Linha Redes VEICULARES

IC – Instituto de Computação
UNICAMP

Campinas, May 21st, 2024

HVCFL: Um Estudo de Aprendizado Federado Centralizado, Descentralizado e Híbrido em Redes Veiculares com Dados não-IID

Introdução

- Aprendizado Federado pode ser centralizado (com servidor coordenador), descentralizado (agentes se comunicam entre si) ou híbrido
- Desafios da centralização: ponto único de falha, escalabilidade, dados não-IID
- Desafios da descentralização: sincronização, disseminação de informação mais lenta, dados não-IID
- VANETs (Vehicle Ad Hoc Networks) são redes sem fio broadcast com veículos e a infraestrutura, com a capacidade de prover serviços
- Desafios VANETs: rede de curto alcance, mobilidade, rede desconexa temporariamente, shadowing

Objetivos

- Adaptar métodos de aprendizado federado com dados não-IID, feitos para redes estáticas, para redes veiculares, como o WSCC (Weight-Similarity Client Clustering)[1]
- Criar um método híbrido de aprendizado federado para tratar dos diferentes desafios
- Experimentos com simulações de redes veiculares (OMNeT++/Veins/SUMO e mapa de Luxemburgo[2]) e diferentes distribuições de dados não-IID

1. Pu Tian, Weixian Liao, Wei Yu, and Erik Blasch. Wscc: A weight-similarity-based client clustering approach for non-iid federated learning. IEEE Internet of Things Journal, 9(20):20243–20256, 2022.
2. Lara Codecá, Raphaël Frank, Sébastien Faye, and Thomas Engel. Luxembourg SUMO Traffic (LuST) Scenario: Traffic Demand Evaluation. IEEE Intelligent Transportation Systems Magazine, 9(2):52–63, 2017.

Soluções Propostas

- Utilizar comunicação entre veículos e também com a infraestrutura
- WSCC utiliza métricas de similaridade para criar grupos (clusters) de usuários com distribuiçoes de dados similares no servidor
- WSVC (Weight-Similarity Vehicle Clustering) proposto é um método centralizado para VANETs adaptando WSCC
- HVCFL (Hybrid Vehicle Clustered Federated Learning) proposto utiliza o servidor do WSVC e também inclui a lógica de clusters em cada veículo

Arquitetura

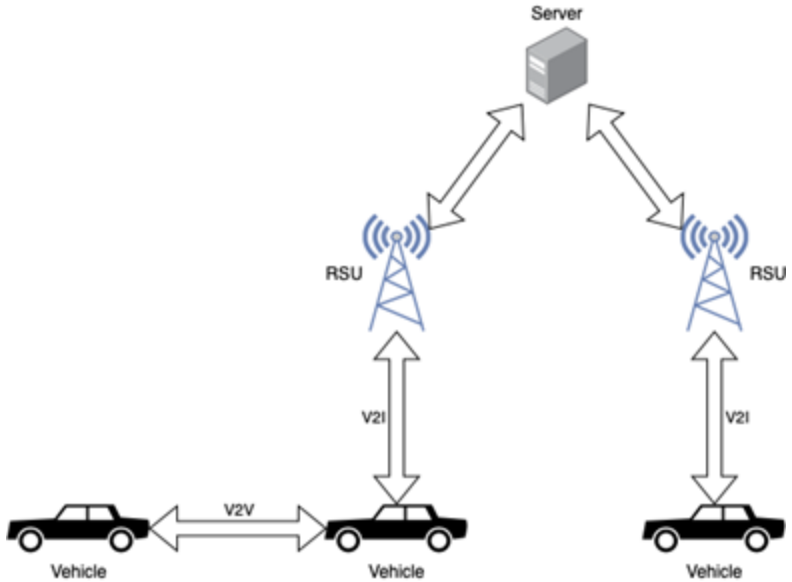


Figura 1: Arquitetura da solução com comunicação entre os veículos e com a infraestrutura

Resultados

Methods	Balanced Accuracy		
	FMNIST 4 Rotations	FMNIST Dirichlet	FMNIST WSCC
Personalized FedAvg	75.39%	73.09%	84.24%
WSVC	77.75%	72.40%	84.78%
Gossip Learning	77.81%	70.31%	85.05%
Decentralized WSCC	82.77%	70.53%	86.91%
HVCFL	**83.47%**	**74.83%**	**87.06%**

