Drift with Devil: Security of Multi-Sensor Fusion based Localization in High-Level Autonomous Driving under GPS Spoofing

Junjie Shen, *Jun Yeon Won, Zeyuan Chen, Qi Alfred Chen*

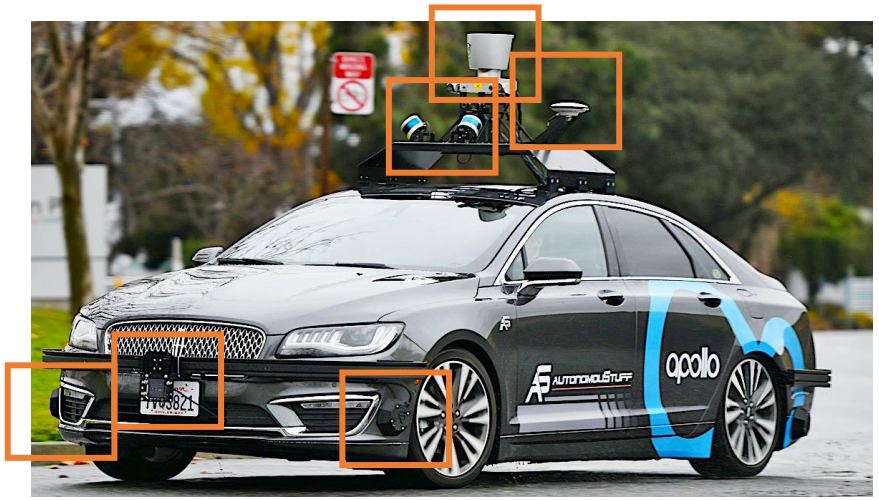
ASGuard Autonomous System Guard Research Group

UCI

Autonomous Vehicles (AVs) are finally on public roads

High-Level Autonomous Driving (AD) System

A typical Level-4 AV:



Abundant sensors:
LiDAR, GPS, IMU, Camera, Radar, etc.

