



PUC Minas

# **“MITM ATTACK DETECTION SCHEME USING MONITORING INFORMATION IN V2X COMMUNICATION”**

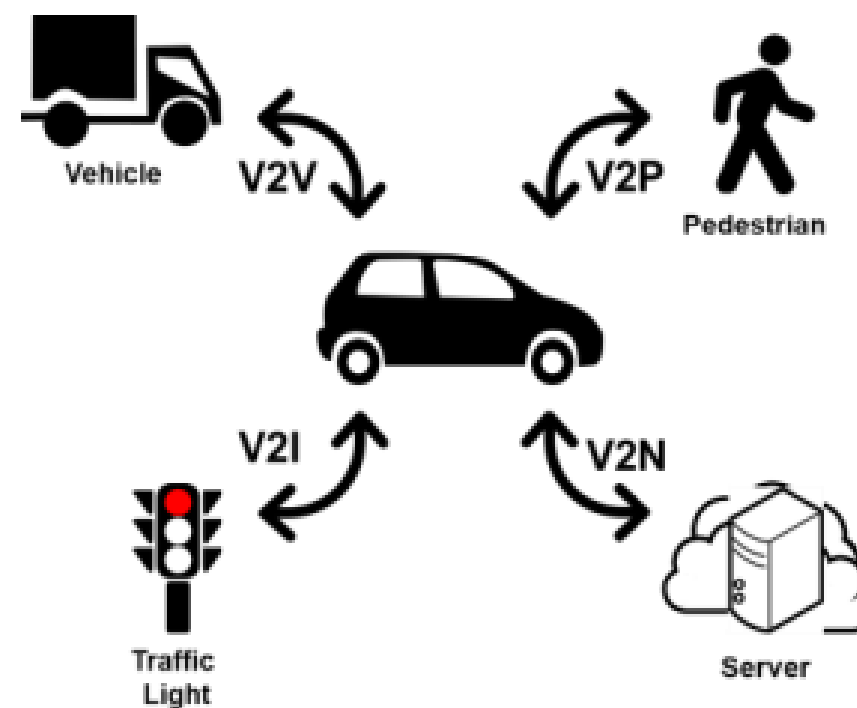
Wonjin Chung, Jungsub Ahn, Taeho Cho

Ana Fernanda  
Arthur Matos  
Gabriel Praes  
Guilherme Otávio  
Júlia Pinheiro  
Vitória Araújo



# CONCEITOS BÁSICOS

- **V2X (Vehicle-to-Everything):** Comunicação entre veículos e diferentes elementos do ambiente



- **Lógica Temporal:** sintaxe para especificações que descrevem como o comportamento de um sistema evolui ao longo do tempo

O (next) → próximo momento no tempo

◇ (someday) → algum momento no futuro

□ (always) → todos os momentos futuros

U (until) → “até” um determinado ponto no tempo

# CONCEITOS BÁSICOS


**Ataques Man-in-the-Middle (MiTM):** Ataque em que o invasor atrasa, modifica ou descarta uma conversa entre dois alvos. (veículos e infraestrutura )



- **BM-DEVS:** Modelo para monitorar comportamento de sistemas com regras formais
- **Trust Model:** Método para avaliar confiabilidade de veículos com base em interações
- **BSM (Basic Safety Message):** Mensagens trocadas para coordenar manobras entre veículos.

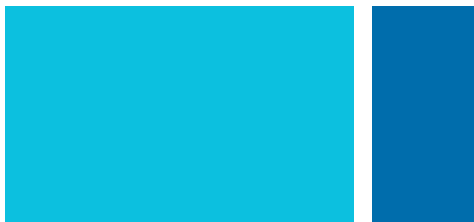


# PROBLEMA

- MiTM Attacks modificam ou bloqueiam mensagens em V2X e em certas situações, tornam-se difíceis de detectar pelos esquemas de segurança existentes.
  - Ataques podem causar decisões erradas por veículos autônomos.
  - Métodos existentes falham em detectar ataques em alguns cenários específicos.
- 




