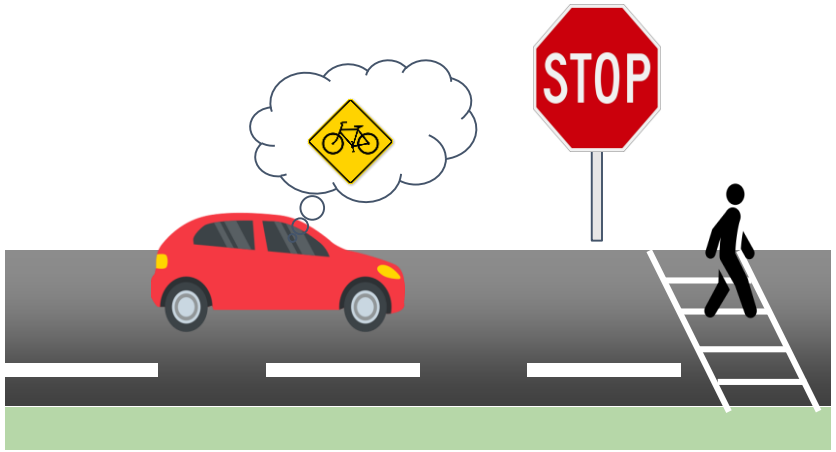
WIP: Infrared Laser Reflection Attack Against Traffic Sign Recognition Systems

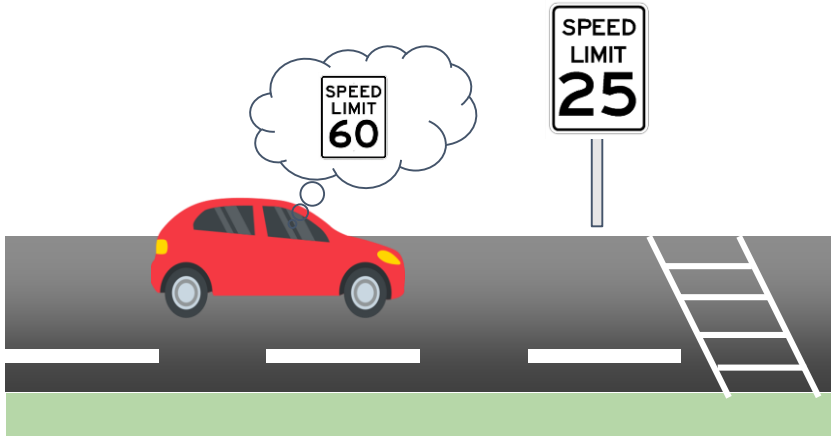
Takami Sato[1], **Sri Hrushikesh Varma Bhupathiraju**[2], Michael Clifford[3], Takeshi Sugawara[4], Qi Alfred Chen[1], and Sara Rampazzi[2]

1 UCI 2 UF 3 TOYOTA InfoTech Envisioning Mobility 4 UEC

Autonomous vehicle must obey traffic signs



- Hit pedestrians in crosswalk



- Sudden acceleration

- Attacker can cause safety implications by attacking traffic sign recognition

Limitations of Existing Attacks: Visibility for Human

[Eykholt et al., 2018]

[Chen et al., 2019]

[Zhao et al., 2019]

[Jia et al., 2022]

Existing attacks against vision-based traffic sign recognition are generally **visible to human eyes**

Our Attack: Infrared Laser Reflection (ILR) Attack

To human eye (normal camera)

A camera used in autonomous driving (AD)

Idea: Project IR laser onto traffic signs

- **IR laser trace is totally invisible for humans**
- Can perturbe **quite large area on traffic sign** w/o harming stealthiness
  - But, trace can be simple shape with monotonous purplish color
- **I-Can-See-the-Light attack** [Wang et al., 2021] also use IR laser to attack AD cameras
  - Not designed for traffic sign recognition systems
  - **Need to aim at camera in fastly moving vehicle**