Tabela 1: Resultados da acurácia balanceada para o dataset Fashion MNIST e diferentes distribuições de dados

- Métodos centralizados convergem mais rapidamente para distribuições de dados de convergência mais lenta
- Métodos centralizados perdem alguns veículos que não conseguem se comunicar com a infraestrutura da rede
- Métodos híbridos conseguem um melhor resultado final para os desafios, mas gastando mais mensagens
- Entretanto, métodos centralizados atingem melhores resultados quanto maior a cobertura da infraestrutura da rede

SeqWatch:

Unsupervised Sequence-based Intrusion Detection System for Automotive Ethernet

Maurício S. G. A. Leandro, Paulo Freitas de Araujo-Filho,
Divanilson R. Campelo, Luigi F. Marques da Luz, 2025

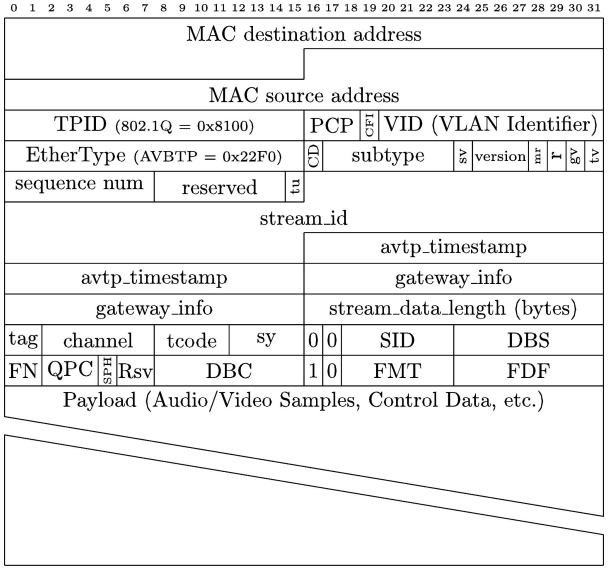
Centro de Informática UFPE
Universidade Federal de Pernambuco

Automotive Ethernet

Automotive **Ethernet** as a high-bandwidth, flexible IVN solution

- Several standards such as IEEE 100BASE-T1
  - Meet bandwidth requirements
- AVB/TSN standards
  - Ensure the **deterministic** traffic, **timely**, and **synchronized** transmission of critical data
    - Audio–video Transport Protocol (AVTP)
    - Precision Time Protocol (gPTP)

Ethernet must coexist with CAN, which remains cost-effective and efficient for safety-critical applications



Structure of stream AVTP [12]

