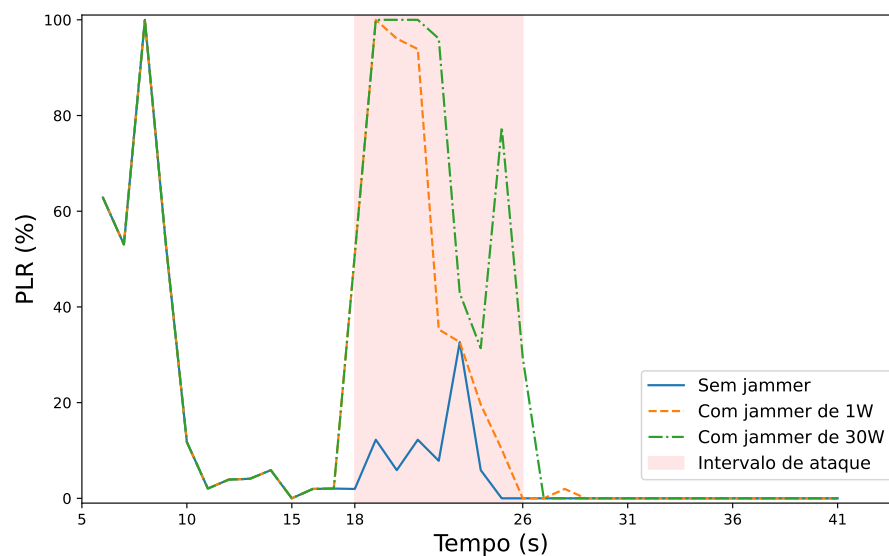


Fonte: Produzido pelo autor.

A Figura 4.13 exibe a taxa de perda de pacotes entre os veículos car[1] e car[2]. Com os nós inicialmente distantes, como indicado na Figura 4.10c, a perda de pacotes no cenário sem ataque *jamming* é inicialmente alta, mas diminui à medida que os veículos se aproximam do cruzamento.

Durante o intervalo de ataque, marcado em vermelho, a perda de pacotes é considerável no caso com *jammer* em laranja e ainda mais intensa no caso em verde, que tem uma potência de saída maior. Após o ataque, as perdas de pacotes nos casos em verde e laranja começam a diminuir, mas não imediatamente, refletindo as consequências do ataque.

Figura 4.13 – Variação da taxa de perda de pacotes entre car[1] e car[2] no IMA

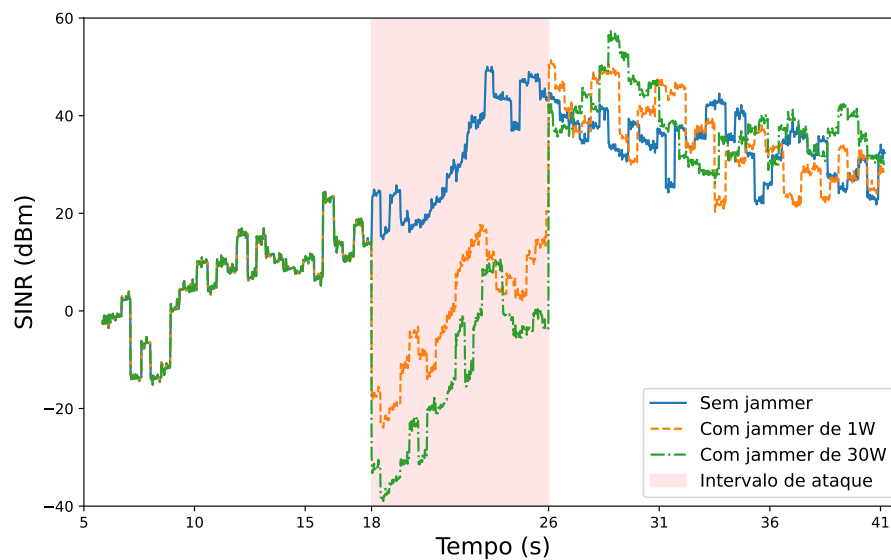


Fonte: Produzido pelo autor.

A Figura 4.14 mostra a qualidade do sinal entre os nós car[1] e car[2]. Inicialmente, a considerável distância entre os nós resulta em uma qualidade de sinal próxima ao limiar de SINR de 0 dBm. Conforme os veículos se aproximam, a qualidade do sinal melhora progressivamente.