# MOTIVAÇÃO

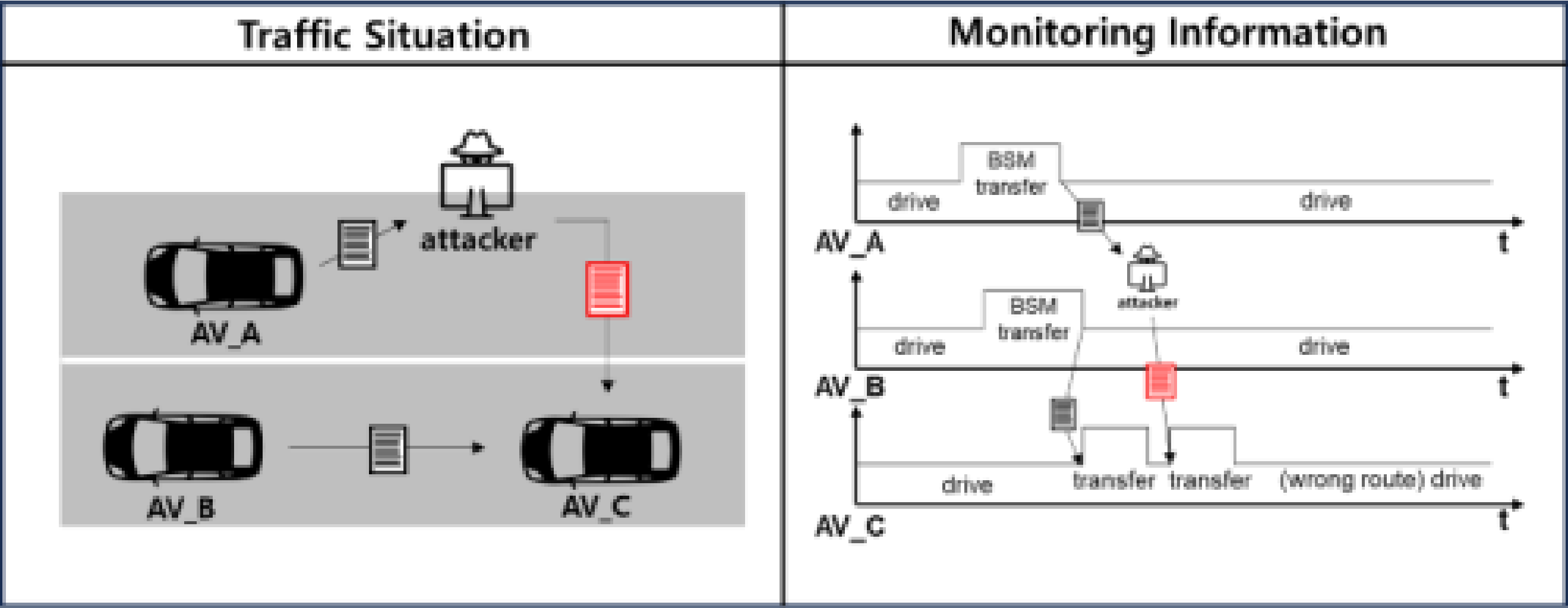
- Garantir a integridade das mensagens trocadas entre veículos.
  - Aumentar a segurança viária em ambientes com veículos autônomos.
  - Reduzir danos (prejuízos materiais e perda de tempo) causados quando os veículos recebem mensagens incorretas.
  - Melhorar a eficácia de detecção de ataques em situações diversas.
- 