Problem statement

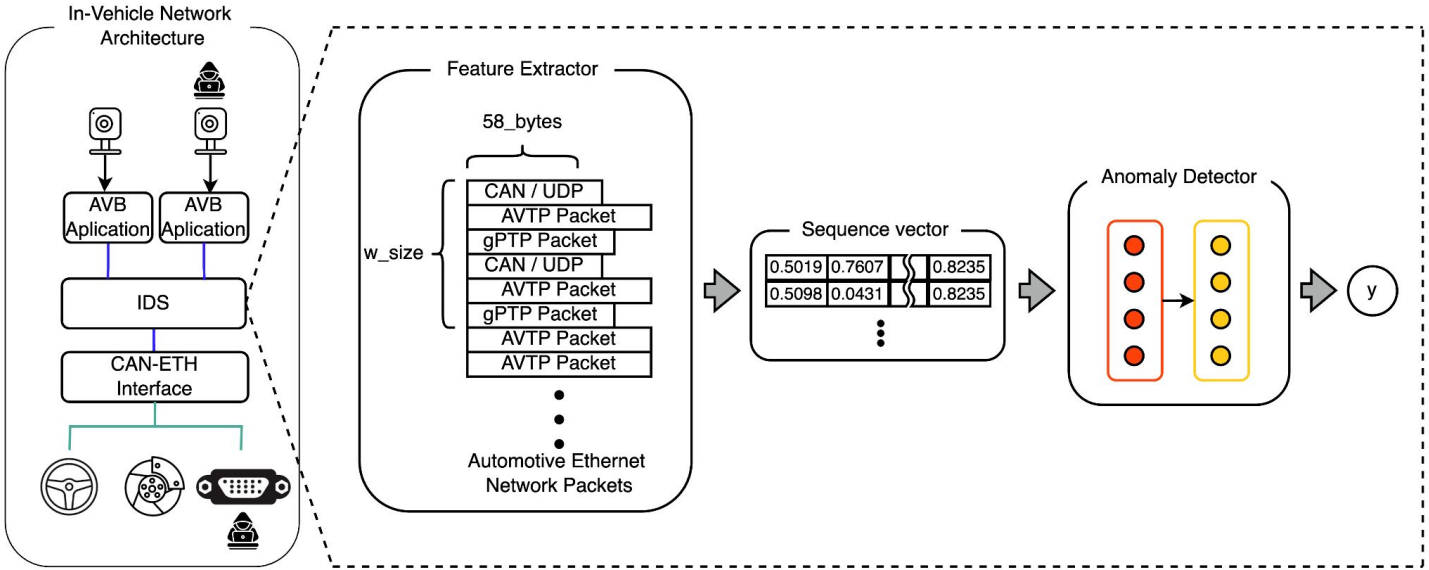
Is it possible to develop sequential **ML-based Intrusion Detection Systems** with the potential to detect known and **unknown (zero-day) attacks** on automotive Ethernet networks?

Contributions

SeqWatch proposal

- Offline **unsupervised** anomaly-based IDS
  - Designed to **detect known and unknown (zero-day) attacks**
- Leverages sequential ML models
  - **Capture the temporal relationships** in network traffic
- State-of-art systems comparison
  - Baseline works
- Detect attacks in a heterogeneous network
  - Analyzing traffic from AVTP, gPTP, and CAN protocols
  - Video streaming, synchronization and safety-critical applications
- Demonstrated using two datasets
  - Ethernet-based traffic
  - CAN-based traffic

Overview



Block diagram of our proposed IDS main components.