No entanto, durante o intervalo de ataque, a qualidade do sinal é afetada, sendo mais comprometida no caso em laranja e ainda mais no caso em verde, onde o *jammer* tem uma maior potência de saída. Após o intervalo de ataque, os veículos continuam próximos, o que mantém a qualidade do sinal recebido alta.

Figura 4.14 – Variação da qualidade de sinal entre car[1] e car[2] no IMA



Fonte: Produzido pelo autor.

5 Conclusões

Este trabalho descreveu as etapas e estratégias adotadas para modelar cenários de DNPW, IMA e ataques *jamming* em uma rede de veículos autônomos com comunicações V2X. O processo para realizar as simulações e análises, bem como as ferramentas de simulação empregadas, foram detalhados.

Os resultados obtidos nas simulações e análises foram apresentados, fazendo uma comparação entre os cenários simulados que foram afetados pela interferência emitida pelo *jammer* nos canais de recepção. Parâmetros como a qualidade do sinal recebido, a taxa de perda de pacotes entre transmissores e receptores, a distância entre veículos e a potência de saída do *jammer* foram considerados.

Nos cenários DNPW e IMA, onde não há interferência, as curvas de recepção de pacotes entre os veículos demonstram o comportamento confiável de comunicação esperado quando estão próximos. Contudo, nos cenários onde ocorrem ataques, observa-se uma queda na qualidade e um aumento na taxa de perda de pacotes. Essas ocorrências são mais acentuadas durante os intervalos de ataque, resultando em uma diferença na transferência e recebimento de pacotes que não é imediatamente recuperada.

A partir das análises realizadas, destaca-se a importância de implementar medidas de segurança avançadas para proteger a integridade das comunicações em ambientes de transportes inteligentes. É evidente a necessidade de desenvolver contramedidas eficazes para mitigar ataques *jamming* e assegurar a confiabilidade das redes de comunicação de veículos autônomos.

Em trabalhos futuros, propõe-se a criação de estratégias específicas para combater os ataques modelados. Tais estratégias incluem o controle de potência nos canais de recepção, a aplicação de filtros estocásticos como de Beamforming e de Kalman, além de técnicas adaptativas e de aprendizado de máquina. Essas contramedidas serão fundamentais para garantir a confiabilidade da comunicação entre os veículos autônomos, preservando a integridade dos canais de informação e a segurança dos indivíduos.

Referências

- CHEN, S.; HU, J.; SHI, Y.; PENG, Y.; FANG, J.; ZHAO, R.; ZHAO, L. Vehicle-to-Everything (V2X) services supported by LTE-based systems and 5G. **IEEE**, v. 1, n. 2, p. 70–76, 2017. Citado na p. 19.
- CHEN, S.; HU, J.; SHI, Y.; ZHAO, L.; LI, W. A vision of C-V2X: Technologies, field testing, and challenges with chinese development. **IEEE**, v. 7, n. 5, p. 3872–3881, 2020. Citado na p. 18.
- FENG, Y.; HUANG, S. E.; WONG, W.; CHEN, Q. A.; MAO, Z. M.; LIU, H. X. On the cybersecurity of traffic signal control system with connected vehicles. **IEEE**, v. 23, n. 9, p. 16267–16279, 2022. Citado na p. 25.
- GUAN, T.; HAN, Y.; KANG, N.; TANG, N.; CHEN, X.; WANG, S. An overview of vehicular cybersecurity for intelligent connected vehicles. **Sustainability**, v. 14, n. 9, p. 5211, 2022. Citado na p. 16.
- HAROUNABADI, M.; SOLEYMANI, D. M.; BHADAURIA, S.; LEYH, M.; ROTH-MANDUTZ, E. V2X in 3GPP standardization: NR sidelink in release-16 and beyond. **IEEE**, v. 5, n. 1, p. 12–21, 2021. Citado na p. 18.
- HBAIEB, A.; RHAJEM, O. B.; CHAARI, L. In-car gateway architecture for intra and inter-vehicular networks. *In: 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*. [S.l.]: IEEE, 2018. p. 1489–1494. Citado na p. 15.
- JIANG, D.; DELGROSSI, L. IEEE 802.11p: Towards an international standard for wireless access in vehicular environments. *In: . [S.l.: s.n.]*, 2008. p. 2036–2040. Citado na p. 18.
- KATO, S.; TAKEUCHI, E.; ISHIGURO, Y.; NINOMIYA, Y.; TAKEDA, K.; HAMADA, T. An open approach to autonomous vehicles. **IEEE**, v. 35, n. 6, p. 60–68, 2015. Citado na p. 15.
- KRAYANI, A.; BARABINO, G.; MARCENARO, L.; REGAZZONI, C. Integrated sensing and communication for joint GPS spoofing and jamming detection in vehicular V2X networks. *In: IEEE. 2023 IEEE Wireless Communications and Networking Conference (WCNC)*. [S.l.], 2023. p. 1–7. Citado nas pp. 25 e 28.
- KRAYANI, A.; WILLIAM, N.; MARCENARO, L.; REGAZZONI, C. Jammer detection in vehicular V2X networks. *In: . [S.l.: s.n.]*, 2022. Citado nas pp. 21 e 28.
- LOPEZ, P. A.; BEHRISCH, M.; BIEKER-WALZ, L.; ERDMANN, J.; FLÖTTERÖD, Y.-P.; HILBRICH, R.; LÜCKEN, L.; RUMMEL, J.; WAGNER, P.; WIESSNER, E. Microscopic

