ADoPT: LiDAR Spoofing Attack Detection Based on Point-Level Temporal Consistency

Minkyoung Cho[1], Yulong Cao[2], Zixiang Zhou[1], Z. Morley Mao[1]

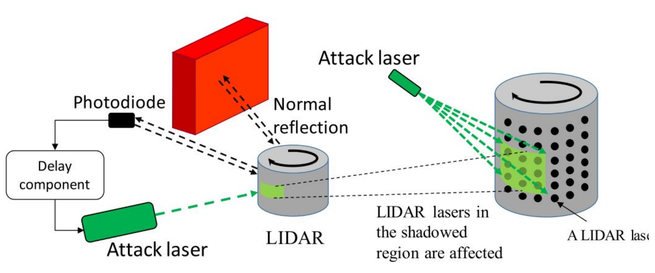
1: University of Michigan 2: NVIDIA Research

BMVC 2023

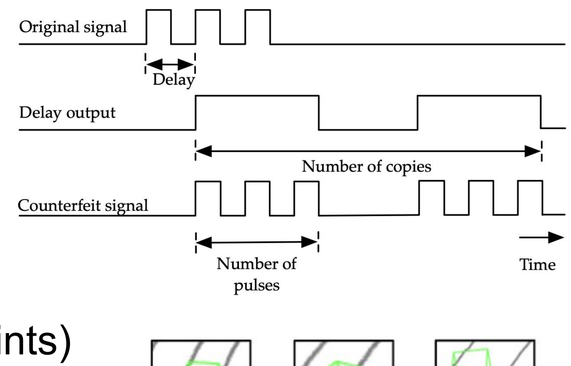
Background

LiDAR Spoofing Attack

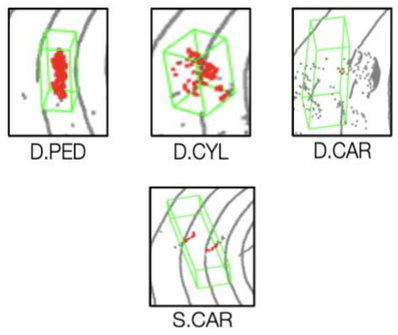
Emitting spurious LiDAR purses



Jamming LiDAR signal



- Dense Point Injection (< 200 points)
  - Visually recognizable fake object
  - Attack success rate: 96~97%
- Sparse Point Injection (< 64 points)
  - Difficult to visually identify
  - Attack success rate: < 21%



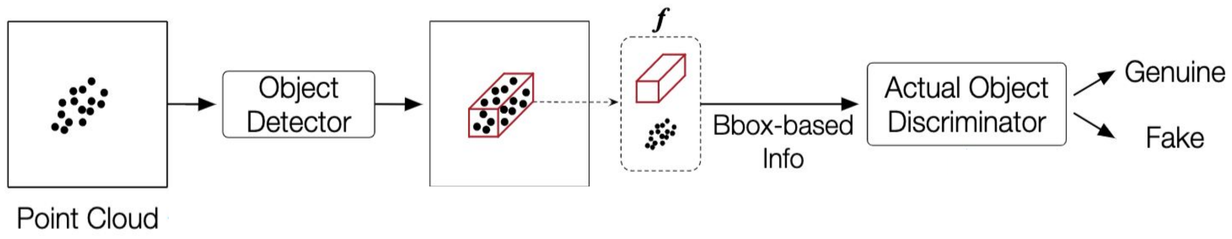
Previous Solutions

Physical law-based Defense

- Free and occluded space in **box**
- Shadow region dictated by **bbox**
- Point density in **bbox** and distance to sensor

Consistency-based Defense

- Moving pattern of **bboxes**
- temporal consistency & motion prediction of **bboxes**

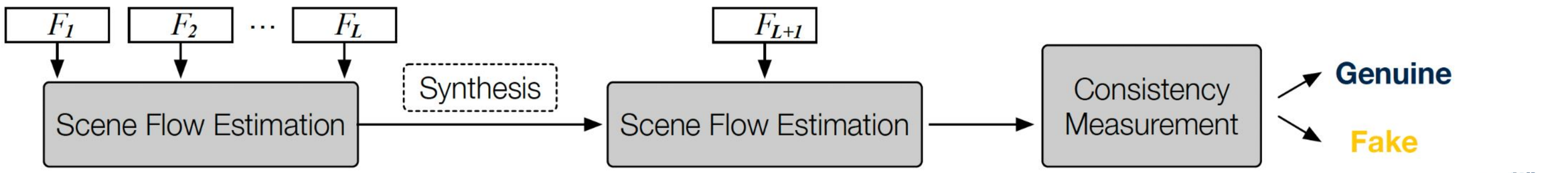


What if object detector yields erroneous bounding box info?

ADoPT: Anomaly Detection on Point-Level Temporal Consistency

How to quantitatively measure point-level temporal consistency and identify abnormal object?

KEY: Object consists of point clusters with a certain degree of point intensity, moving coherently.