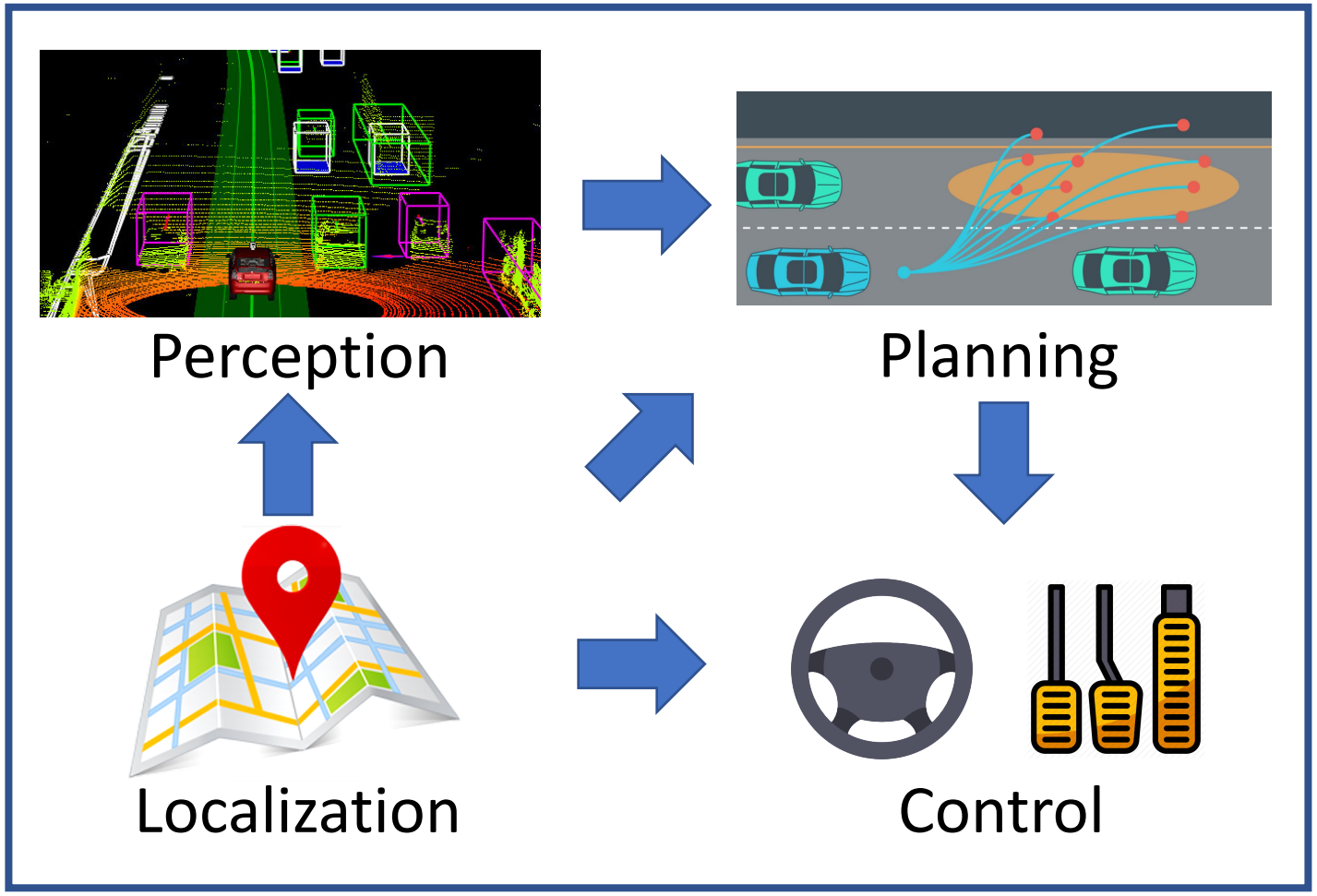
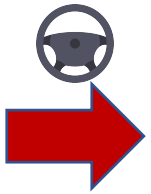
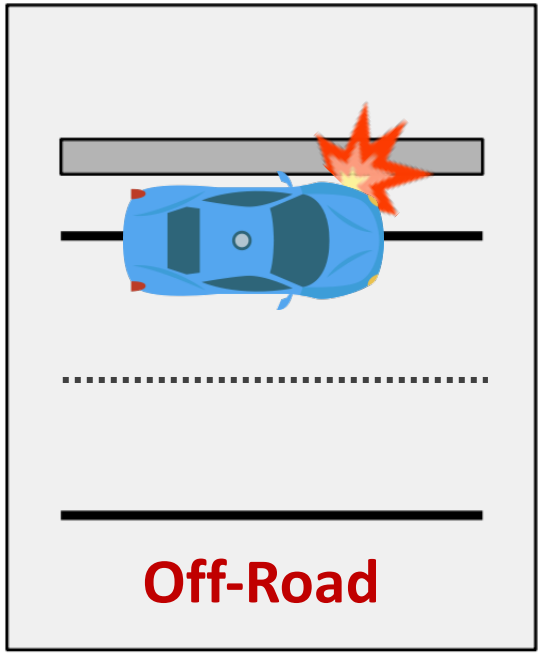