- traffic simulation using SUMO. *In: The 21st IEEE International Conference on Intelligent Transportation Systems*. [S.l.: s.n.], 2018. Citado na p. 30.
- MORADI-PARI, E.; TIAN, D.; BAHRAMGIRI, M.; RAJAB, S.; BAI, S. DSRC versus LTE-V2X: Empirical performance analysis of direct vehicular communication technologies. *IEEE*, v. 24, n. 5, p. 4889–4903, 2023. Citado na p. 18.
- NARDINI, G.; SABELLA, D.; STEA, G.; THAKKAR, P.; VIRDIS, A. Simu5G – An OMNeT++ library for end-to-end performance evaluation of 5G networks. *IEEE*, v. 8, p. 181176–181191, 2020. Citado nas pp. 28, 29, 39 e 40.
- OTHMAN, K. Public acceptance and perception of autonomous vehicles: a comprehensive review. *AI Ethics*, v. 1, n. 3, p. 355–387, 2021. Citado na p. 15.
- PELECHRINIS, K.; BROUSTIS, I.; KRISHNAMURTHY, S. V.; GKANTSIDIS, C. A measurement-driven anti-jamming system for 802.11 networks. *IEEE*, v. 19, n. 4, p. 1208–1222, 2011. Citado nas pp. 20 e 28.
- PIRAYESH, H.; ZENG, H. Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. *IEEE*, v. 24, p. 767–809, 2021. Citado na p. 59.
- PUSAPATI, S.; SELIM, B.; NIE, Y.; LIN, H.; PENG, W. Simulation of NR-V2X in a 5G environment using OMNeT++. *In: 2022 IEEE Future Networks World Forum (FNWF)*. [S.l.: s.n.], 2022. p. 634–638. Citado na p. 30.
- SEREDYNSKI, P. **Autonomous vehicles and their cloud computing networks**. 2021. SAE International. <https://www.sae.org/news/2021/04/autonomous-vehicles-and-their-cloud-computing-networks> – acesso em 15 jul. 2023. Citado na p. 15.
- SHEN, J.; WAN, Z.; LUO, Y.; FENG, Y.; MAO, Z. M.; CHEN, Q. A. Detecting data spoofing in connected vehicle based intelligent traffic signal control using infrastructure-side sensors and traffic invariants. *In: 2023 IEEE Intelligent Vehicles Symposium (IV)*. [S.l.: s.n.], 2023. p. 1–8. Citado na p. 26.
- SILVA, A. S. D.; COSTA, J. P. J. D.; SANTOS, G. A.; MIRI, Z.; FAUZI, M. I. B. M.; VINEL, A.; FREITAS, E. P. de; KASTELL, K. Radio jamming in vehicle-to-everything communication systems: Threats and countermeasures. *In: 2023 23rd International Conference on Transparent Optical Networks (ICTON)*. [S.l.: s.n.], 2023. p. 1–4. Citado nas pp. 16, 34, 35 e 36.
- SOMMER, C.; GERMAN, R.; DRESSLER, F. Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis. *IEEE*, v. 10, n. 1, p. 3–15, 2011. Citado na p. 29.
- TONG, W.; HUSSAIN, A.; BO, W. X.; MAHARJAN, S. Artificial intelligence for Vehicle-to-Everything: A survey. *IEEE*, v. 7, p. 10823–10843, 2019. Citado nas pp. 15 e 16.

-
- TWARDOKUS, G.; RAHBARI, H. Toward protecting 5G sidelink scheduling in C-V2X against intelligent DoS attacks. **IEEE**, v. 22, n. 11, p. 7273–7286, 2023. Citado nas pp. 22 e 28.
- WYGLINSKI, A. M.; WICKRAMARATHNE, T.; CHEN, D.; KIRSCH, N. J.; GILL, K. S.; JAIN, T.; GARG, V.; LI, T.; PAUL, S.; XI, Z. Phantom car attack detection via passive opportunistic RF localization. **IEEE**, v. 11, p. 27676–27692, 2023. Citado nas pp. 24 e 28.
- YANG, M.; JU, Y.; LIU, L.; PEI, Q.; YU, K.; RODRIGUES, J. J. P. C. Secure mmWave C-V2X communications using cooperative jamming. *In: 2022 IEEE Global Communications Conference GLOBECOM*. [S.l.: s.n.], 2022. p. 2686–2691. Citado nas pp. 23, 24 e 28.
- YANG, X.; SHI, Y.; XING, J.; LIU, Z. Autonomous driving under V2X environment: state-of-the-art survey and challenges. **Intelligent Transportation Infrastructure**, v. 1, 2022. Citado na p. 18.
- YANG, Z.; YING, J.; SHEN, J.; FENG, Y.; CHEN, Q. A.; MAO, Z. M.; LIU, H. X. Anomaly detection against GPS spoofing attacks on connected and autonomous vehicles using learning from demonstration. **IEEE**, v. 24, n. 9, p. 9462–9475, 2023. Citado na p. 27.
- YAO, Y.; ZHAO, J.; LI, Z.; CHENG, X.; WU, L. Jamming and eavesdropping defense scheme based on deep reinforcement learning in autonomous vehicle networks. **IEEE**, v. 18, p. 1211–1224, 2023. Citado nas pp. 19 e 28.

Apêndices

Apêndice A – Tipos de ataque *jamming*

A seguir estão listados os tipos de ataque *jamming* em telecomunicações, conforme descritos em (Pirayesh; Zeng, 2021). Cada ataque apresenta características distintas em termos de impacto nas comunicações, eficiência energética e padrões de interferência.

- *Constant jamming*: são ataques nos quais dispositivos *jammers* emitem sinais potentes de forma contínua, interrompendo as transmissões legítimas e ocupando o canal.
- *Reactive jamming*: conhecidos como ataques conscientes de canal, são desencadeados pela detecção de transmissões legítimas. Eles são eficientes, mas exigem controles temporais estritos para operar.
- *Deceptive jamming*: envolvem o envio de vários sinais de rádio para desperdiçar recursos de redes, impedindo o acesso legítimo ao canal via saturação.
- *Random jamming*: o dispositivo *jammer* emite sinais de interferência por períodos aleatórios, poupando energia em relação aos ataques constantes.
- *Periodic jamming*: o dispositivo *jammer* emite pulsos de interferência de forma previsível e regular. Pode ser mais eficiente em termos de consumo de energia do que os ataques aleatórios, desde que o ciclo de trabalho seja controlado de forma eficiente.
- *Frequency sweeping jamming*: permite que um *jammer* alterne rapidamente entre múltiplos canais, visando prejudicar as redes, mesmo com limitações de *hardware*.

Tabela A.1 – Comparação dos mecanismos de ataque *jamming*

Mecanismo	Pontos fortes	Pontos fracos
<i>Constant jamming</i>	Altamente eficaz	Ineficiente em energia
<i>Reactive jamming</i>	Altamente eficaz	Limitações de <i>hardware</i>
<i>Deceptive jamming</i>	Eficiente em energia	Menos eficaz
<i>Random jamming</i>	Eficiente em energia	Menos eficaz
<i>Periodic jamming</i>	Eficiente em energia	Menos eficaz
<i>Frequency sweeping jamming</i>	Altamente eficaz	Ineficiente em energia

Fonte: (Pirayesh; Zeng, 2021)