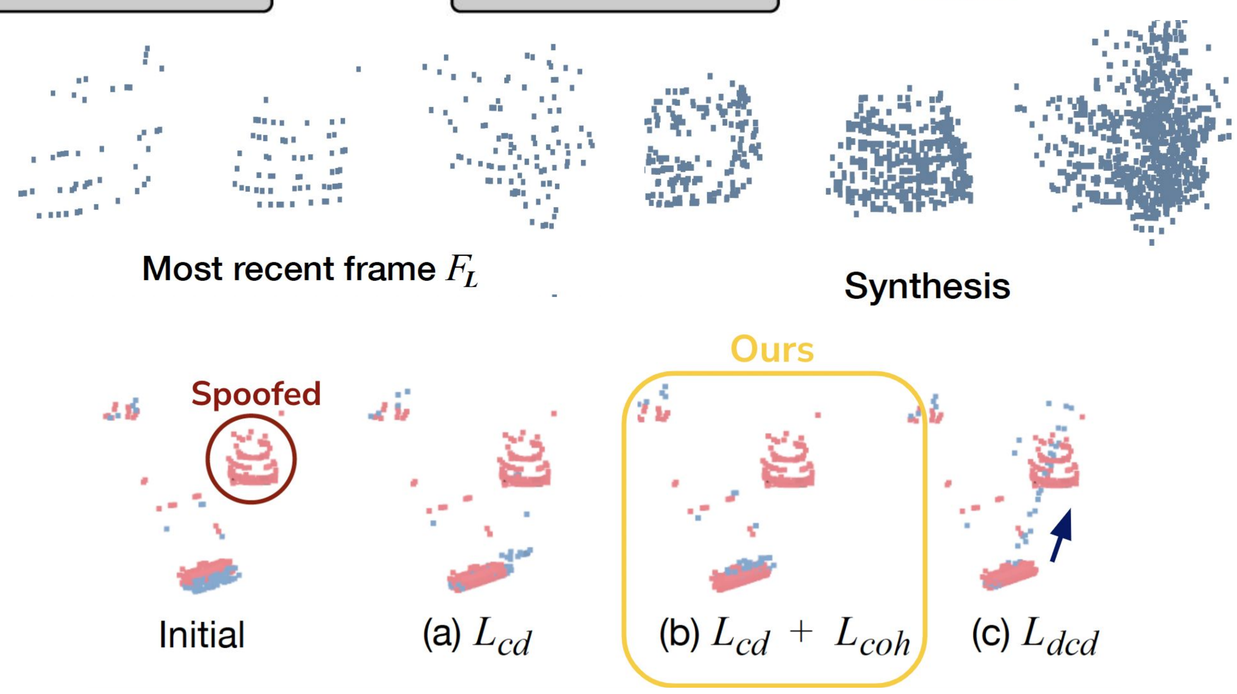


Coherence-Enhanced Scene Flow Estimation

- **Goal:** Make points of an object move coherently over time-series frames
- Online optimization-based scene flow estimation
  - Objective: Chamfer Distance + Coherence loss

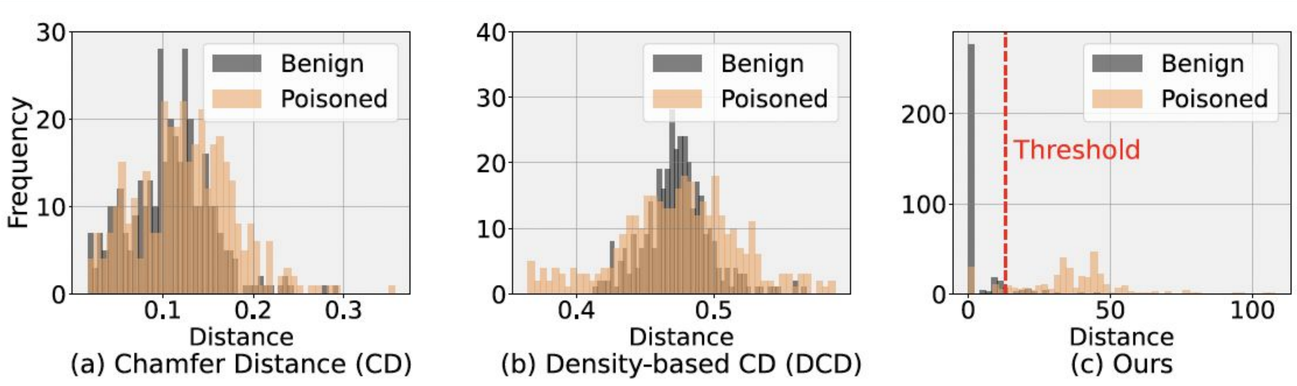
Cluster-based Consistency Measurement

- **Goal**: Distinguish between benign frame and poisoned frame
- Perform spatial clustering (DBSCAN) to find out clusters which exclusively contains points in F_{L+1}



Evaluation Results

- **Our consistency metric allows for establishing a threshold for attack detection**



- **ADoPT achieves lower false positive rates and higher true positive rates**

	Dense Point Injection				Sparse Point Injection	
	FP ↓	TP (D.CAR) ↑	TP (D.CYL) ↑	TP (D.PED) ↑	FP ↓	TP (S.CAR) ↑
CARLO [23]	47.2	48.0	49.4	48.0	47.9	54.4
3D-TC2 (PP) [33]	20.7	98.6	95.0	56.9	16.6	53.5
3D-TC2 (SEC) [33]	19.6	98.3	45.8	47.5	16.3	84.2
ADoPT	4.5	97.2	98.3	95.2	9.3	85.4