Physical Hijacking Attacks against Object Trackers

Review

Dishant Sharma[1] Harshit Kashyap[1] Udrasht Pal[1]

[1]International Institute Of Information Technology
Hyderabad,Telangana,India

SNS, APR 2023

Table of Contents

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

Paper Objective

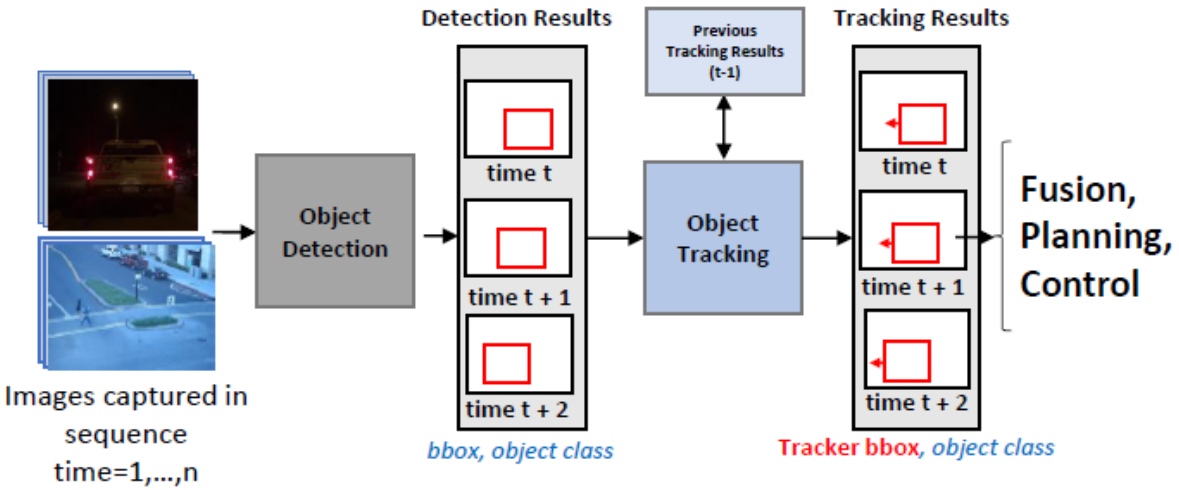
Siamese Tracker Control Hijacking(AttrackZone)

This attack method involves identifying specific areas within a physical environment that can be used for physical interference, allowing the attacker to take control of the tracker.

How It Works

Objection Detection,Objection tracking

object detection and object tracking is the main task in Autonomous system like Self-driving cars,Video surveillance,etc



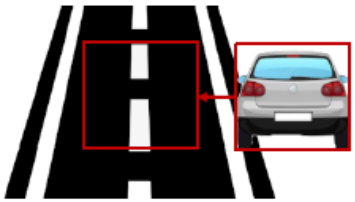
TERNATIONAL INSTITUTE OI INFORMATION TECHNOLOGY
HYDERABAD

Types of Attack

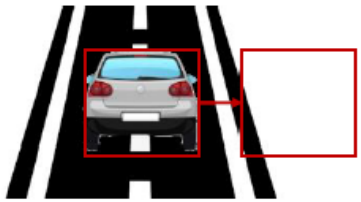
Attack Perform

-Move-in

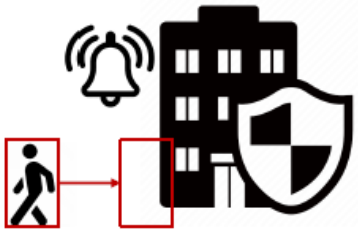
-Move-out



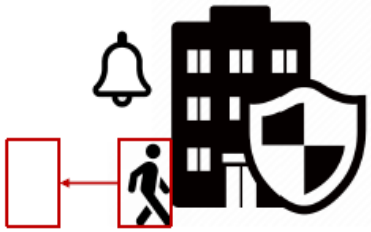
Move-in Attack



Move-out Attack



Move-in Attack



Move-out Attack

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY

HYDERABAD

Assumptions

Attacker Know the Victim view

-Where the camera or cameras are mounted.

-For finding the victim view attacker use surrogate camera.