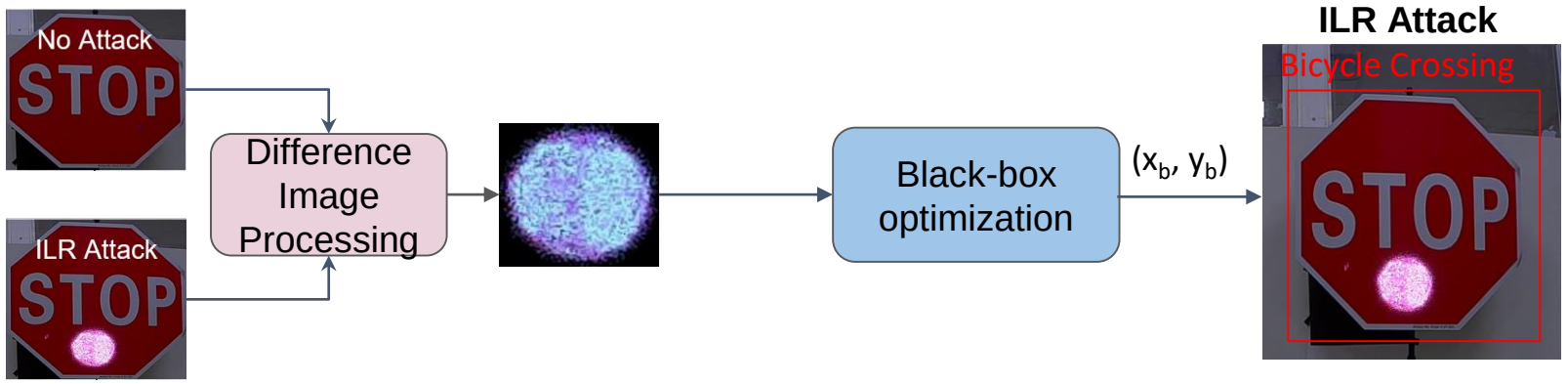
Trace Modeling and Optimization

Technical Challenges

1. Accurate IR laser reflection modeling
2. Effective optimization of attack parameters

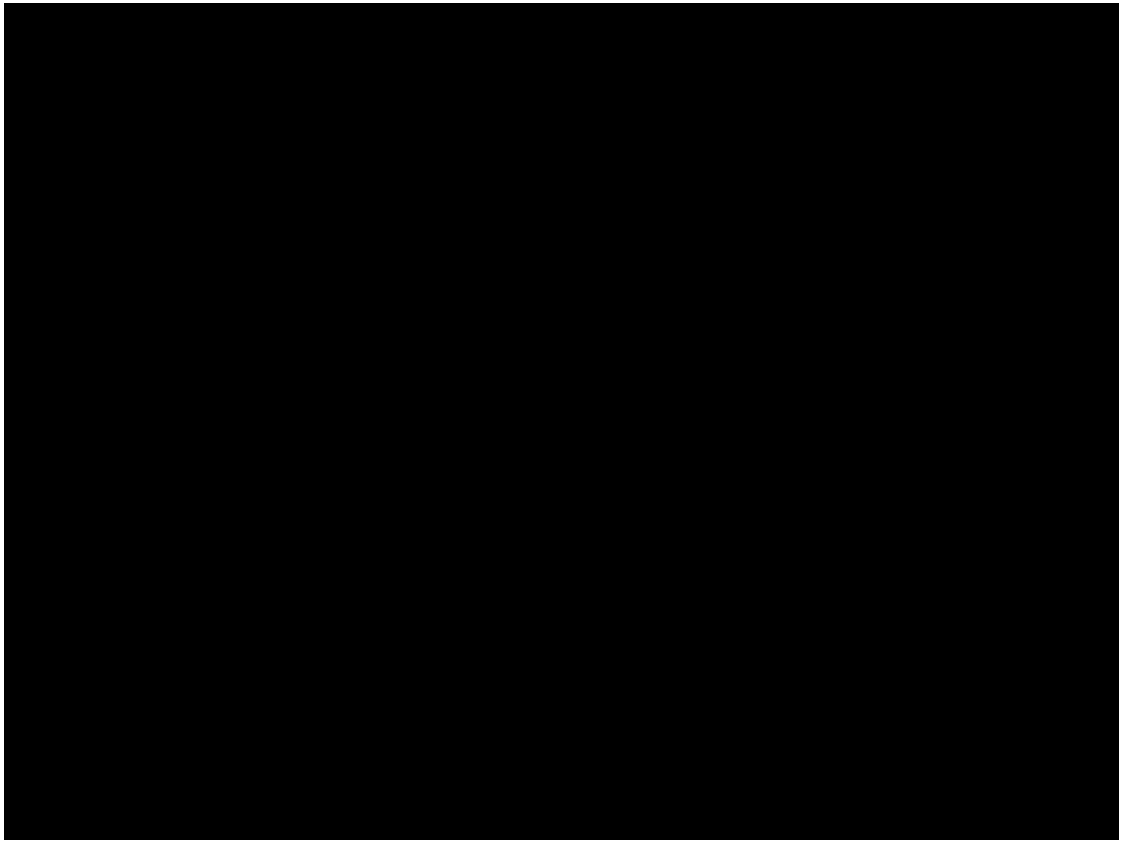
1. Image Difference-based IR Trace Modeling

2. Optimization Trace Position (x_b, y_b)



- **100% Attack Success Rate** (not detected as correct sign) in indoor lab setup
  - Random projection: only 20% attack success rate
- **90% Simulation Consistency Rate** (detected label is the same as simulated)

ILR Attack Demonstration



Take Away & Future Plan

- We present our ILR attack, a serious threat on traffic sign recognition systems due to its simple implementation.
- **ILR attack has a significantly higher attack success rate (100%) than the random attacks (20%)** in our indoor test environment

Future Plan

- **Evaluation on Outdoor Dynamic Scenarios and Real Vehicle**
  - Can attack be robust to different angles, lighting conditions, cameras, and etc.
- **More Faithful Trace Modeling for Attack Optimization**
  - To seek the most robust attack (e.g., ray tracing-based simulation)
- **Defense Evaluation**
  - Can existing defenses for patch attacks be effective?

Thank you!

WIP: Infrared Laser Reflection Attack Against Traffic Sign Recognition Systems

Takami Sato, **Sri Hrushikesh Varma Bhupathiraju**, Michael Clifford, Takeshi Sugawara, Qi Alfred Chen, and Sara Rampazzi

Download our paper here

For more details, please visit our demo (#55)

UCI UF TOYOTA InfoTech Envisioning Mobility UEC