Politécnica UFRJ

COPPE UFRJ

uff

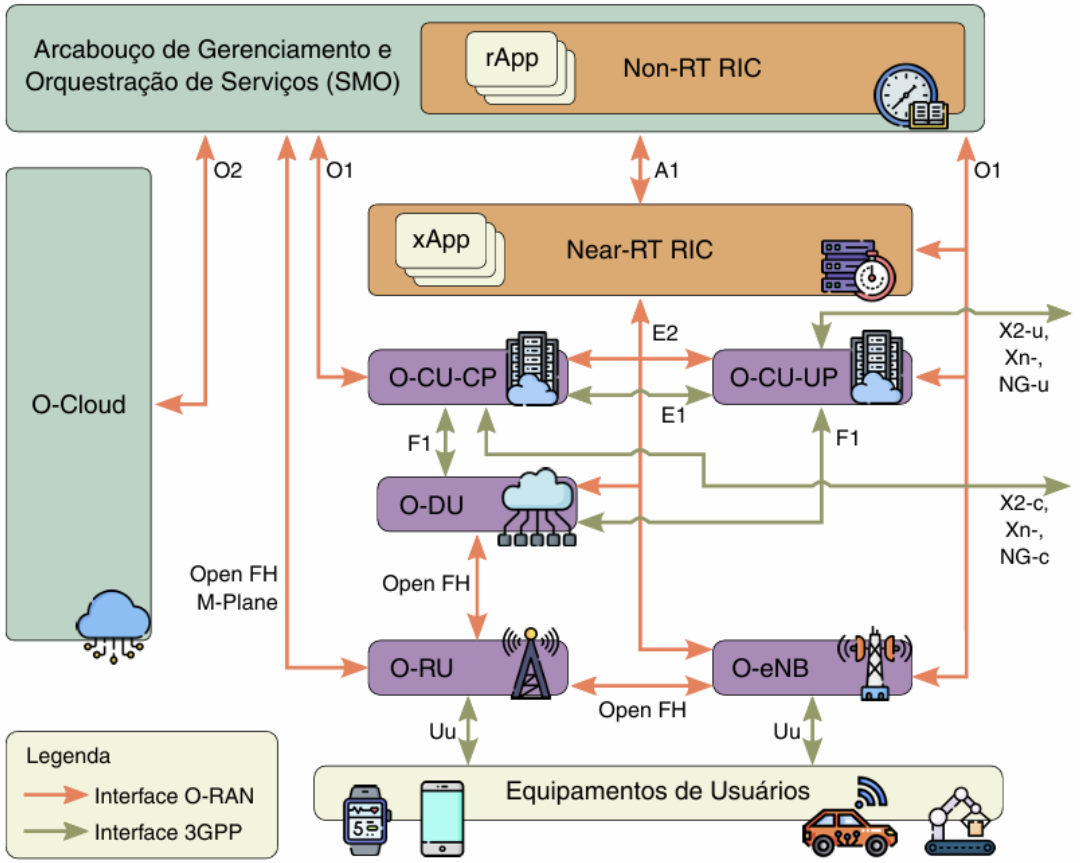
SIMULAÇÕES DE OPEN-RAN: EVOLUÇÃO EM FERRAMENTAS PARA O SIMULADOR NS-3

Felipe Táparo, Igor M. Moraes, Miguel Elias M. Campista

A ser apresentado no Salão de Ferramentas do SBRC 2025

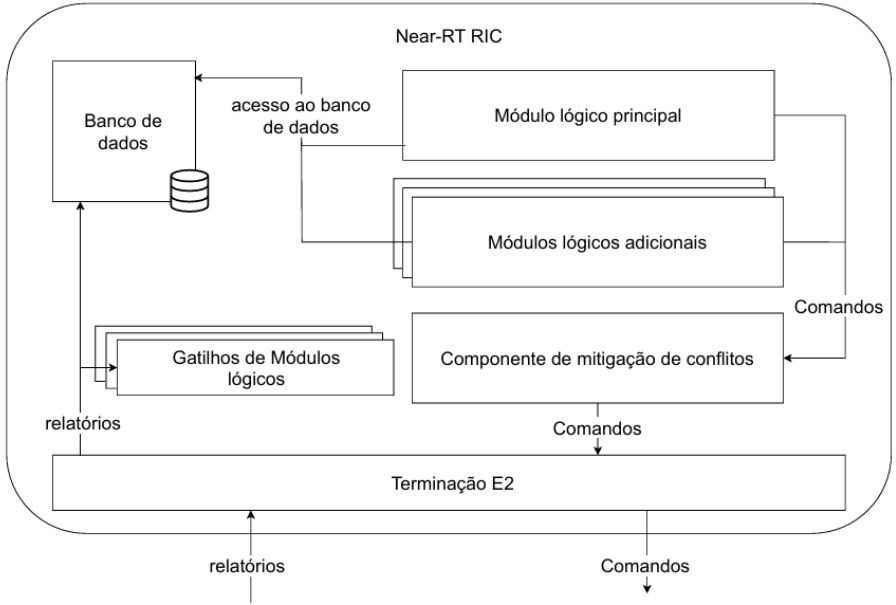
O-RAN

- Arquitetura para redes de acesso via rádio
- Componentes abertos e padronizados
- Interoperabilidade entre fabricantes
- Interfaces abertas
- Aplicações personalizadas
- Controladores inteligentes para orquestração da rede
- Virtualização



ns-3 e ns3-oran

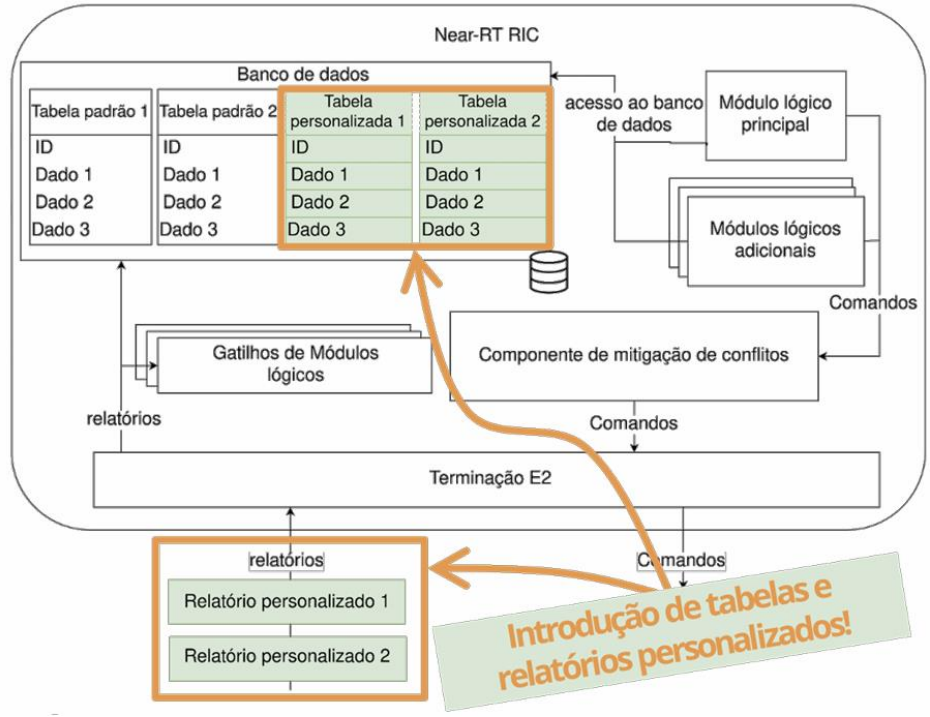
- ns-3
  - Simulador de eventos discretos para comunicações em redes
  - Código aberto
  - Funcionalidades expandidas via plugins
- ns3-oran
  - Adiciona componentes da arquitetura O-RAN no ns-3
  - Near-RT RIC para controle da rede
  - Os relatórios do ns3-oran não são personalizáveis, limitando a aplicabilidade do simulador



Arquitetura do Near-RT RIC do ns3-oran

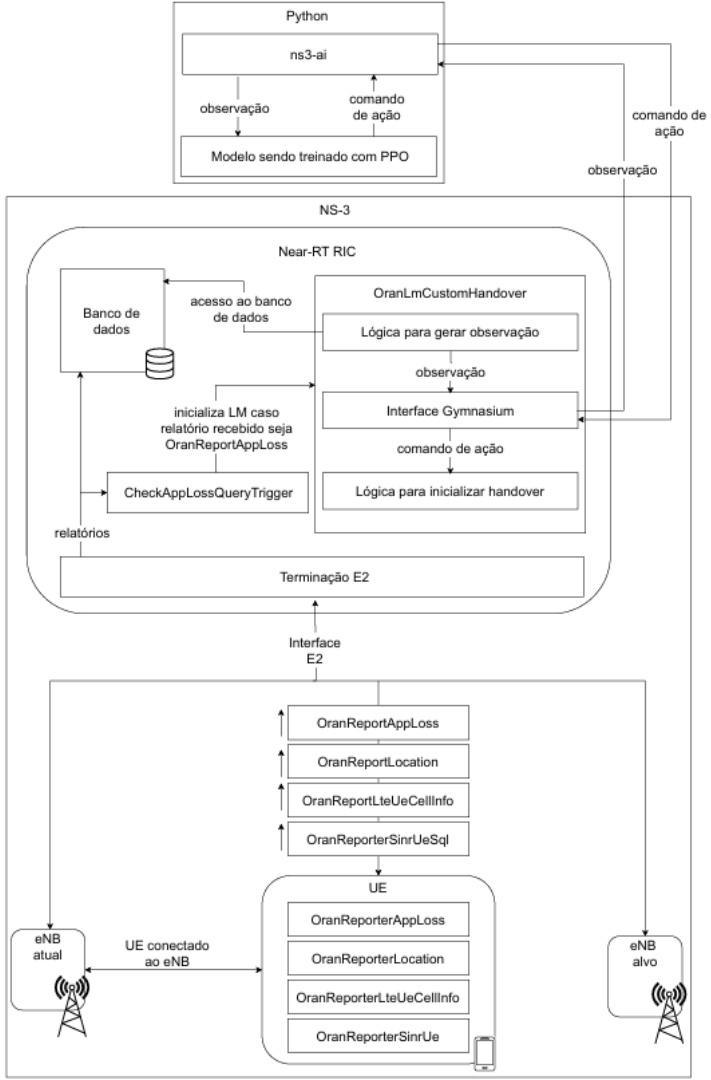
Proposta: ns3-oran-customizable-db

- Expande o ns3-oran
- Cria novo sistema de banco de dados
- Suporta relatórios personalizados definidos pelo usuário
- Cria tabelas em tempo de execução
- Permite consultas personalizadas
- Garante retrocompatibilidade com ferramenta original