# OBJETIVO

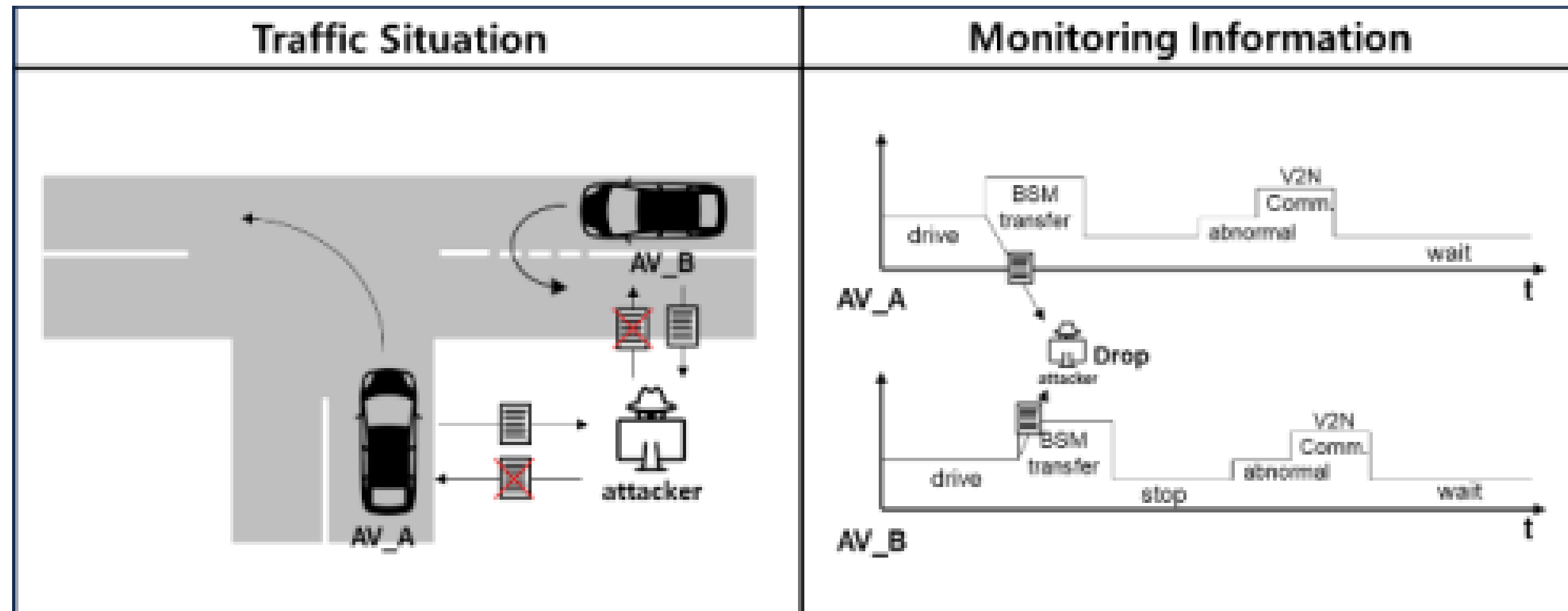
- Propor um esquema de segurança que detecta ataques MiTM com base no monitoramento do ambiente ao redor dos veículos que demonstram comportamento anormal
  - BM-DEVS para analisar o trajeto e ações do veículo.
  - Aumentar a taxa de detecção de ataques em comparação com modelos existentes.
- 