Siamese-based object tracker

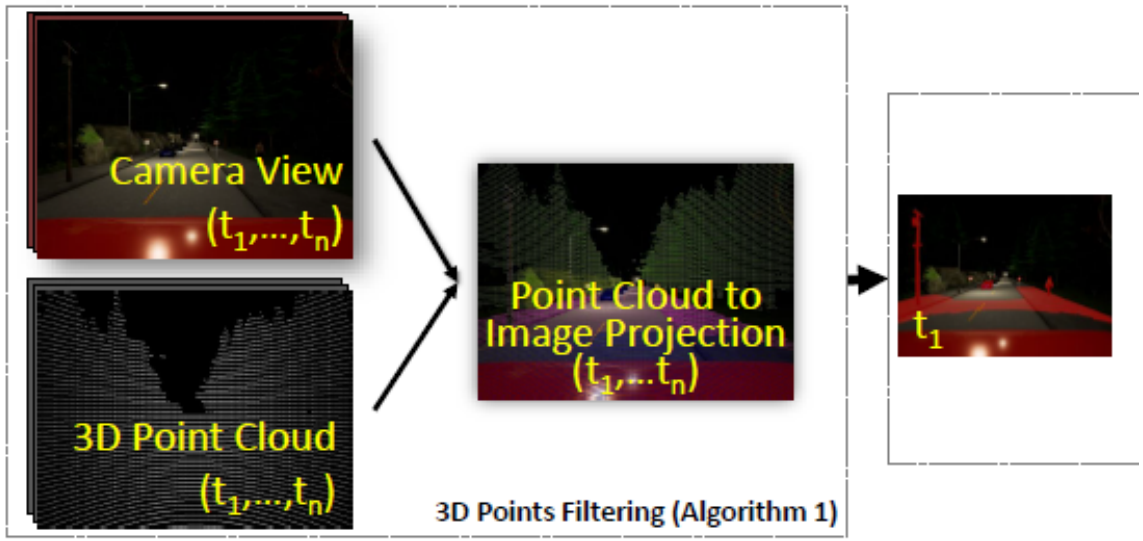
Attacker has access to any open-source Siamese-based object tracker for generating the physical perturbations based on the surrogate camera feed

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY

HYDERABAD

Generate Victim View

-Point Cloud Remapping
-Attack Zone Generation



Perturbation Generation

- Create Perturbation using siamese-based Network

-Apply siamese on Final Attack Zone Generated

- Minimize the loss function

- For create the effective Perturbation minimize the loss function

$$L(I, N, \theta) = \sum_{n=1}^{N} [L_c(I_n, p_c, \theta) + \lambda * L_r(I_n, p_r, \theta)]$$

-Test the Perturbation on Kalman filter

-If the Intersection over Union (IoU) of the Kalman Filter results is less than 70%.
The noise is ineffective
Discard that pattern.

Attack SetUp

Emulated Attacks

Perform Attack on VOT dataset
-visual dataset that includes samples from various object-tracking applications