Apêndice B – Códigos de programação

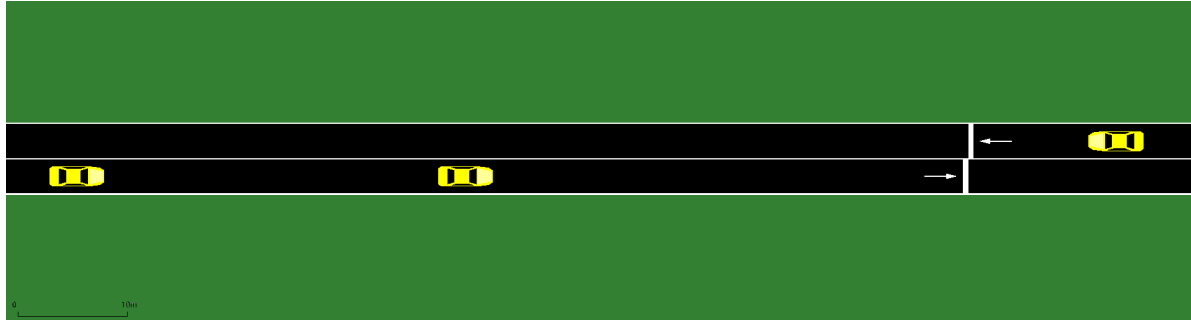
Os códigos desenvolvidos neste trabalho estão disponíveis via Github¹.

¹ <https://github.com/deivis6x7/V2X>

Anexos

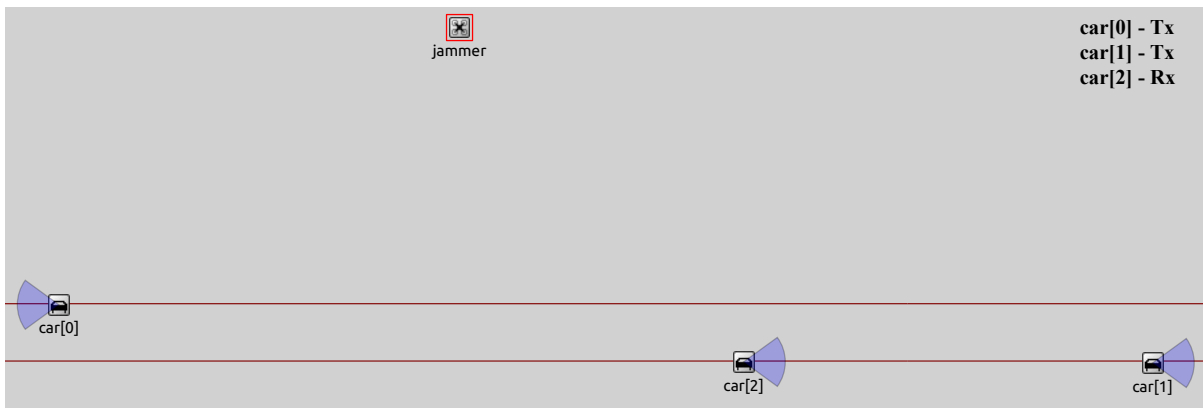
Anexo A – Figuras dos cenários

Figura A.1 – Cenário DNPW no SUMO



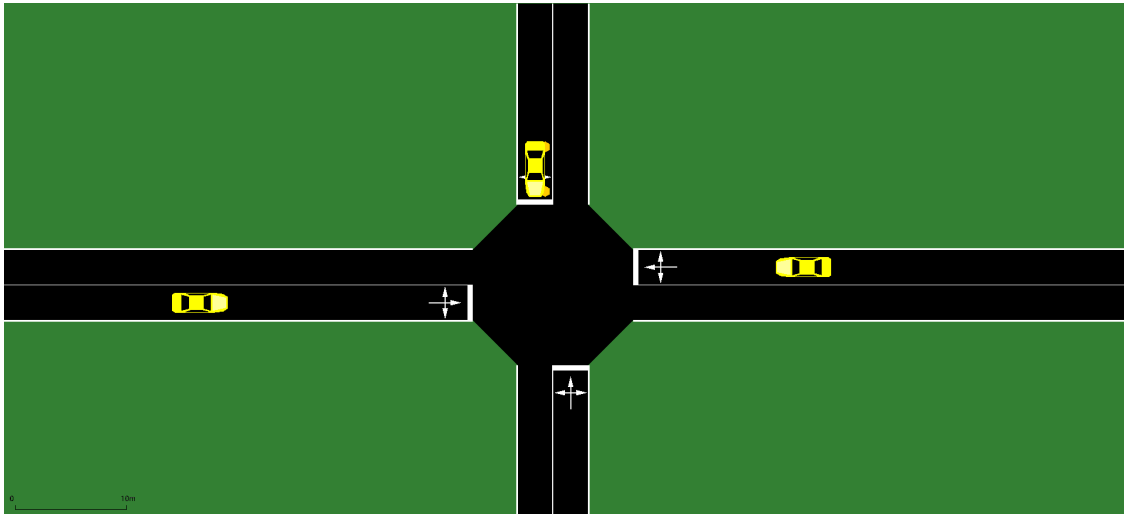
Fonte: Produzido pelo autor.