# MODELO



A. Ataque de Modificação de Mensagem

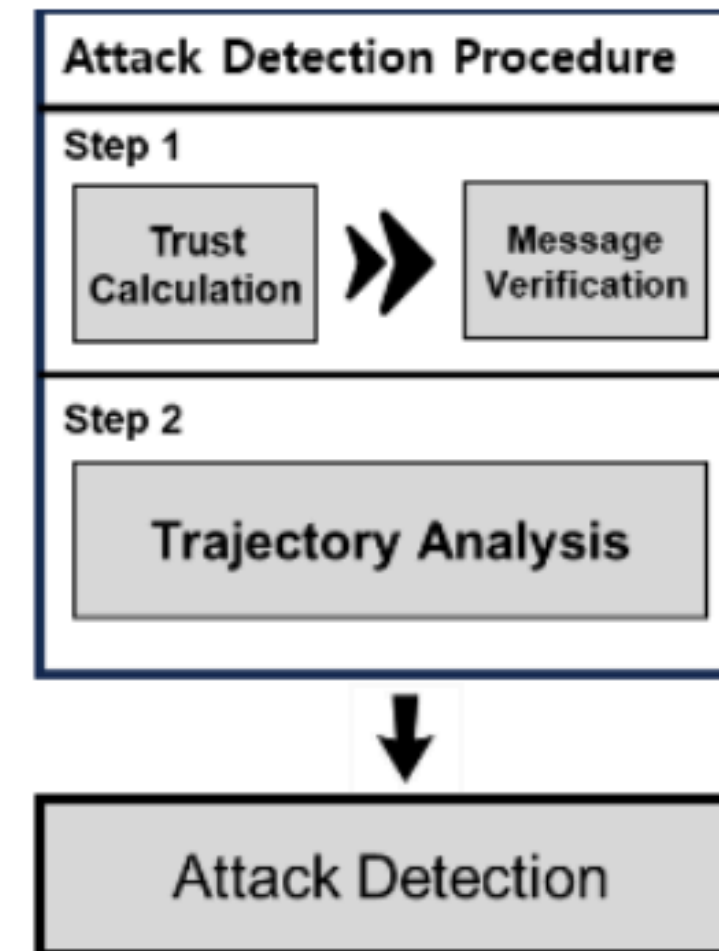
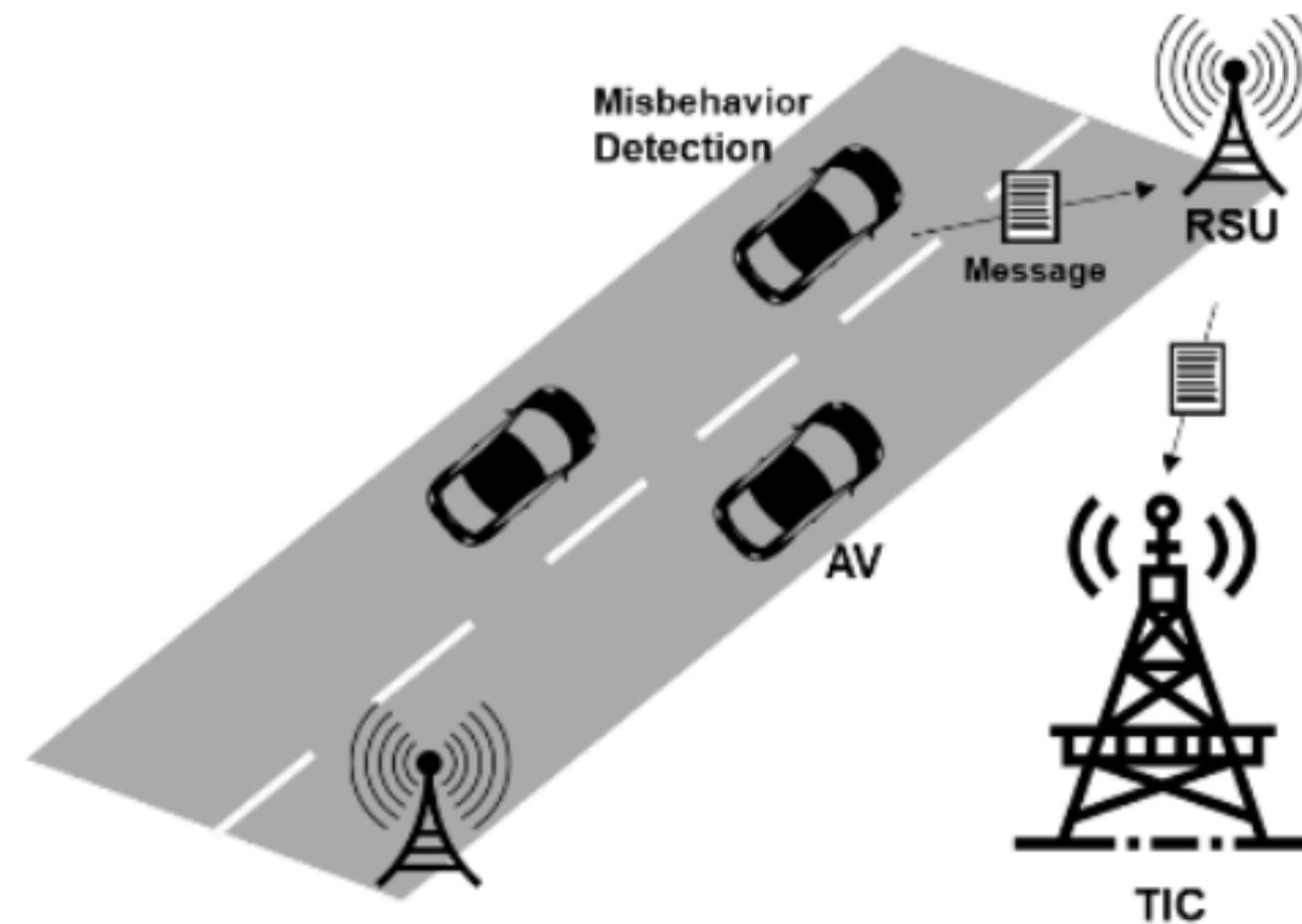
# MODELO