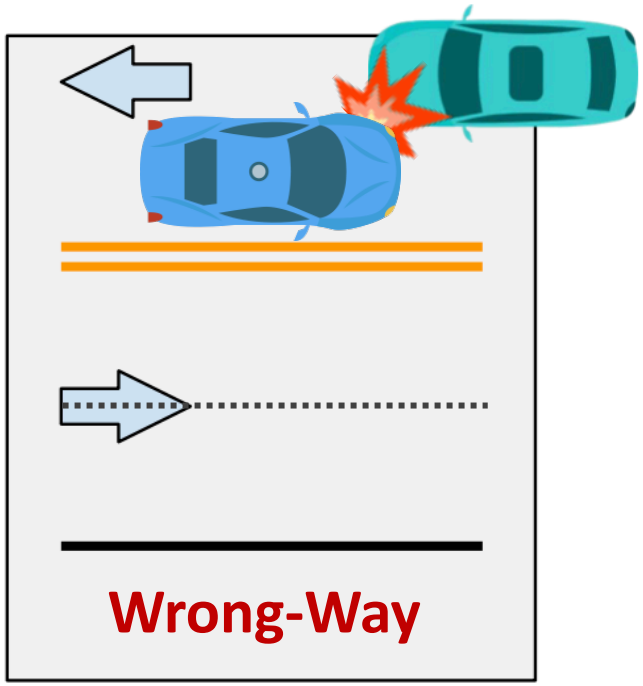
Photo Credit: Baidu

Localization is critical to the safety of AV

Localization

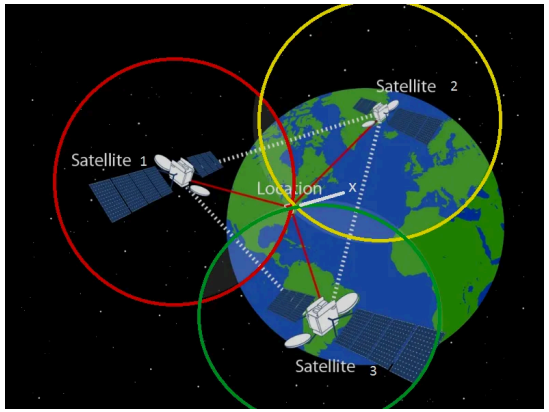


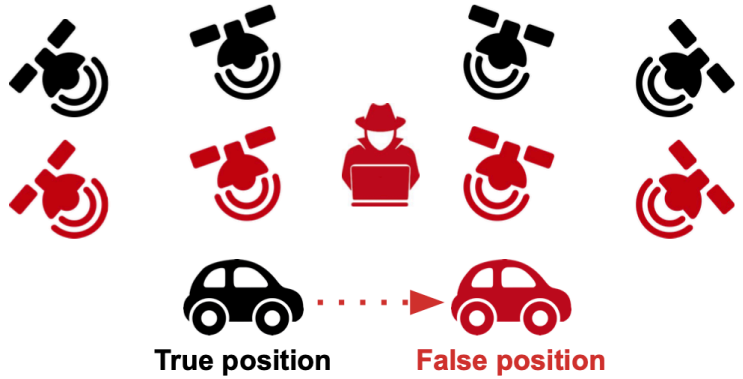


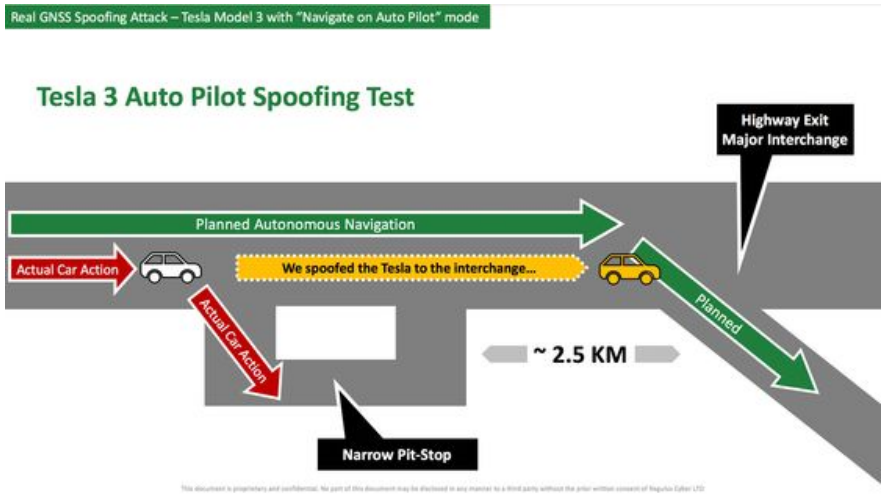


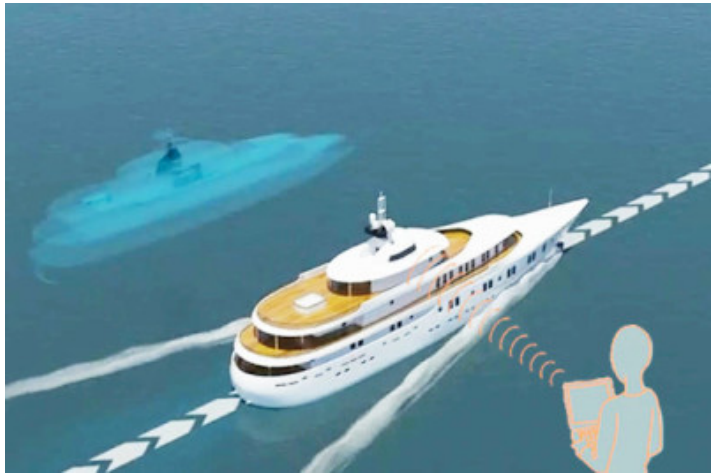
GPS spoofing attack

- GPS is the *de facto* location input for AD localization
- GPS spoofing attacks
  - Attacker sets **arbitrary position** by sending fake satellite signals
  - Still an **open problem**
    - Demonstrated in cars, yachts, drones, smartphones, etc.

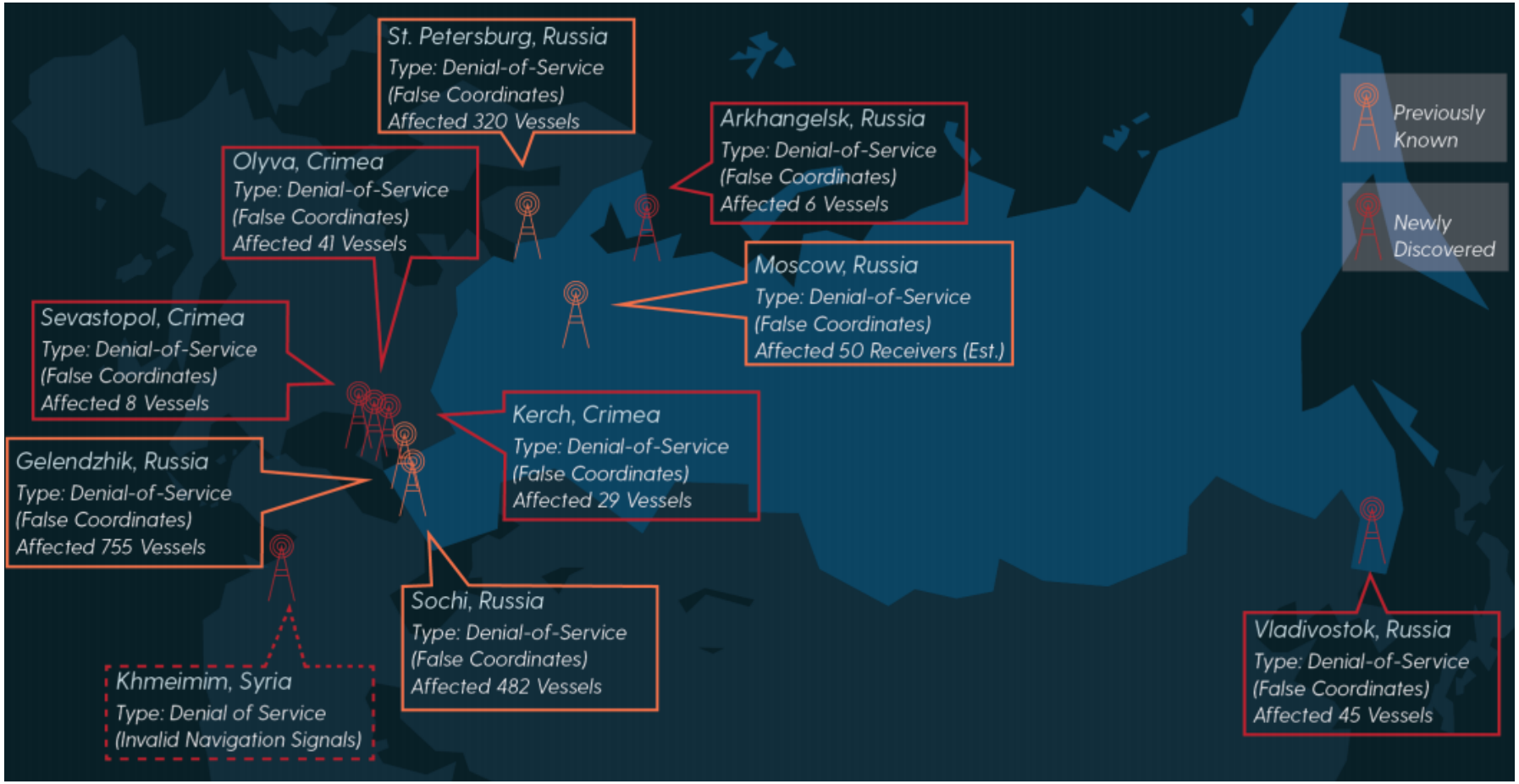








GPS spoofing is pervasive!

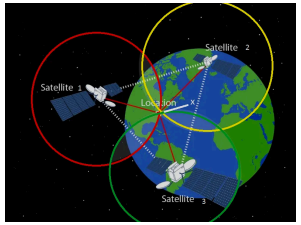


Over 9,883 spoofing events identified; **1,311** civilian vessels affected since Feb. 2016 in Russia.

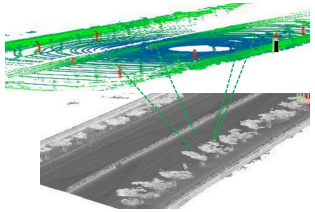
Source: Above Us Only Stars @ C4ADS

Multi-Sensor Fusion (MSF) based AD localization

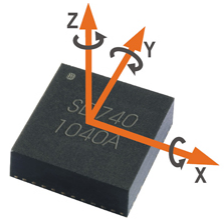
- However, production high-level AD systems widely adopt **MSF-based localization** design
  - Baidu Apollo, [ICRA'18] [ITS'16] [IV'16] [Sensors'15] [IROS'13] [IJRR'11], etc.
  - **Leverage strengths & compensate weaknesses** of different sensors to generally improve ***accuracy*** & ***robustness***
    - Most popularly fuse from GPS, LiDAR, and IMU
    - Can achieve ***5.4 cm*** accuracy
- In such a design, GPS alone cannot dictate the localization results



GPS



LiDAR locator



IMU

MSF: Generally believed to have potential to defend against GPS spoofing

Sensor Fusion: Resilient estimation algorithms usually assume a variety of multi-modal sensors to achieve their security guarantees. This is also the idea behind sensor fusion, where sensors of different types can help "confirm" the measurement of other sensors [134, 135, 136]. A basic example of sensor fusion in automotive systems is to verify that both the LiDAR readings and the camera measurements report consistent observations.

[Cardenas, CyBOK '19]

Sensor fusion: Combining data from multiple distinct sensors, known as *sensor fusion* [3], significantly raises the difficulty of sensor input spoofing attacks. As an ex-

[Davidson et al., WOOT '16]

We hope the results can help to raise the attention in the community to develop *practically deployable* defense mechanisms (*e.g.*, location verification, signal authentication, sensor fusion) to protect the massive GPS device users and emerging GPS-enabled autonomous systems.

[Zeng et al., USENIX Security '18]

This research presented a statistical approach to the problem of attack detection on the multi-sensor integration of autonomous vehicle navigation systems. Starting with a state-space model of the system under attack, a parametric statistical tool with a multi-sensor integration strategy was developed to identify an attack. Finally, a simulation was designed to verify the proposed detection system and results were presented. A

[Lee et al., SMC '17]

SENSOR FUSION

As should be apparent from earlier discussions, different technologies available for detection and tracking of UAVs have various trade-offs related to cost, accuracy, precision, range, energy efficiency (critical if sensors operate on batteries),
l at other UAVs),
example, while
nly operate very
mputer vision),
NLOS environ-
es). For accurate
JAVs, data fusion
isly use informa-
ors carry critical
for joint use of
coustic sensors,
optical camer-
as), and this constitutes an open research area.

[Guvenc et al., IEEE Comm '18]

Research Question:

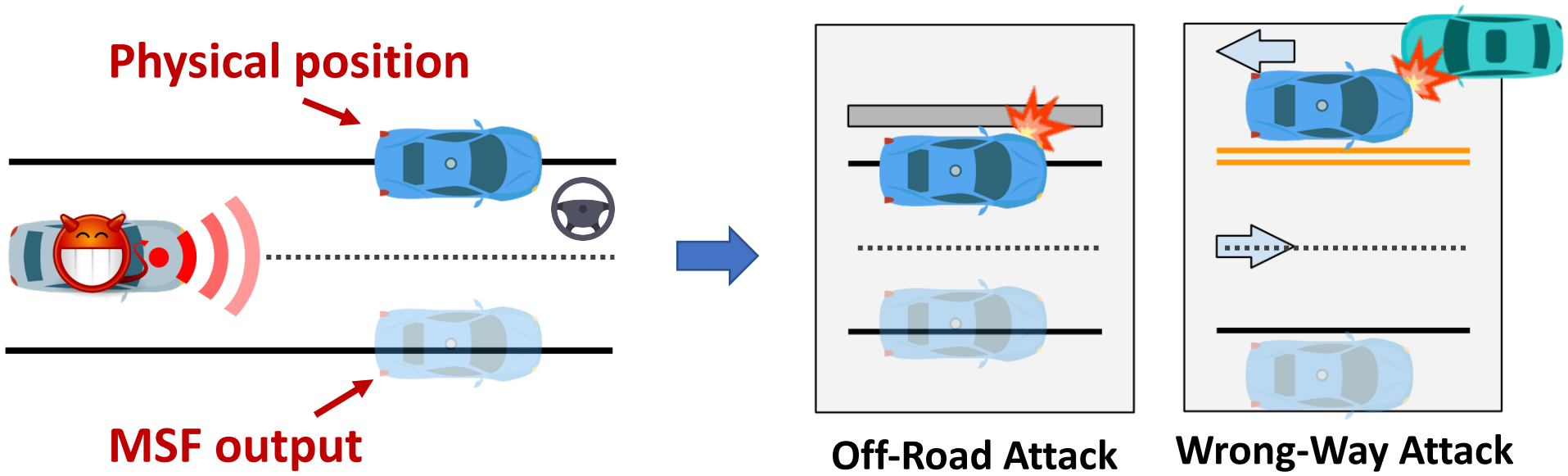
In AV settings, whether state-of-the-art MSF algorithms are ***indeed sufficiently secure*** under GPS spoofing?

***Short Answer: No**, as long as the spoofing is done **strategically**!*

End-to-end attack demo

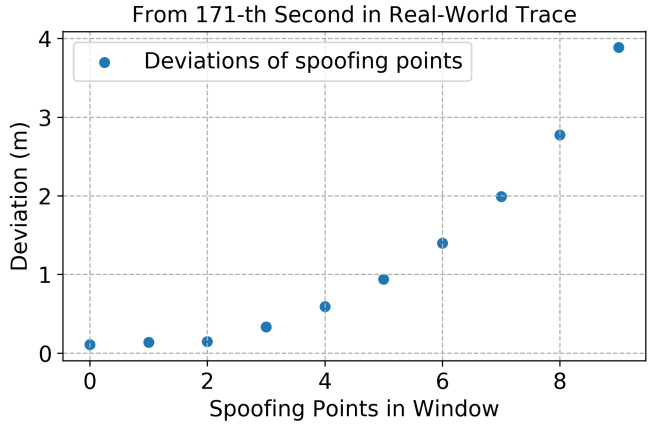
Problem formulation and attack goals

- Problem formulation
  - Attacker spoofs GPS inputs with certain distances to victim's physical positions
  - Aim to **maximize lateral deviation** in MSF output w.r.t. no attack
- Attack goals: cause victim to drive **off-road** or onto a **wrong-way**



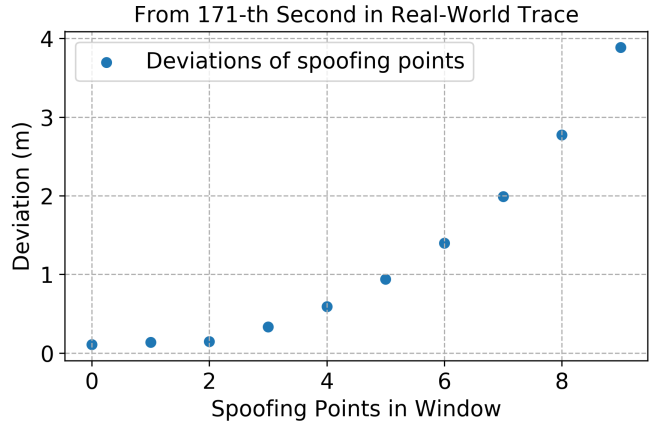
Security analysis

- Aim to find **maximum possible deviation** achievable by spoofing
- Target: Baidu Apollo MSF (representative in both design & impl.)
- MSF ***indeed* improves** security against GPS spoofing
- Discovered an interesting **take-over effect,** causing an ***exponential growth trend*** of deviations
  - Spoofed GPS becomes **dominating source** to MSF



Security analysis

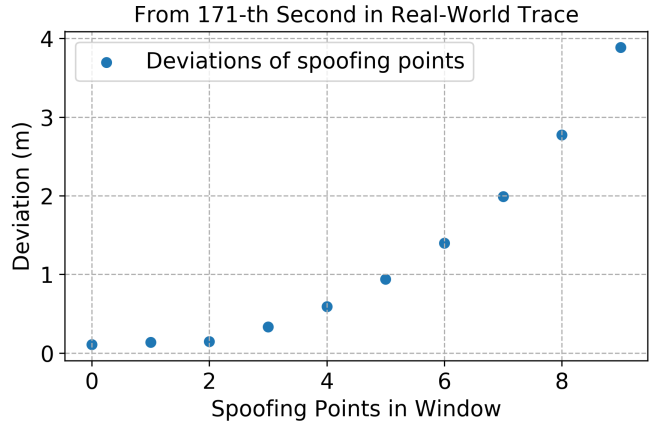
- Aim to find **maximum possible deviation** achievable by spoofing
- Target: Baidu Apollo MSF (representative in both design & impl.)
- MSF ***indeed* improves** security against GPS spoofing
- Discovered an interesting **take-over effect,** causing an ***exponential growth trend*** of deviations
  - Spoofed GPS becomes **dominating source** to MSF



Take-over effect: ***fundamentally*** defeats **design principle** of MSF!

Security analysis

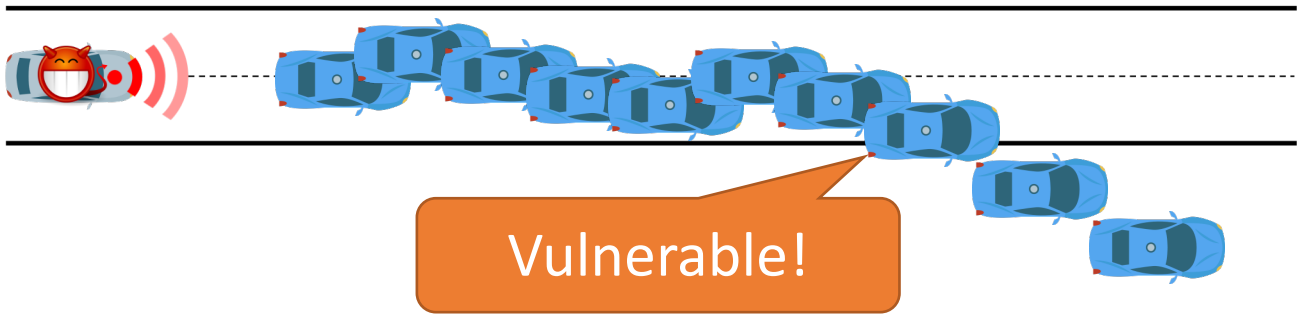
- Aim to find **maximum possible deviation** achievable by spoofing
- Target: Baidu Apollo MSF (representative in both design & impl.)
- MSF ***indeed* improves** security against GPS spoofing
- Discovered an interesting **take-over effect,** causing an ***exponential growth trend*** of deviations
  - Spoofed GPS becomes **dominating source** to MSF
- Cause: ***Dynamic*** and ***non-deterministic*** factors
  - e.g., sensor noises, algorithm inaccuracies, etc.



Take-over effect: ***fundamentally*** defeats **design principle** of MSF!

Attack design: FusionRipper

- Take-over vulnerability is **hard to predict/control** by attacker
- Needs to exploit in an **opportunistic** way
- FusionRipper: 2-stage attack
  - **Vulnerability profiling + aggressive spoofing**



Stage 1: vulnerability profiling **Stage 2: aggressive spoofing**

Evaluation result highlights

- Evaluate on 6 real-world AV sensor traces
  - ***Always*** exists **>= one** attack parameter can achieve **98.6%** & **95.9%** success rates to cause **lane departure** or **wrong-way driving**
  - Takes ***only ~30 sec*** to succeed
- Practical attack considerations
  - Robust to ***spoofing inaccuracies*** and ***AD control***
  - Success rate only down by **<= 4%**
- Also did ***ablation study***, ***generality analysis*** *(w/ 2 other MSF designs)*, ***comparison w/ naive attack***, ***black-box attack design*** *(profiling cost <= half a day)*, etc.
  - *More details in the paper…*

Potential defenses

- Fundamental solutions are not immediately deployable
  - Prevent GPS spoofing; improve sensing and AD localization technologies
- **Actionable mitigation: attack detection & emergency stop**
  - Based on GPS spoofing detection, or camera-based lane detection
  - Still can cause DoS, but better than directly causing safety damages

Responsible vulnerability disclosure

- As of 7/20/20, informed **29 companies** developing/testing Level-4 AVs
  - **16** has replied so far and **have started investigation**
  - **1** of them **is working on a fix**

Conclusion

First security analysis on MSF-based AD localization under GPS spoofing

- Discover **take-over vulnerability** that ***fundamentally*** defeats MSF design principle
- Design **FusionRipper** to ***opportunistically*** capture & exploit the vuln.
- Design ***offline*** **profiling method** to improve attack practicality
- Informed **29** companies developing/testing Level-4 AVs

Thank you!

More details please visit our project website:

https://sites.google.com/view/cav-sec/fusionripper

Scan to visit our project website

ASGuard Autonomous System Guard Research Group

UCI