Casos de Uso

- Controle e orquestração da rede com base em dados arbitrários
- Novo sistema permite treinamento e testagem de aplicações de aprendizado de máquina com métricas definidas pelo usuário
- Exemplo disponível ilustrando aplicação de aprendizado por reforço para gerenciamento de *handover*



Linha Temática: **Redes Veiculares**

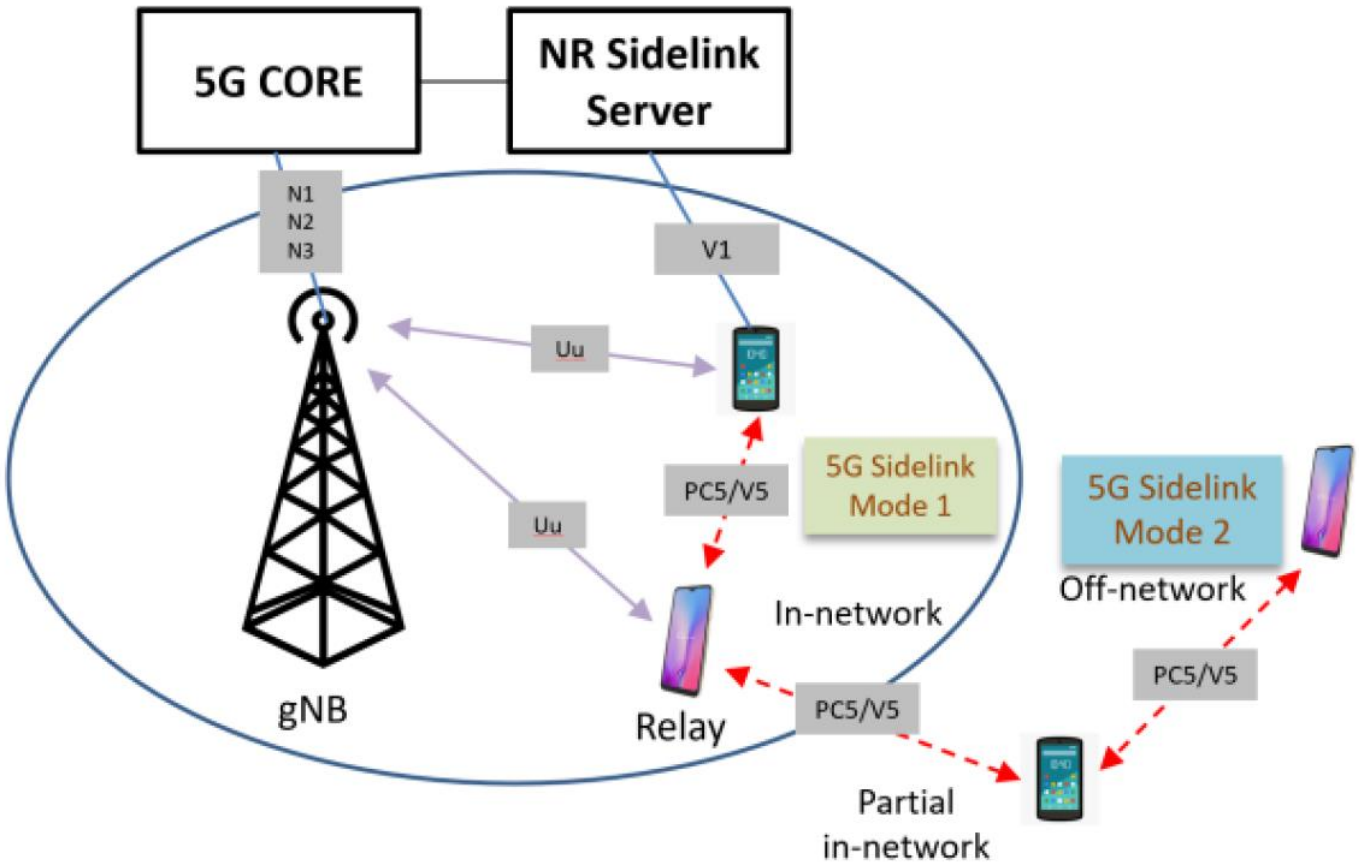
Requisitos das Redes Veiculares

- **Operação Independente de Infraestrutura**: os veículos devem se comunicar diretamente entre si (veículo a veículo – V2V), ou entre veículos e outros elementos, como semáforos e pedestres, mesmo sem depender da infraestrutura da rede celular (como torres de telefonia). Isso torna a comunicação mais robusta, especialmente em áreas onde a cobertura da rede pode ser limitada ou em locais remotos.
- **Eficiência em Redes Densas**: deve ser fornecido meios para redução de congestionamento **de rede** em áreas urbanas com alta densidade de veículos.
- **Baixa Latência**: deve ser fornecido baixa latência para que a rede opere em situações críticas, como evitar colisões, pois a resposta imediata entre os veículos pode ser a diferença entre um acidente e uma condução segura.

Redes Veiculares Usando 5G Sidelink Mode 2

•**5G Sidelink Mode2 oferece:**

- •**Operação Independente de Infraestrutura:** Comunicação direta entre veículos (V2V) e entre veículos e infraestrutura (V2I), sem depender da rede centralizada.
- •**Baixa Latência:** Comunicação rápida e em tempo real para evitar acidentes e melhorar a segurança.
- •**Eficiência em Ambientes Densos:** Redução de congestionamento de rede em áreas urbanas com alta densidade de veículos.



Desafios para Redes Veiculares Usando 5G Sidelink Mode 2

Proposta

Este projeto visa desenvolver e disponibilizar um módulo para o simulador NS-3 que implemente a comunicação D2D via Sidelink Mode 2.

Questions?

Thanks !!!

Results and Discussion

TOW-IDS dataset detection metrics comparison

Model	AUCROC	Accuracy	Precision	Recall	F1-Score
CAE [2]	**0.99666**	0.96862	0.96648	**0.99941**	0.98267
LSTMAE [2]	0.97784	0.95907	0.98682	0.96694	0.97678
SeqWatch	0.99310	**0.98484**	**0.99318**	0.98977	**0.99147**

SAD dataset detection metrics comparison

Model	AUCROC	Accuracy	Precision	Recall	F1-Score
CAE [2]	0.98775	0.95013	0.96164	0.95552	0.95857
LSTMAE [2]	0.96932	0.91497	0.93088	0.92806	0.92947
SeqWatch	**0.99832**	**0.98651**	**0.98314**	**0.99471**	**0.98889**

[2] Alkhatib, N., Mushtaq, M., Ghauch, H., and Danger, J.-L. (2022). Unsupervised network intrusion detection system for AVTP in automotive ethernet networks.

Results and Discussion

Each attack detection scenario for the TOW-IDS dataset

Model	Normal	Attack	Frame injection	PTP sync	CAN replay	MAC flooding	CAN DoS
CAE [2]	0.71862	0.96954	0.95171	0.85035	0.82313	0.82254	0.87144
LSTMAE [2]	0.89519	0.91078	0.97647	0.94426	0.89946	0.93385	0.87065
SeqWatch	**0.94486**	**0.98616**	**0.97945**	**0.97068**	**0.96091**	**0.96523**	**0.97020**

Each attack detection scenario for the SAD dataset

Model	Normal	Attack	Replay	Malfunction
CAE [2]	0.94193	0.95552	0.94509	0.95058
LSTMAE [2]	0.89502	0.92806	0.92448	0.89382
SeqWatch	**0.97401**	**0.99471**	**0.98207**	**0.98387**

[2] Alkhatib, N., Mushtaq, M., Ghauch, H., and Danger, J.-L. (2022). Unsupervised network intrusion detection system for AVTP in automotive ethernet networks.