Figura A.2 – Etapa final do ataque no cenário DNPW



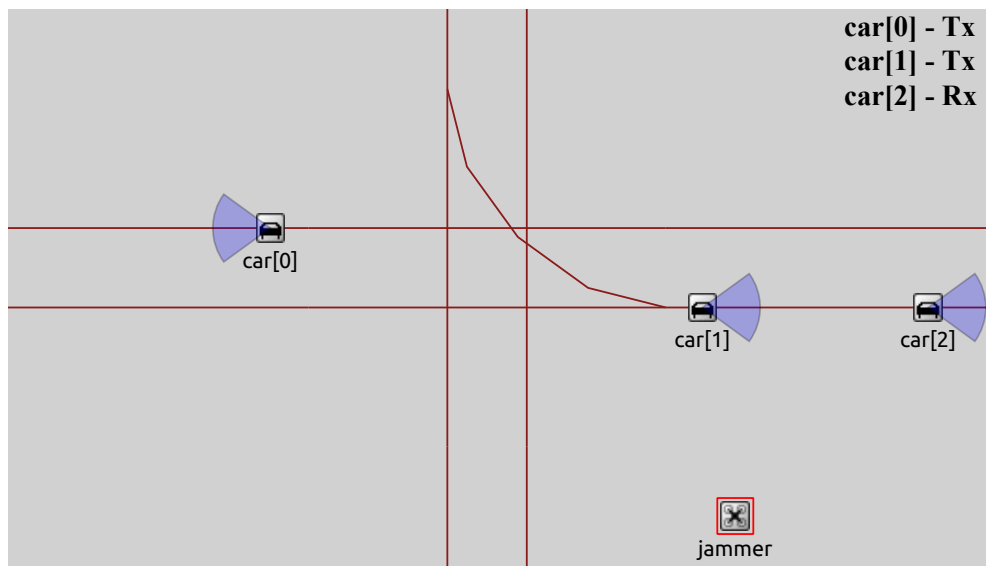
Fonte: Produzido pelo autor.

Figura A.3 – Cenário IMA no SUMO




Fonte: Produzido pelo autor.

Figura A.4 – Etapa final do cenário IMA



























Fonte: Produzido pelo autor.

Anexo B – Cronograma de atividades

O cronograma [Tabela B.1](#), com ícones de Triângulos de Sierpinski de ordem 4 , lista dez tarefas em 2023 a serem desenvolvidas no Trabalho de Graduação (TG). Cada tarefa tem um prazo alinhado ao calendário da UnB.

- **Tarefa 1** - Revisão bibliográfica e estudos teóricos.
- **Tarefa 2** - Análise da documentação do Veins e simuladores complementares.
- **Tarefa 3** - Modelagem de cenários de caso de uso em V2X no Veins.
- **Tarefa 4** - Escrita do relatório de TG1.
- **Tarefa 5** - Análise da documentação do Simu5G e simuladores complementares.
- **Tarefa 6** - Modelagem de cenários de caso de uso em V2X no Simu5G.
- **Tarefa 7** - Implementação e validação de ataque *jamming*.
- **Tarefa 8** - Escrita do relatório de TG2.
- **Tarefa 9** - Apresentação para banca examinadora.
- **Tarefa 10** - Entrega do relatório final.

Tabela B.1 – Cronograma de atividades do TG

Etapa	março	abril	maio	junho	julho
1					
2					
3					
4					
Etapa	agosto	setembro	outubro	novembro	dezembro
1					
5					
6					
7					
8					
9					
10					