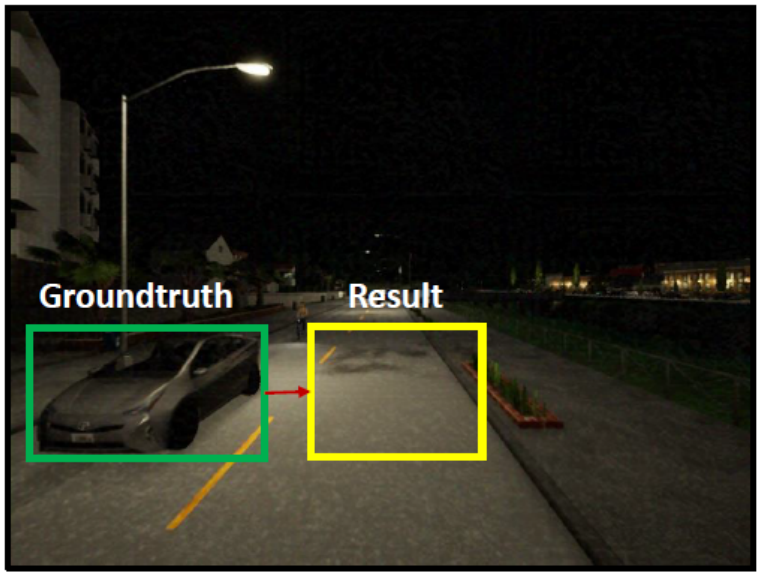
Simulated Attacks on CARLA

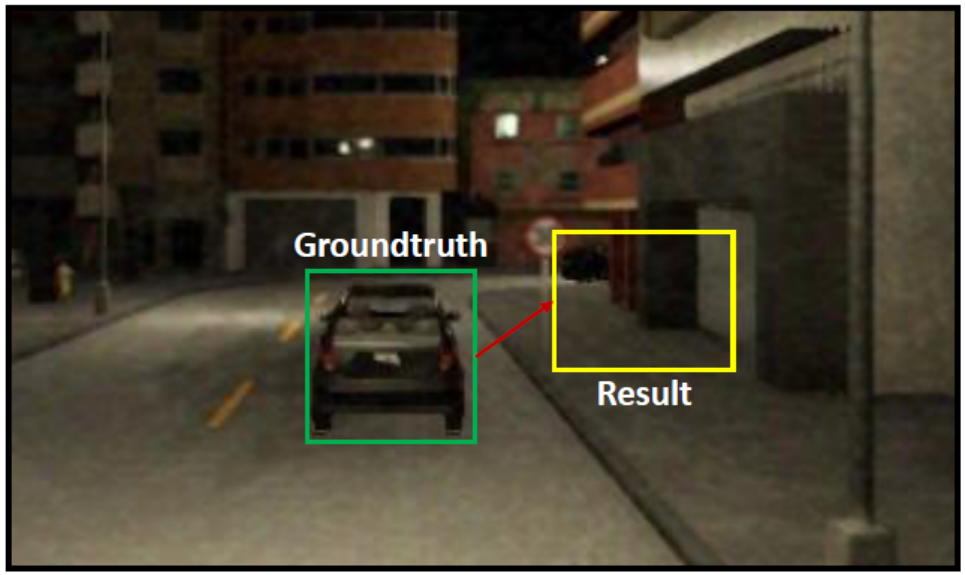
Perform Attack using CARLA simulator
-visual dataset that includes samples from various object-tracking applications

