



UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

Avaliação de Ataques de Spoofing em Percepção Cooperativa Usando o TUMTraf DevKit

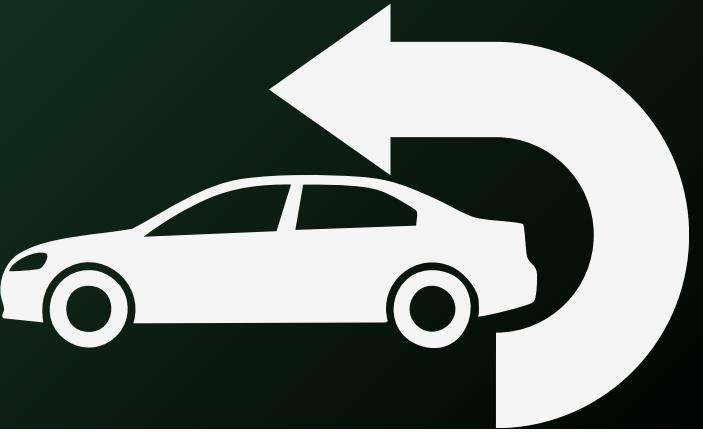
ALUNO:
CARLOS EDUARDO DE SOUSA

PROFESSOR:
JOÃO PAULO JAVIDI DA COSTA

2025

1

AGENDA



- Motivação
- Contribuições
- Arquitetura do experimento
- Ataques implementados
- Métricas e Resultados
- Conclusão
- Demonstração (vídeos)

Motivação



Dados
compartilhados por
múltiplos agentes
(veículos +
infraestrutura)

Vulnerável a
adulterações
nas
mensagens,
sensores ou
anotações

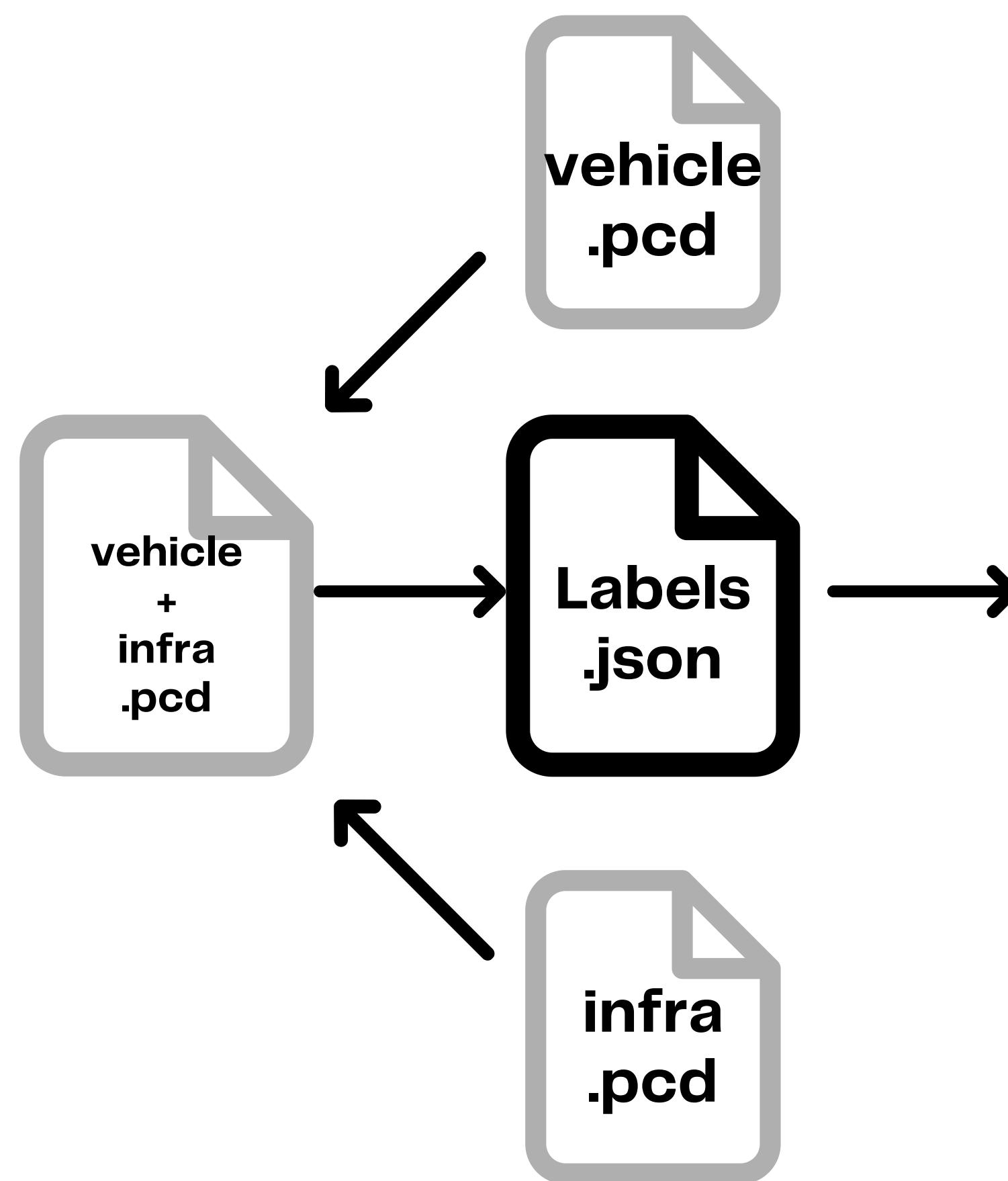
O dataset
TUMTraf oferece
dados
registrados de
múltiplos LiDARs,
mas não avalia
resiliência a
ataques

**Como ataques simples nas anotações podem
deformar a percepção cooperativa e comprometer a
segurança?**

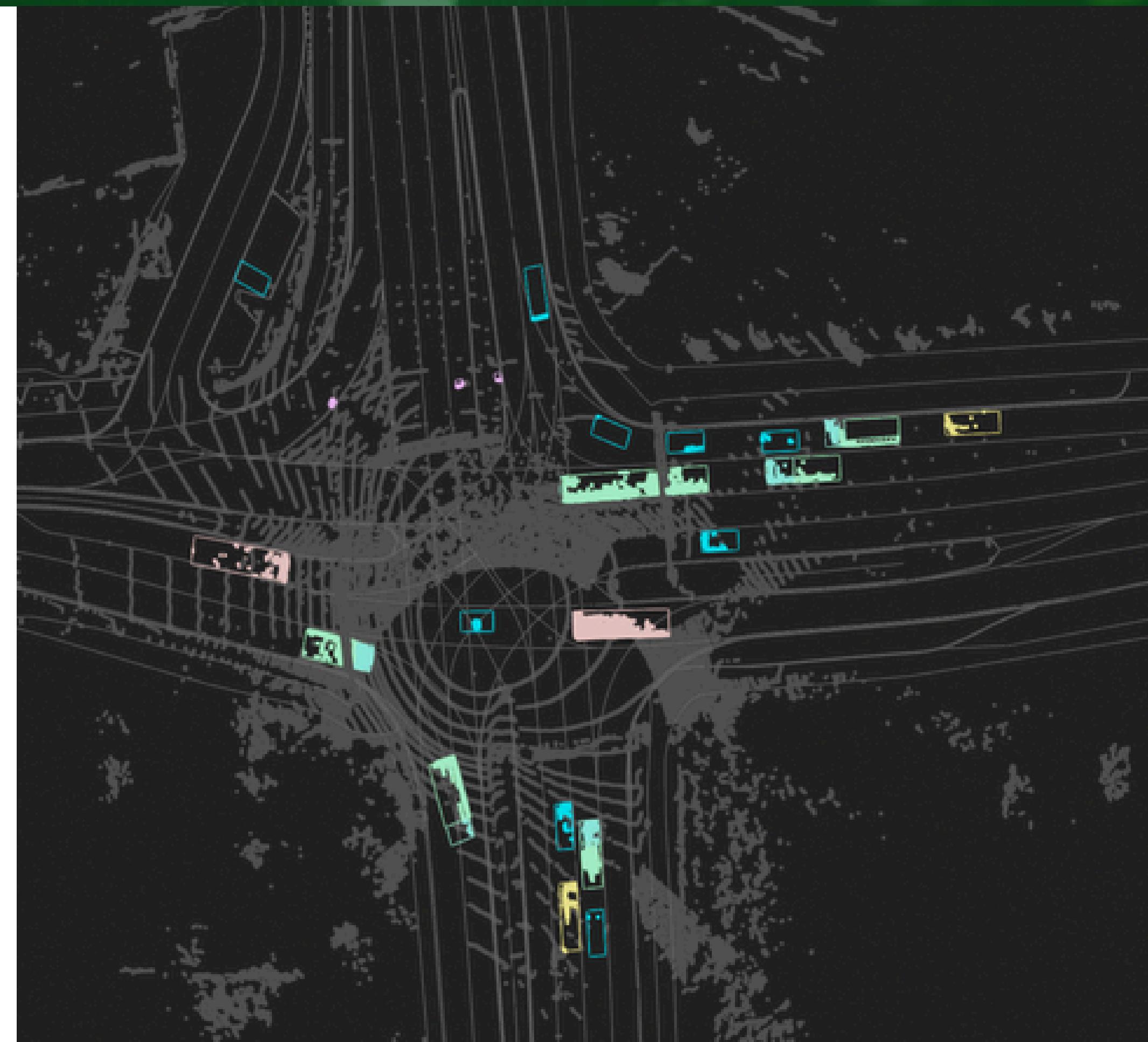
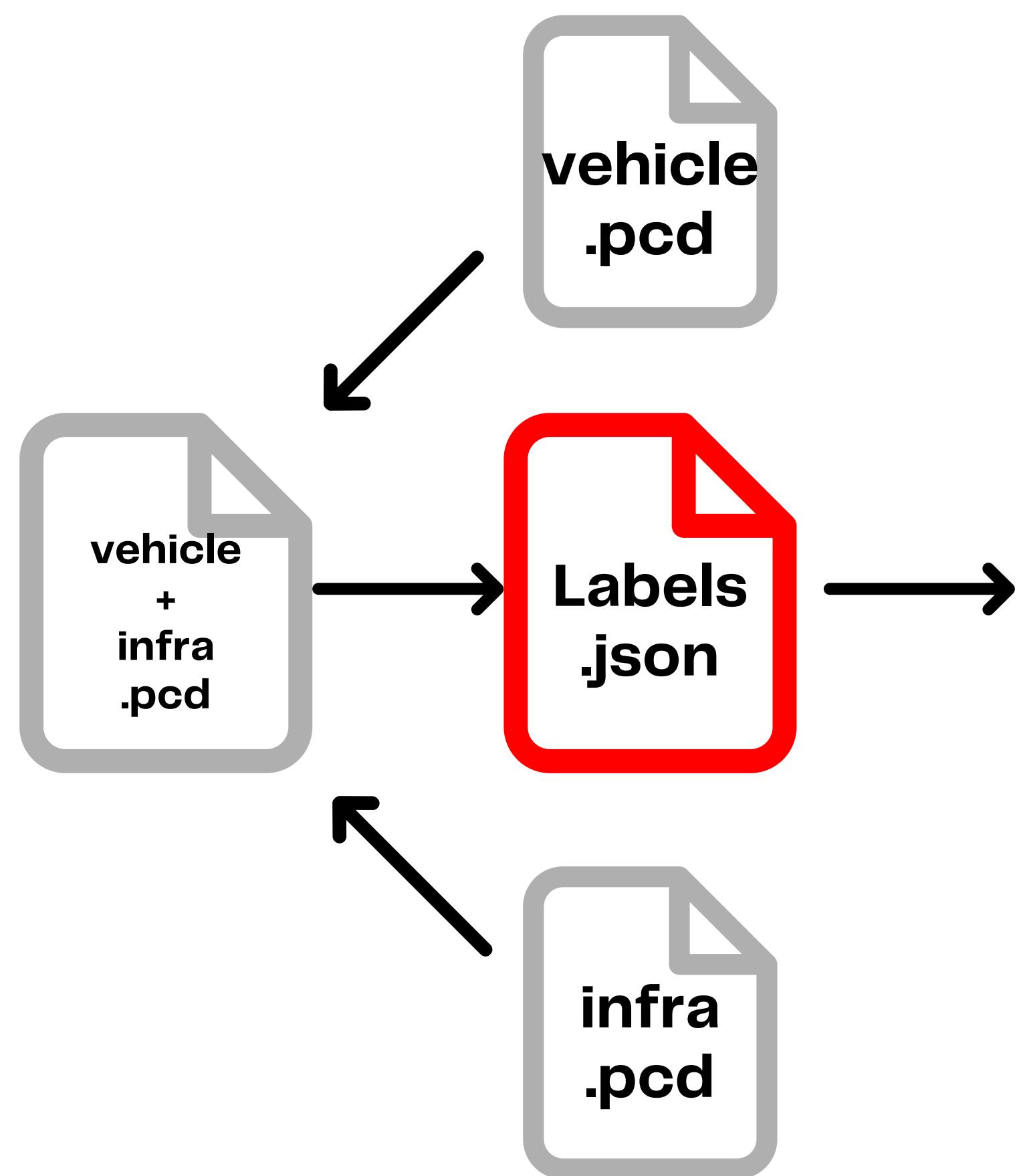
Contribuições

- Três ataques implementados no **TUMTraf-V2X Mini**.
- Dataset automaticamente modificado frame a frame.
- Métricas objetivas de distorção da percepção.
- 400 frames analisados por ataque.
- Spoofing annotation-level já compromete a percepção cooperativa.

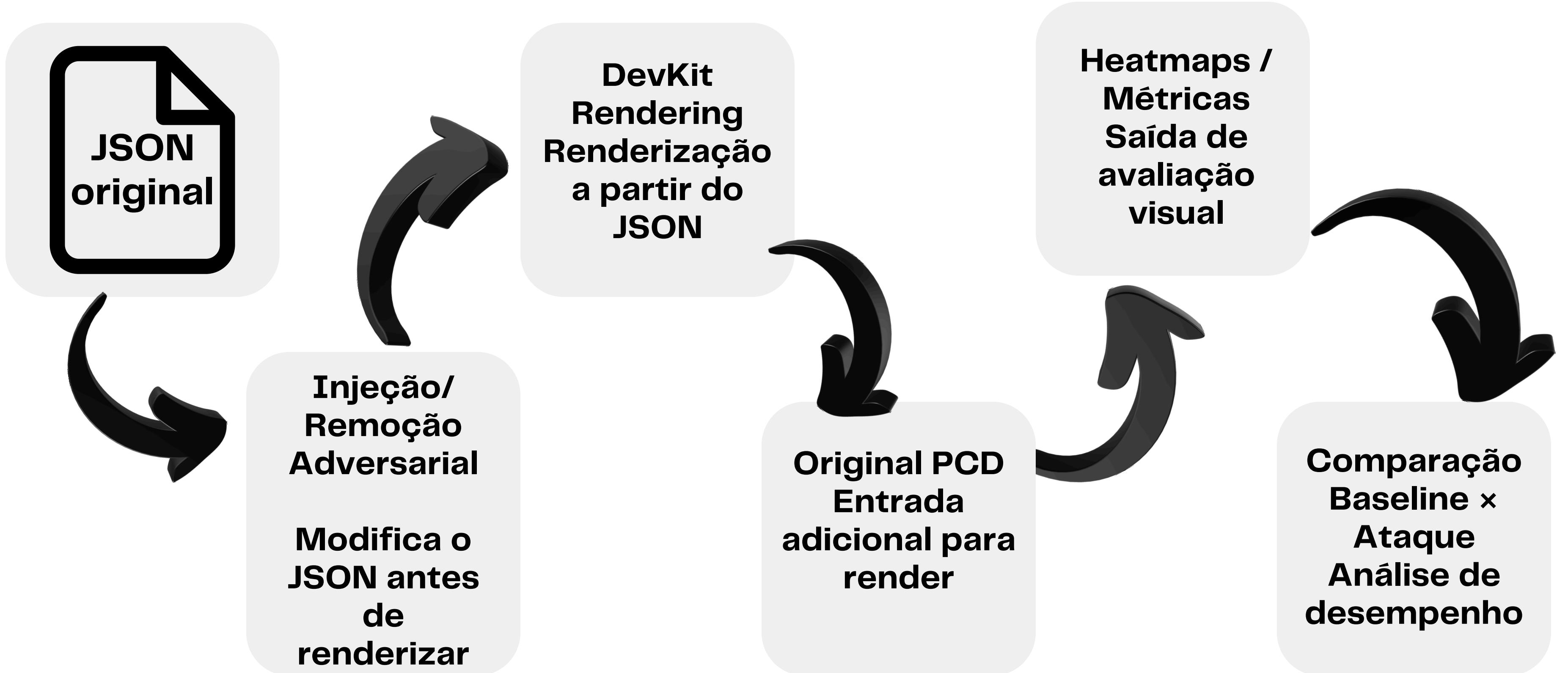
Arquitetura do experimento - Fusão de Percepção no TUMTraf



Arquitetura do experimento - Fusão de Percepção no TUMTraf



Arquitetura do experimento



Ataques implementados - Ataque 1: Phantom Injection (PHANTOM)

Objetivo:

Criar falsos positivos consistentes na cena, injetando objetos inexistentes.

Pseudocódigo:

```
for i in range(n_phantoms):
    x, y ← região à frente
    yaw ← aleatório
    cuboid ← [x, y, z, qx, qy, qz, qw, l, w, h]
    objects[uuid()] = { type: "PHANTOM", cuboid:cuboid }
```

Observação: Os objetos são válidos geometricamente, mas inexistentes fisicamente.

Ataques implementados - Ataque 1: Phantom Injection (PHANTOM)



Ataques implementados - Ataque 2: Random Removal

Objetivo:

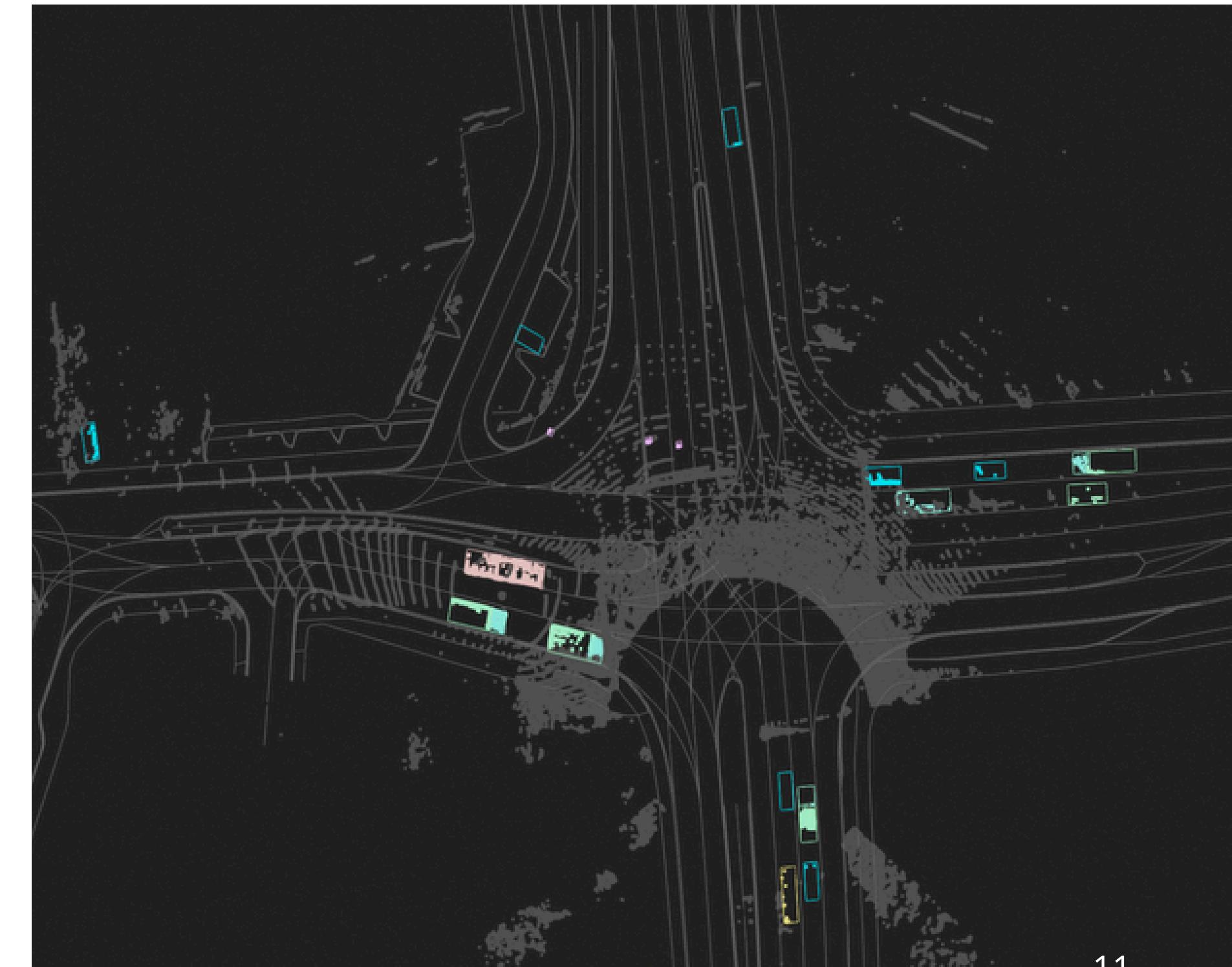
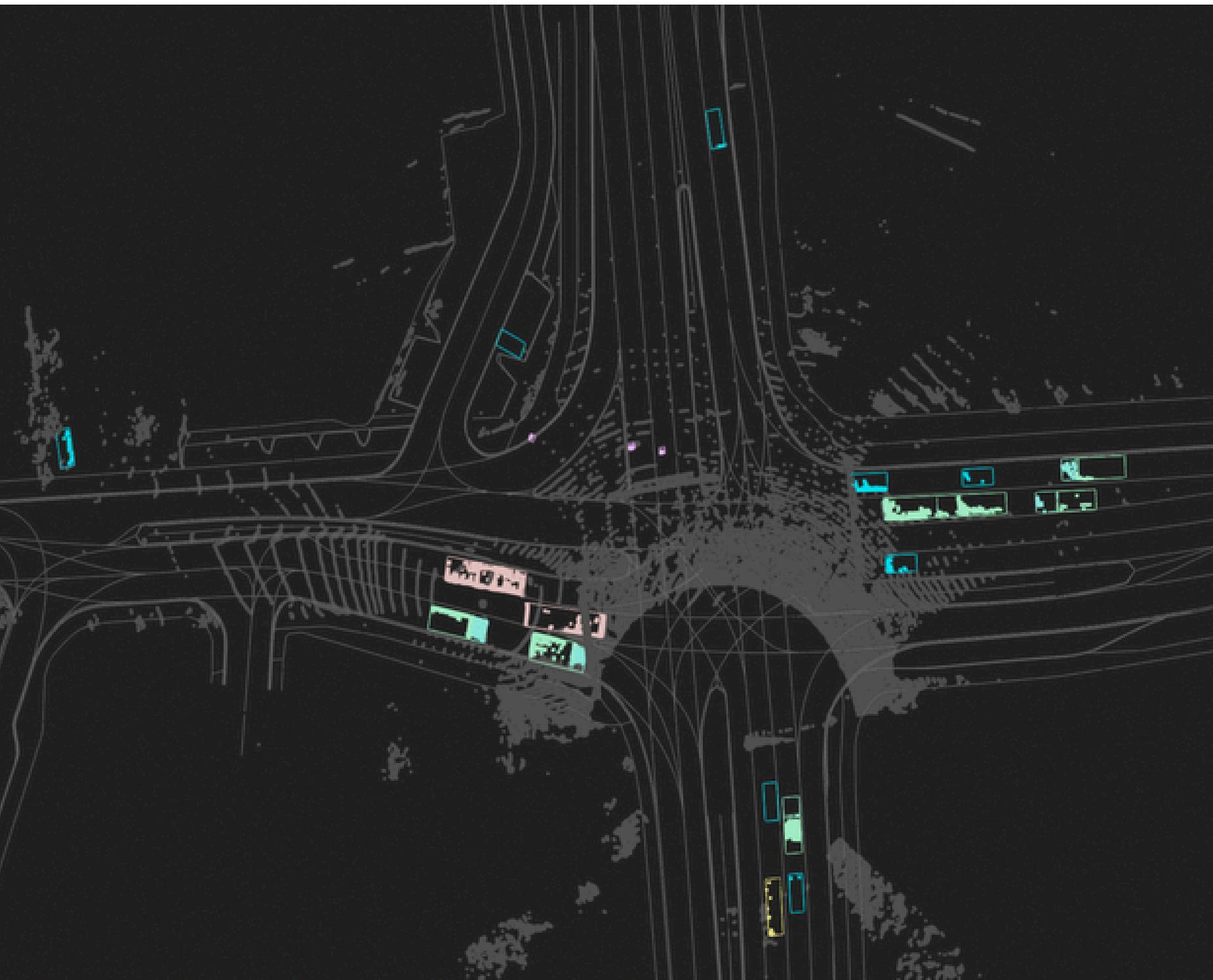
Simular a perda imprevisível de detecções, representando falhas esporádicas ou ruído.

Pseudocódigo:

```
k ← aleatório entre 1 e 10  
ids_remove ← escolher k objetos válidos  
remover objects[ids_remove]
```

Impacto Esperado: Efeito difuso e não sistemático, resultando em uma pequena, porém distribuída, distorção global na percepção.

Ataques implementados - Ataque 2: Random Removal



Ataques implementados - Ataque 3: ROI Removal

Objetivo:

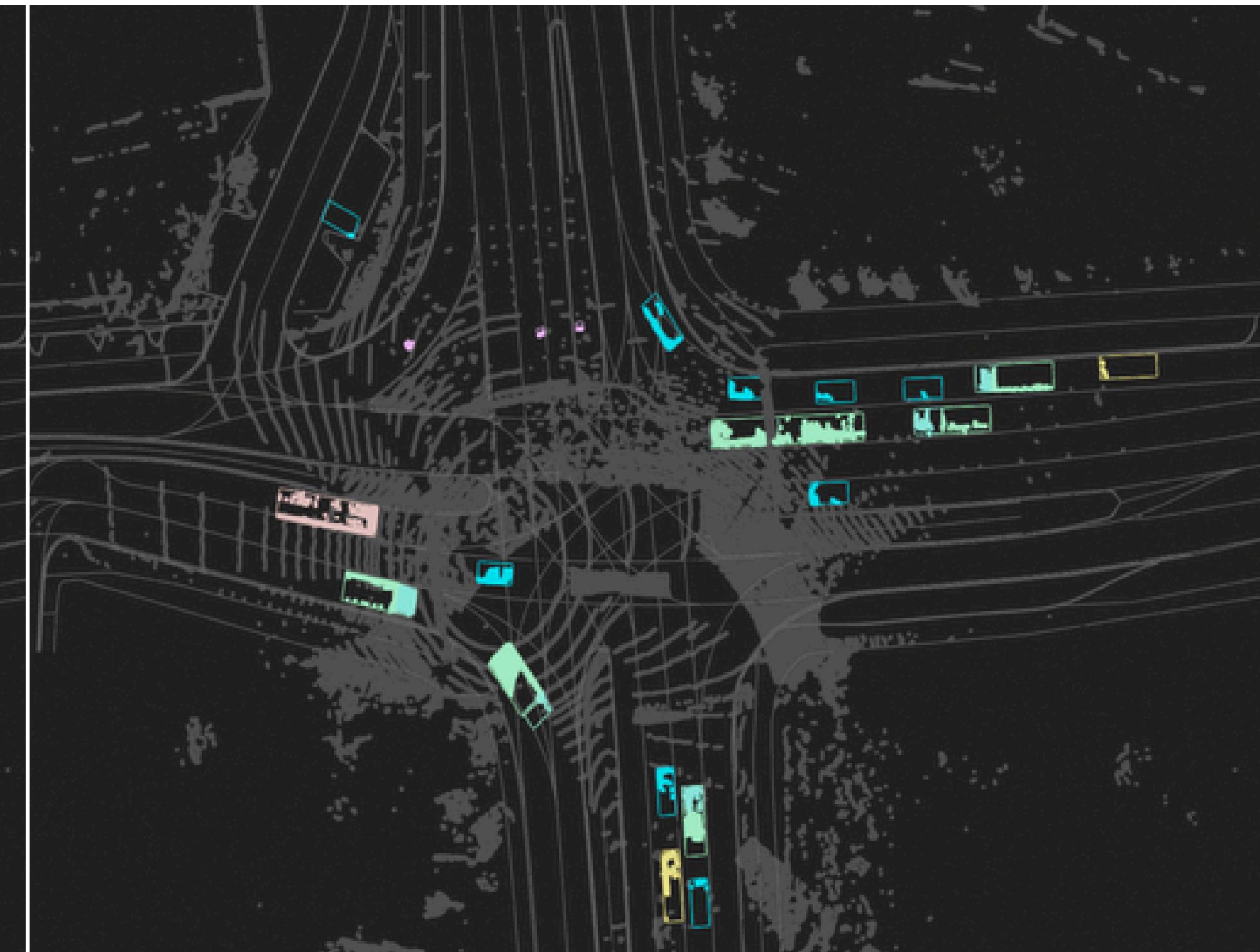
Apagar alvos em regiões críticas da cena, criando pontos cegos deliberados.

Pseudocódigo:

```
for obj in objects:  
    if dentro_da_ROI(obj.xy):  
        remover(obj)
```

Impacto Esperado: Criação de um blindspot forte e sistemático, onde veículos ou outros objetos importantes desaparecem em uma região específica.

Ataques implementados - Ataque 3: ROI Removal



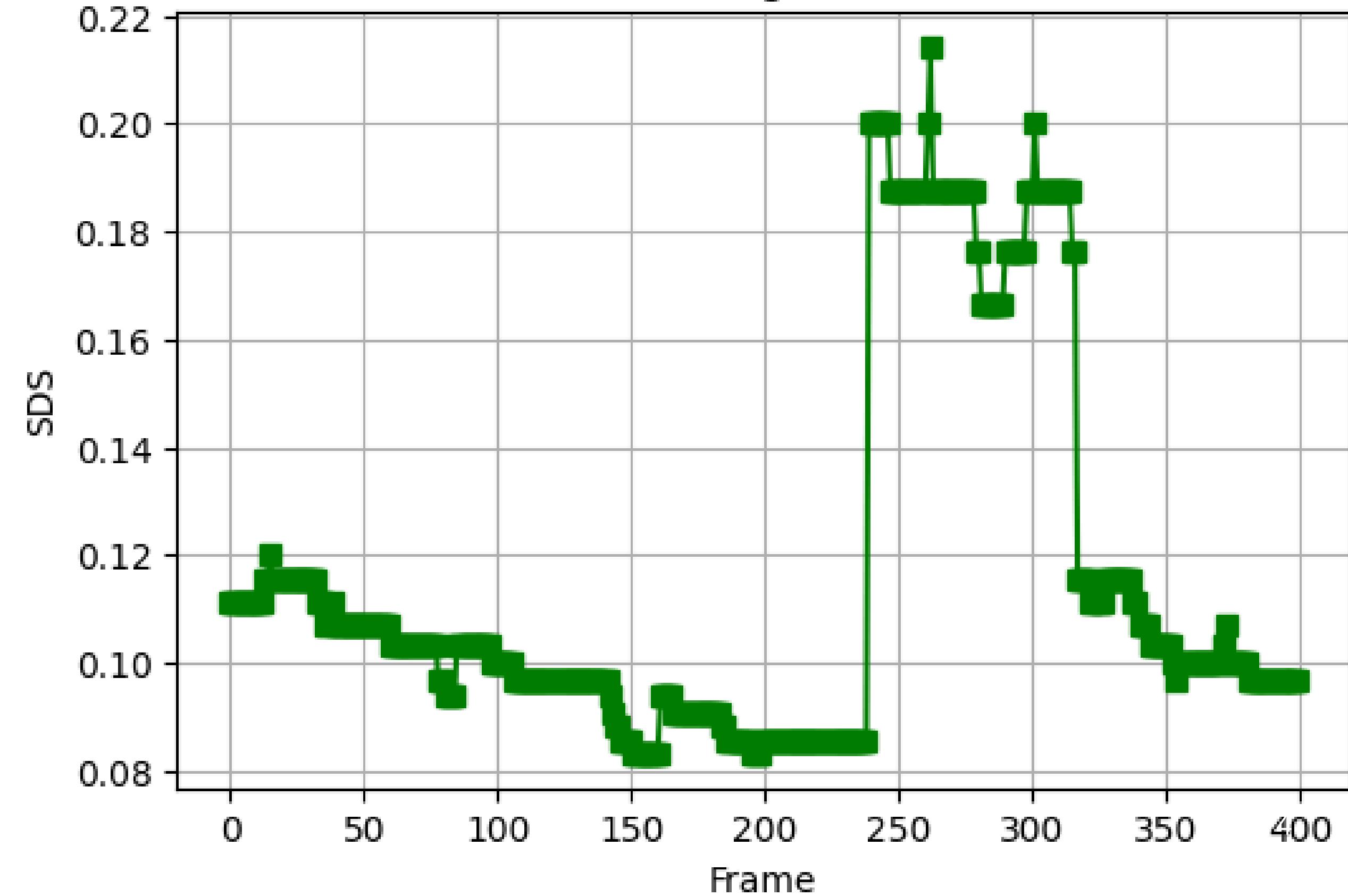


Métricas e Resultados

BASELINE X PHANTOM

$$SDS = |n_{\text{spoof}} - n_{\text{base}}| / n_{\text{base}}$$

Scene Divergence Score

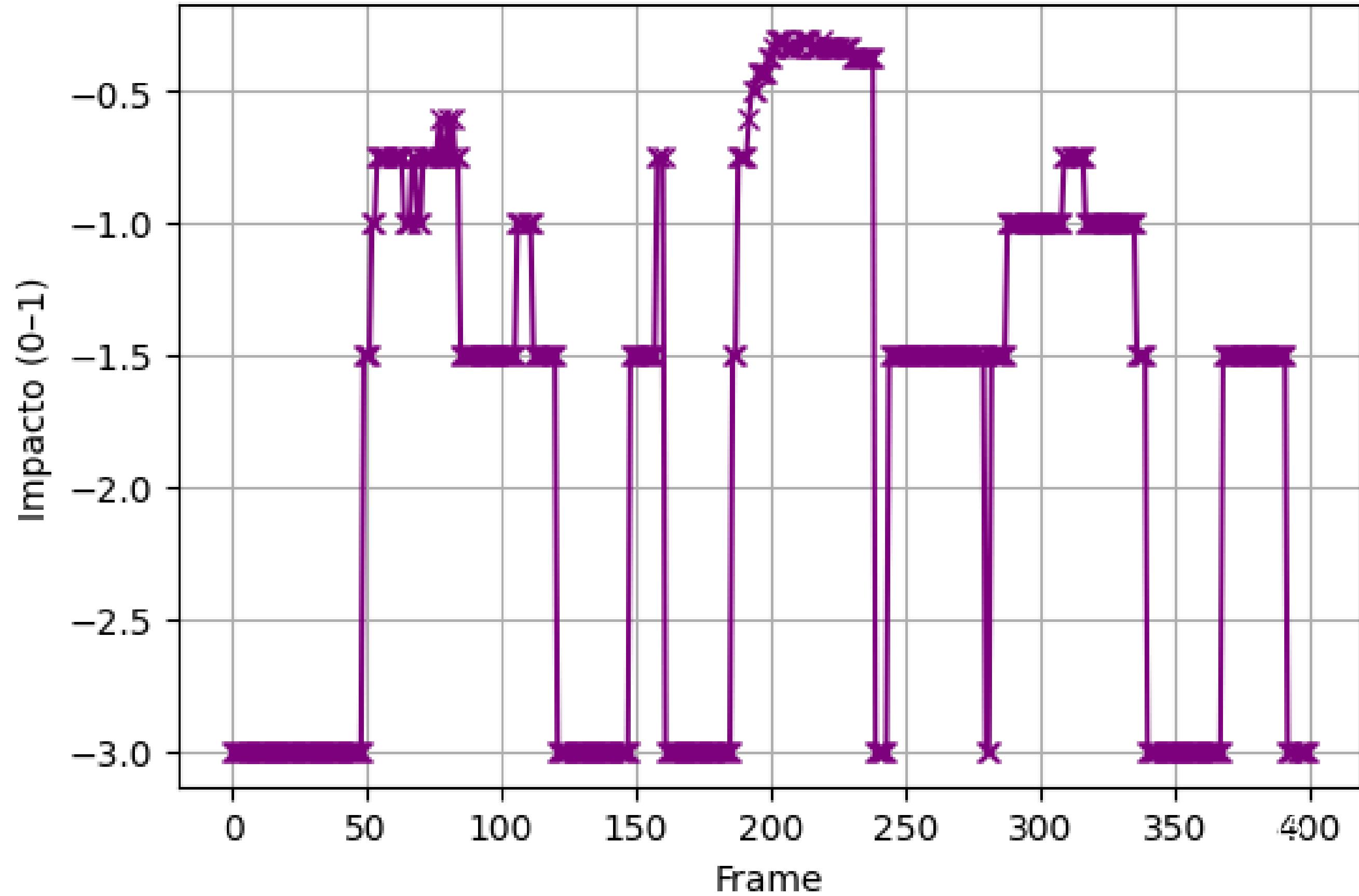




Métricas e Resultados

ROI Impact Score

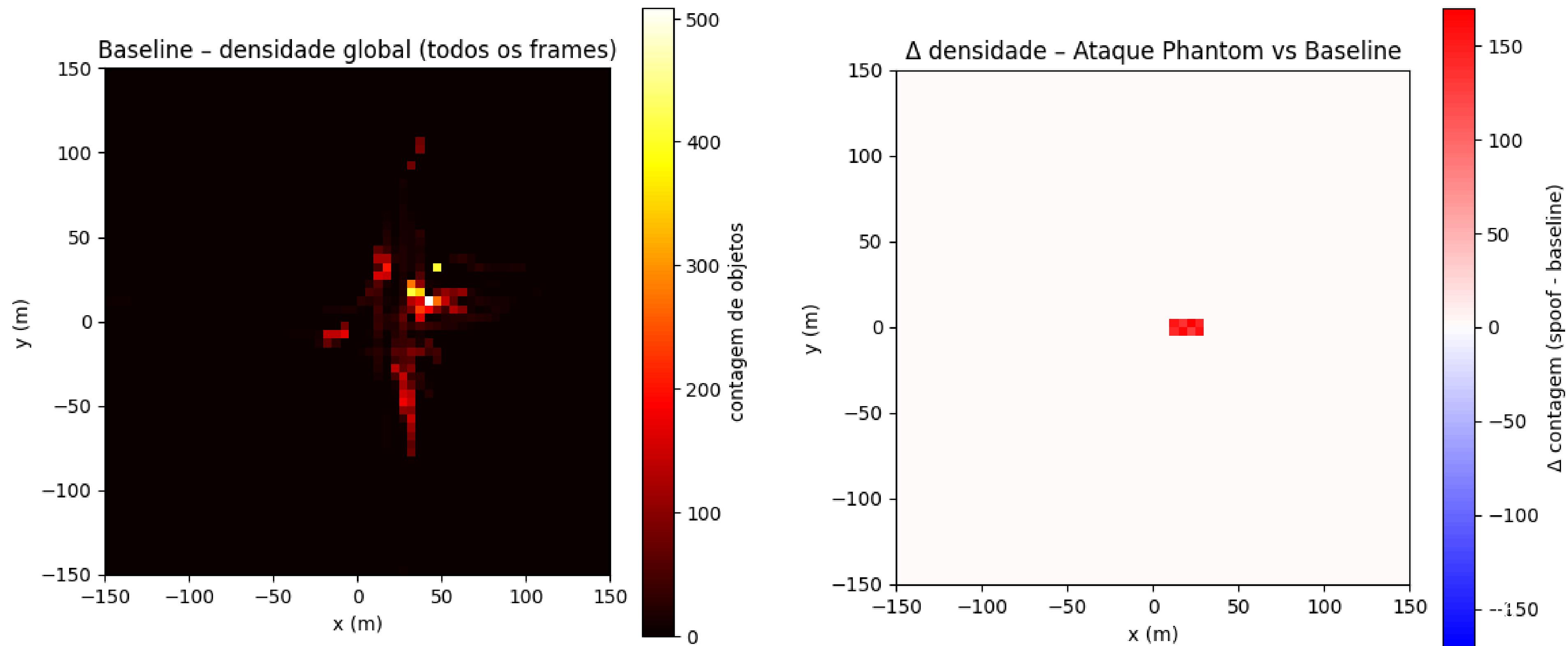
BASELINE X PHANTOM





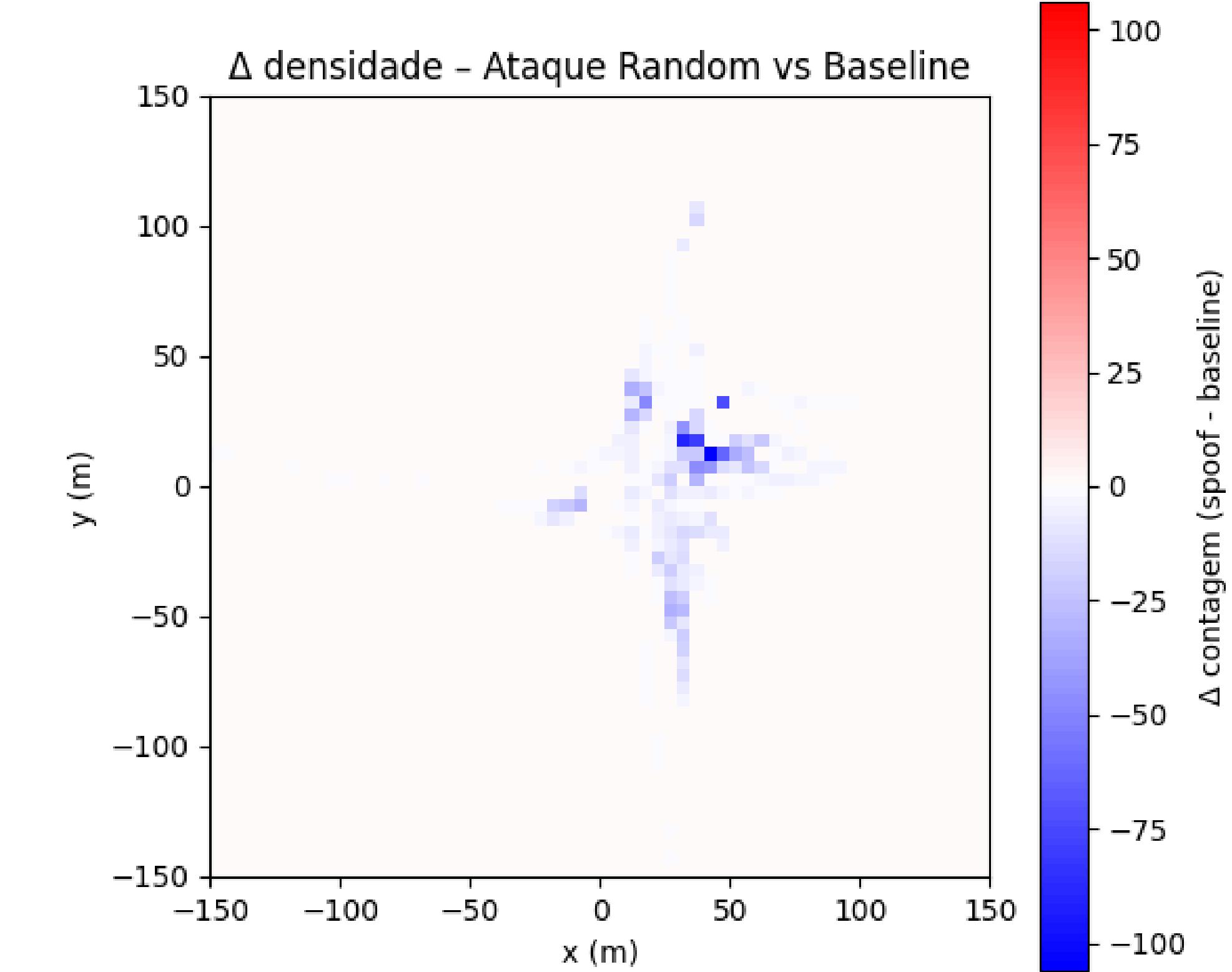
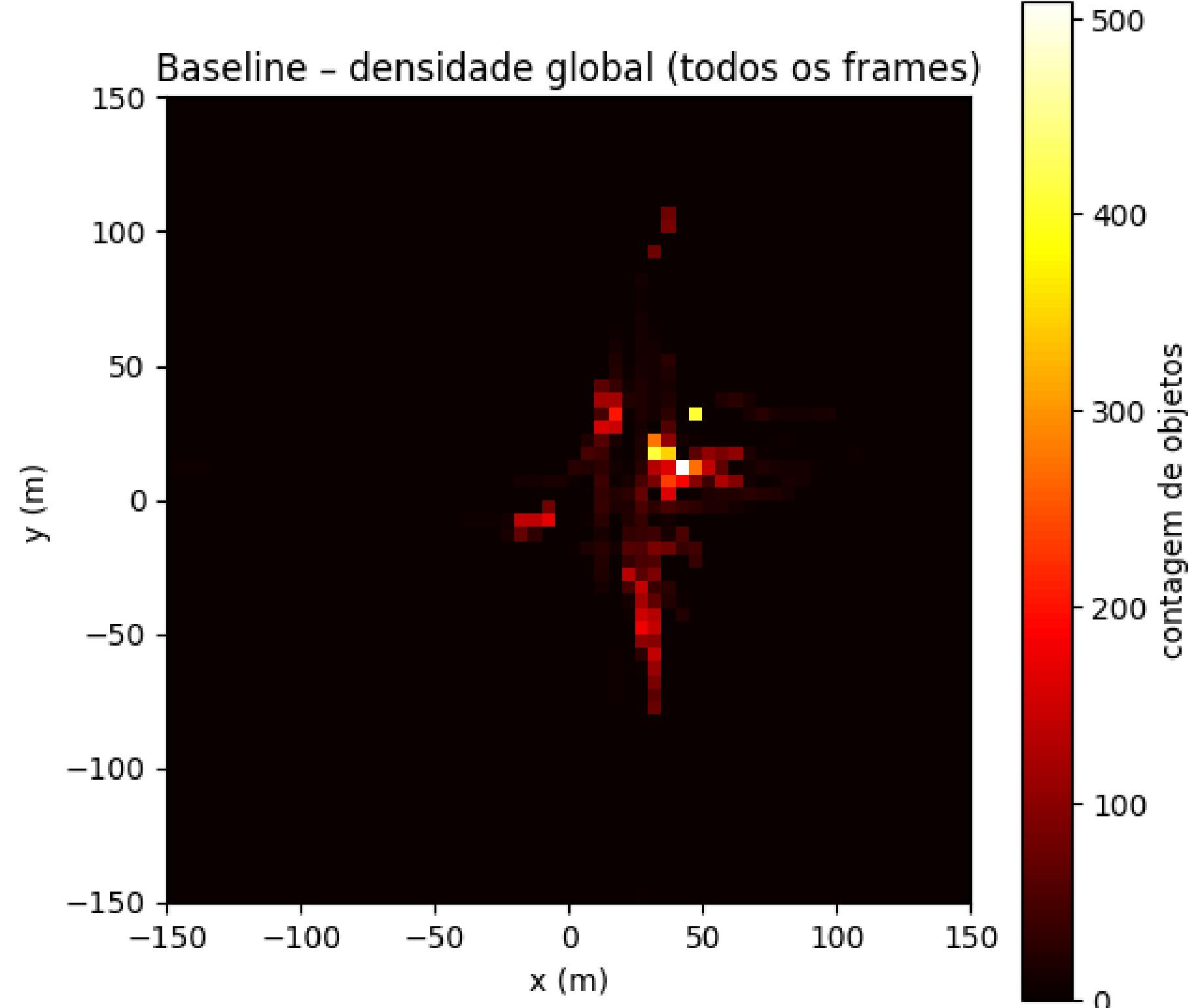
Métricas e Resultados

BASELINE X PHANTOM



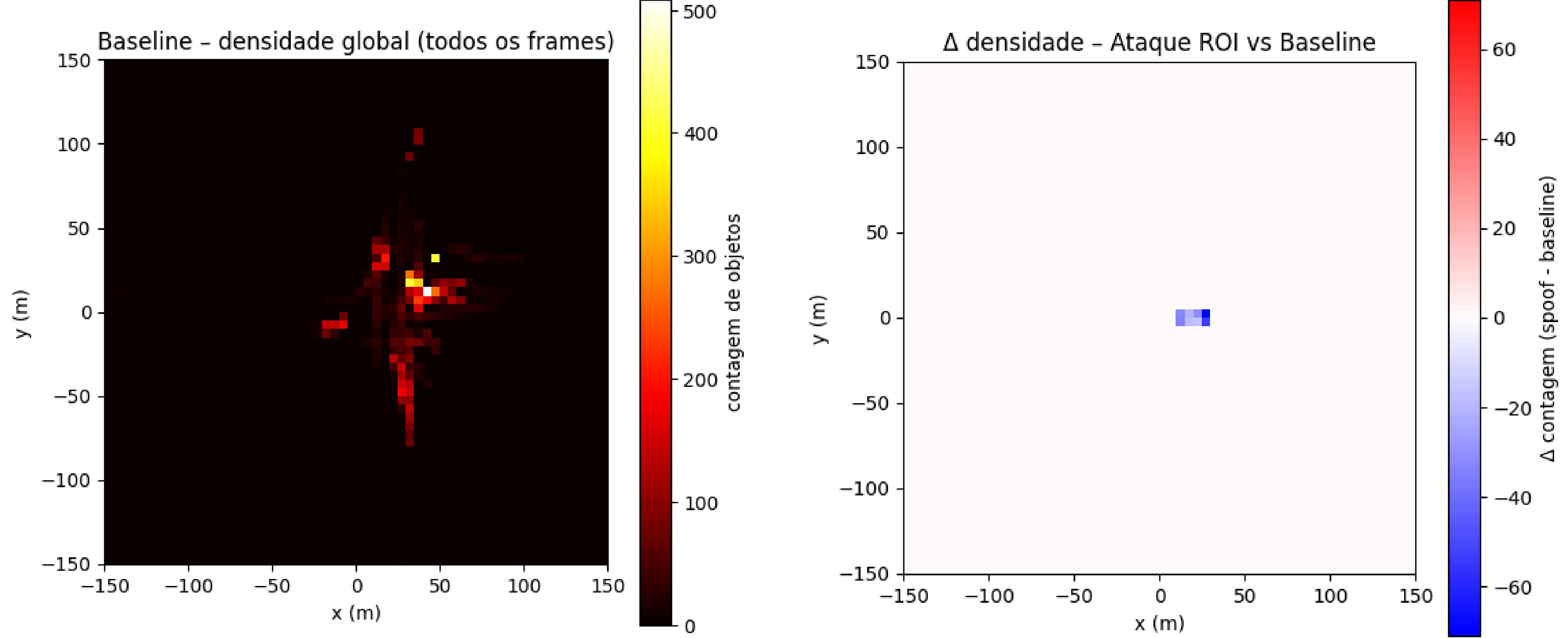
Métricas e Resultados

BASELINE X RANDOM



Métricas e Resultados

BASELINE X ROI



Future Research Directions

Simulation-Based Evaluation

Integrate the framework into simulations and hardware-in-the-loop experiments.

Inconsistency Detection

Develop mechanisms to detect cross-agent discrepancies and semantic implausibility.

Practical Defense Strategies

Extend conceptual insights to specific datasets and models for practical defenses.



Conclusão

- Ataques de spoofing perturbam significativamente a estrutura espacial da percepção cooperativa.
- Phantom, remoção aleatória e remoção em ROI apresentam assinaturas distintas, detectáveis via métricas geométricas.
- A metodologia é leve, reproduzível, e baseada no DevKit oficial – permitindo futura avaliação sobre detectores reais.

Baseline



Phantom



Random



ROI



Obrigado!