## B. Ataque de Descarte de Mensagem



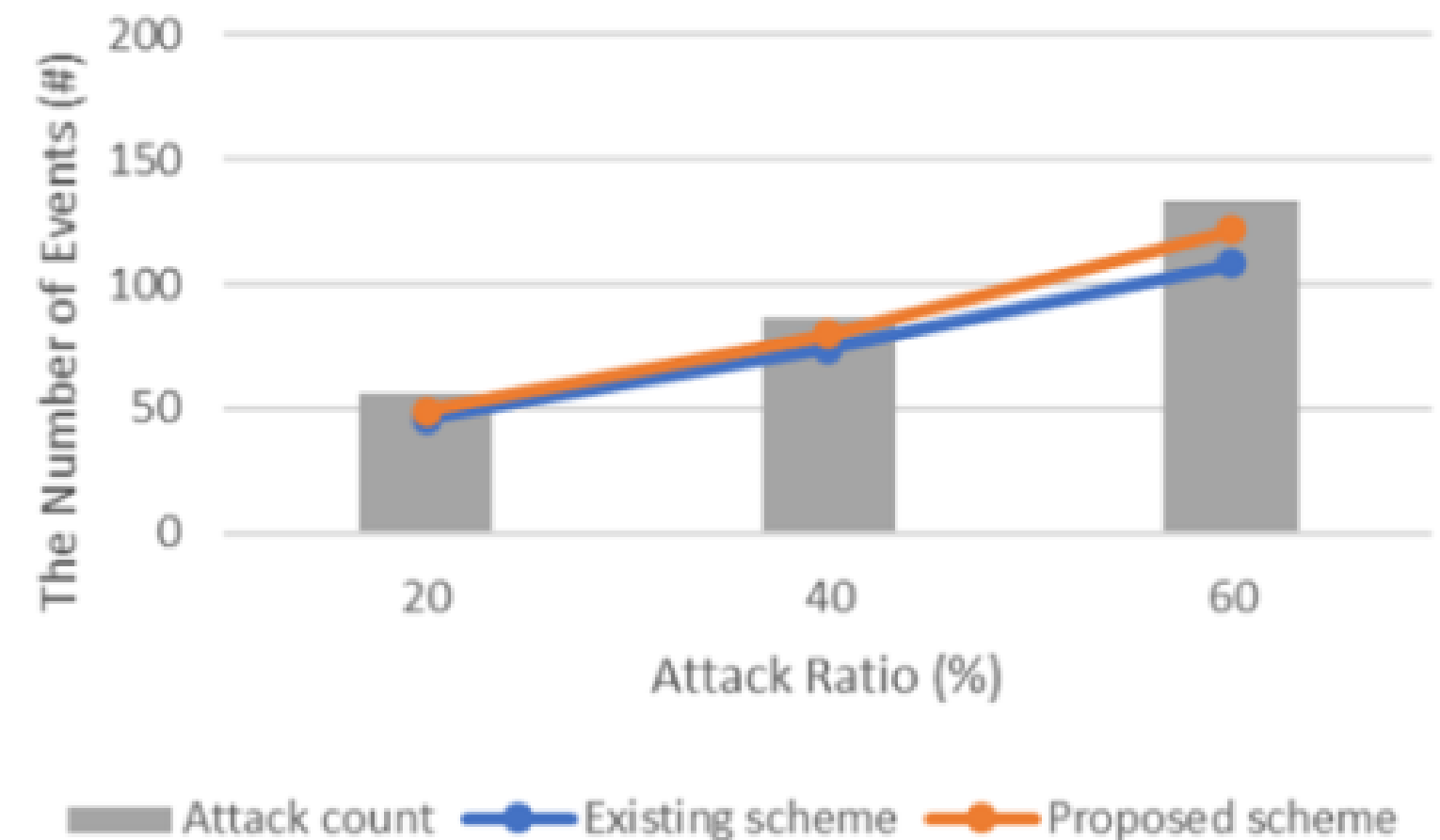
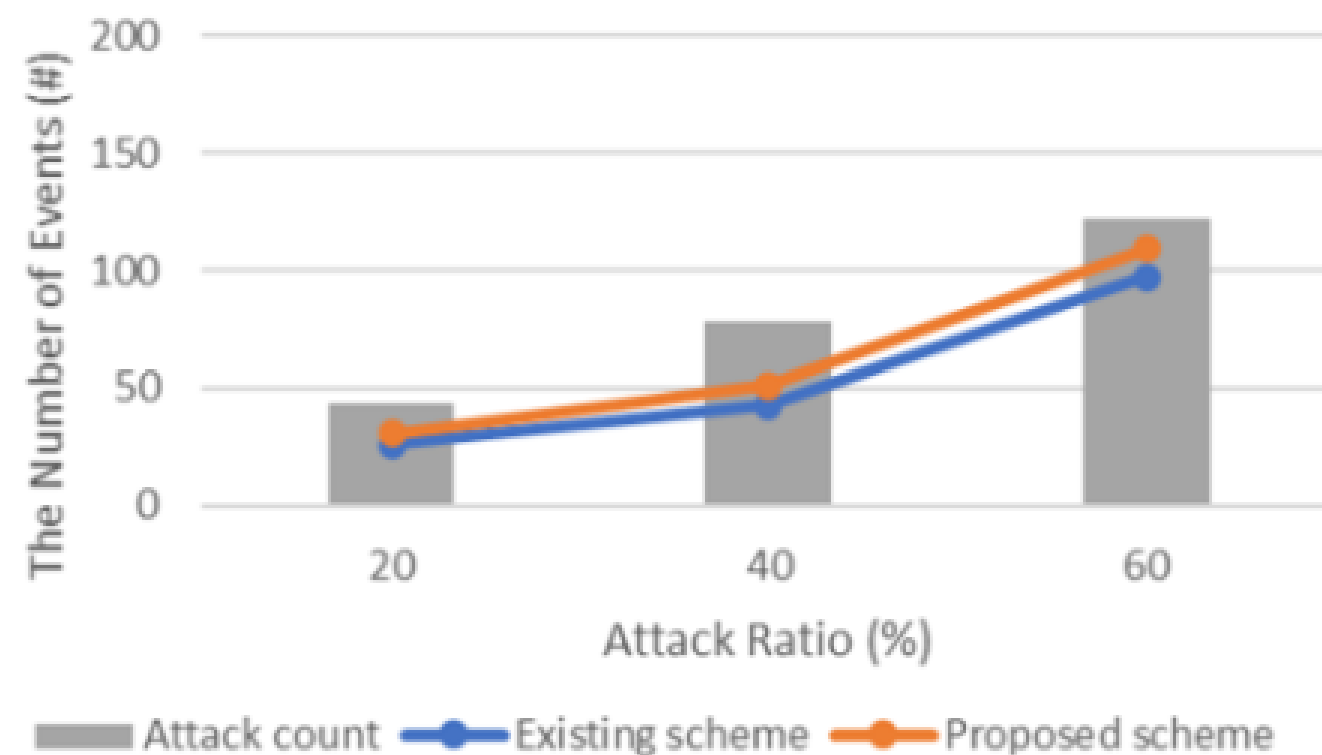
# MODELO



## C. Mecanismo do Esquema Proposto

# RESULTADOS

- Simulações realizadas com 5 veículos autônomos em ambiente ITS (sistemas de transporte inteligente)




Melhoria detecção ataques de modificação: +9,84%

Melhoria detecção de ataques de descarte: +10,45%




# CONCLUSÕES

- **Importância do ITS para Cidades Inteligentes:** Sistemas de Transporte Inteligente (ITS) são essenciais para melhorar a mobilidade urbana e a qualidade de vida dos motoristas.
  - **Eficácia:** Novo método demonstrou uma melhoria na detecção de ataques MiTM em comparação com esquemas baseados em modelos de confiança já existentes.
  - **Impacto:** Reduz riscos de acidentes e congestionamentos causados por mensagens falsificadas ou perdidas, aumentando a segurança e eficiência de veículos autônomos
- 




# CONCLUSÕES (ALUNOS)

- Por mais que uma melhora média de 10% seja um número relativamente pequeno, é significativo tratando-se de evitar acidentes de trânsito
  - Observar comportamentos para detectá-los e preveni-los é um passo grande nos sistemas de segurança de cidades inteligentes
  - Contribui para que possamos ter mais veículos autônomos circulando de forma segura
- 



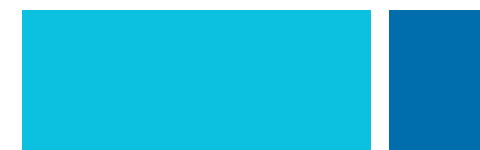
# TRABALHOS FUTUROS PROPOSTOS

- Desenvolver estratégias para detecção simultânea de múltiplos tipos de ataques e analisar situações em que essa detecção falha
  - Adaptar e otimizar o esquema de segurança para diversos cenários de tráfego
  - Aprimorar a robustez do modelo contra ataques combinados
- 



# **TRABALHOS FUTUROS PROPOSTOS (ALUNOS)**

- Desenvolver mecanismos de resposta automática quando ataques são detectados, não apenas identificando-os
- Avaliar o impacto do aumento do número de veículos na eficácia do sistema de detecção





PUC Minas

**OBRIGADO!**