Real-world Physical Attacks

-Online Attack
-Offline Attack

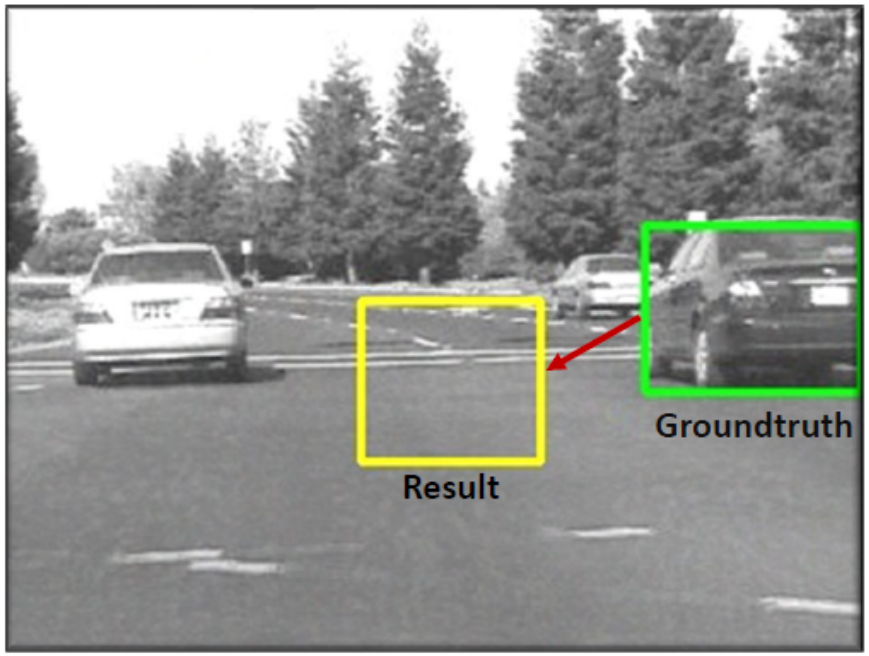
Result Image Of Simulator

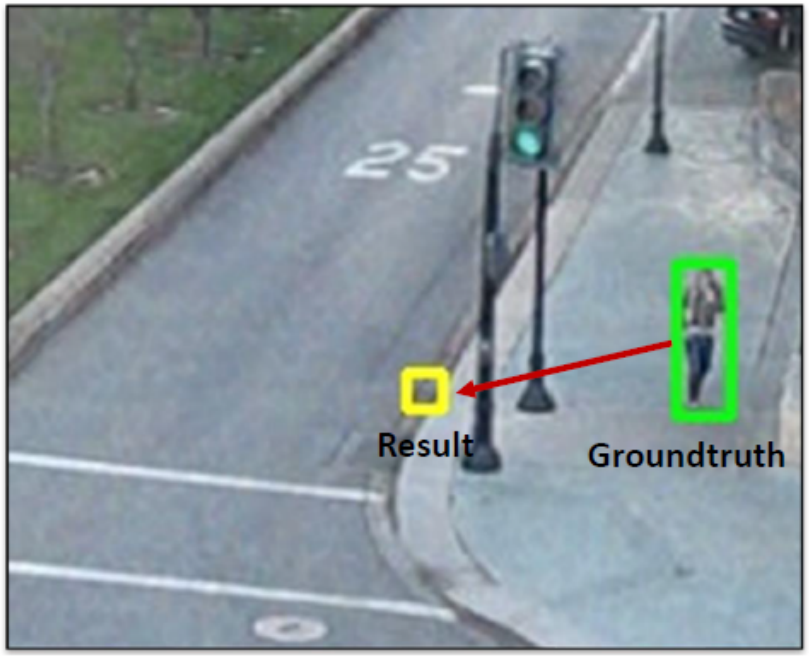




INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

Result Image Of Real-word





INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

Critique

1).Additional use of sensors of different classes

2).Anomaly Detect

3).Lack of Dataset for experiments

4).Flaw in Assumption

5).Technology Issue

Additional use of sensors of different classes

According to their assumption they are trying to hijack controls of autonomous driving and video surveillance but these devices may use different sensors of more then two type like LIDAR or SONAR with camera feed so that if siamese tracker based on camera feed deviates from actual target other sensors will stop shifting of control focus to wrong direction.

ADAS : There are several real-world technologies that use sensor fusion to enhance security and protect against control hijacking attacks on Siamese networks in autonomous driving and video surveillance.

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

Anomaly Detect

To perform control hijacking they have accepted that 10-100 frames with sequential perturbation is necessary in 0.3-3 second of duration therefore we can deploy machine learning algorithms that can detect abnormal activity in the tracking system

Anomaly detection algorithms can detect unusual tracking behavior that may be indicative of an attack. There are various algorithms with the help of this autonomous system to detect anomalies.
Some anomalies detection algorithm are:
-Support Vector Machines (SVMs)
-Hidden Markov Models (HMMs)

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

Lack of Dataset for experiments

Emulated Attack

They are using the complete 15 test samples from the VOT dataset for autonomous driving and give the accuracy 100% which is not feasible and will not give correct analysis of attack in real word
Suggestion: If they are taking that much advantage of manual selection, they should increase the dataset

Real-world Experiments

In attack scenario creation it is mentioned that in the absence of a LiDAR sensor, they are manually mapping valid attack zones for the environments. They have only taken 9 offline real world attack into consideration which is very less and real world have many test case
Suggestion: Increase the test sample dataset

Flaw in Assumption

Based on the assumption used in this paper, the attacker knows the location of the system running the object tracker (where the camera or cameras are mounted).

victim's camera feed directly. In today's world, it is possible to gain access to a victim's camera feed without using a surrogate camera
For example, an attacker could exploit a vulnerability in the victim's camera software or network to gain remote access to the camera feed. They could also use a phishing attack or other social engineering technique to trick the victim 5 into installing malware on their device, which would allow the attacker to gain access to the camera feed

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

Technology Issue

This attack targets trackers based on Siamese networks. However, the results show and it is mentioned that the DaSiamRPN+ algorithm used by the tracker is very effective in detecting the distractions created by the attacker

Suggestion:
use:
-SiamRPN++
-Kernelized Correlation Filters

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

References

[1].shoei Nashimoto, Daisuke Suzuki, Takeshi Sugawara, and Kazuo Sakiyama. Sensor con-fusion: Defeating kalman filter in signal injection attack. In Asia Con- ference on Computer and Communications Security, 2018

[2].Fooling Detection alone is not Enough: Adversarial attack against multiple object tracking,2020

[3].Open Source Computer Vision. Opencv: Kalmanfilter reference. 27-August-2022].

[4].Bing Shuai, Andrew G. Berneshawi, Xinyu Li, Davide Modolo, and Joseph Tighe. Siammot: Siamese multi-object tracking. Computer Vision and Pattern Recognition (CVPR), 2021.

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD