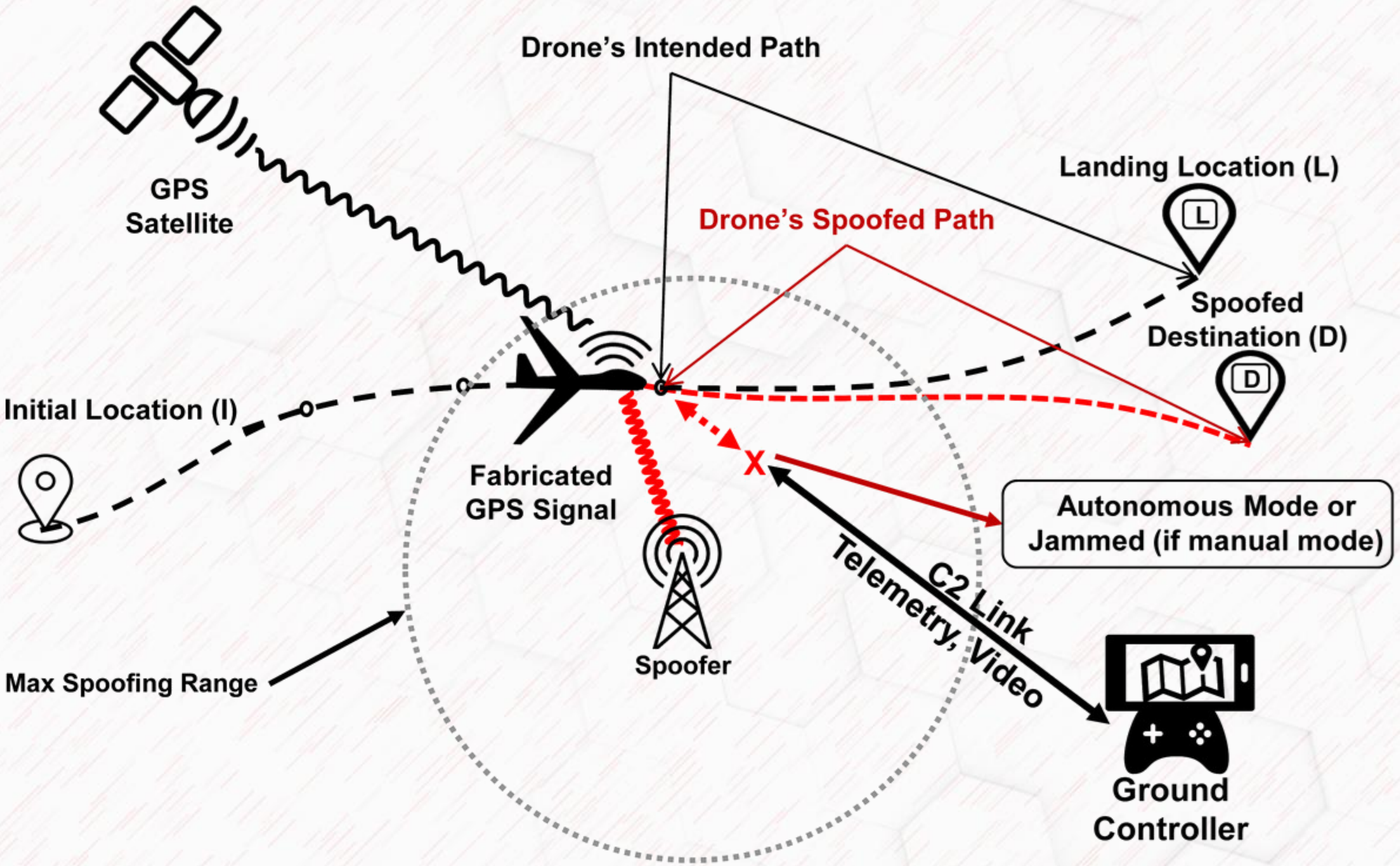
Secure Pose Estimation for Autonomous Vehicles under Cyber Attacks

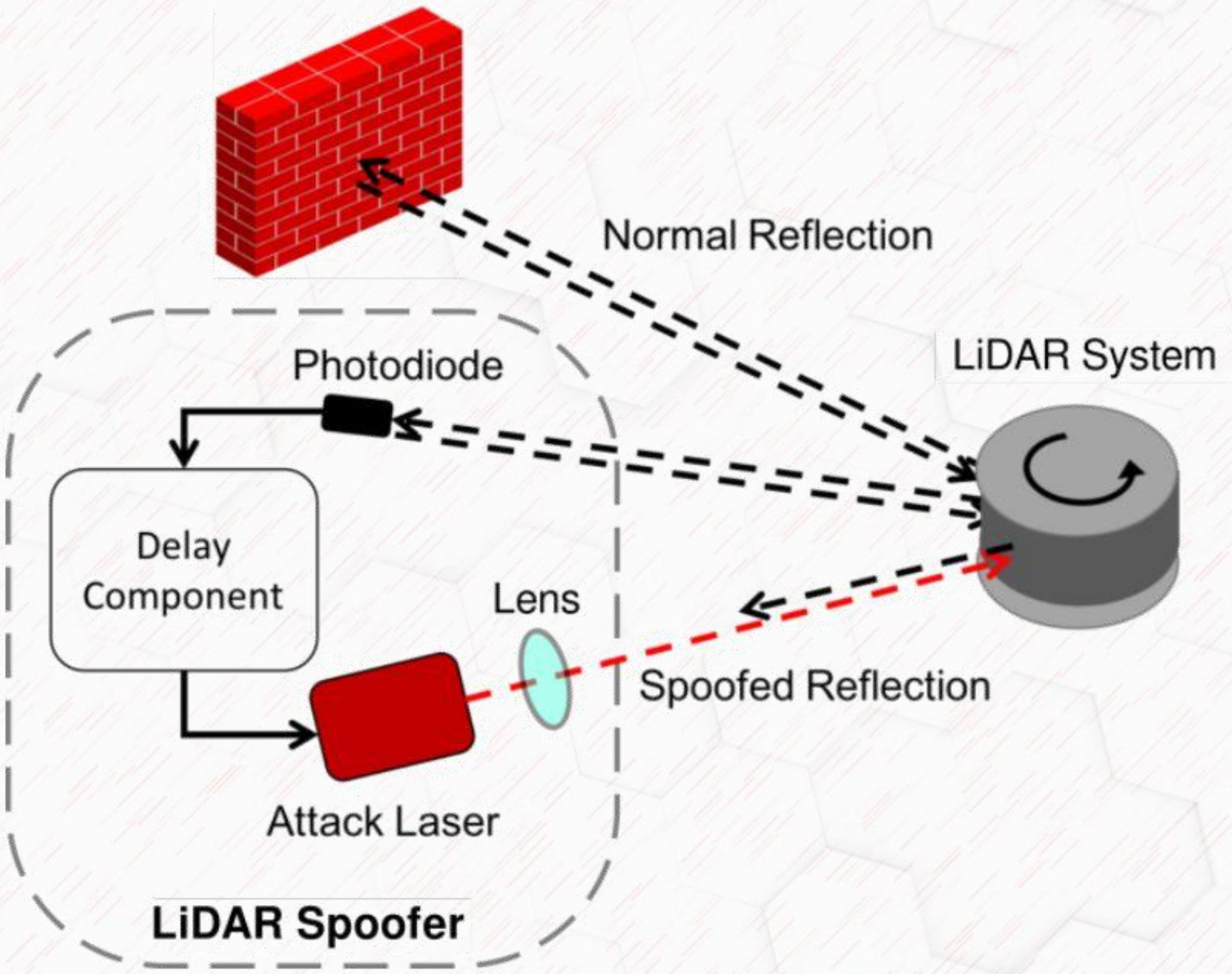
Quipeng, L. et al. (2019)

What is at risk?



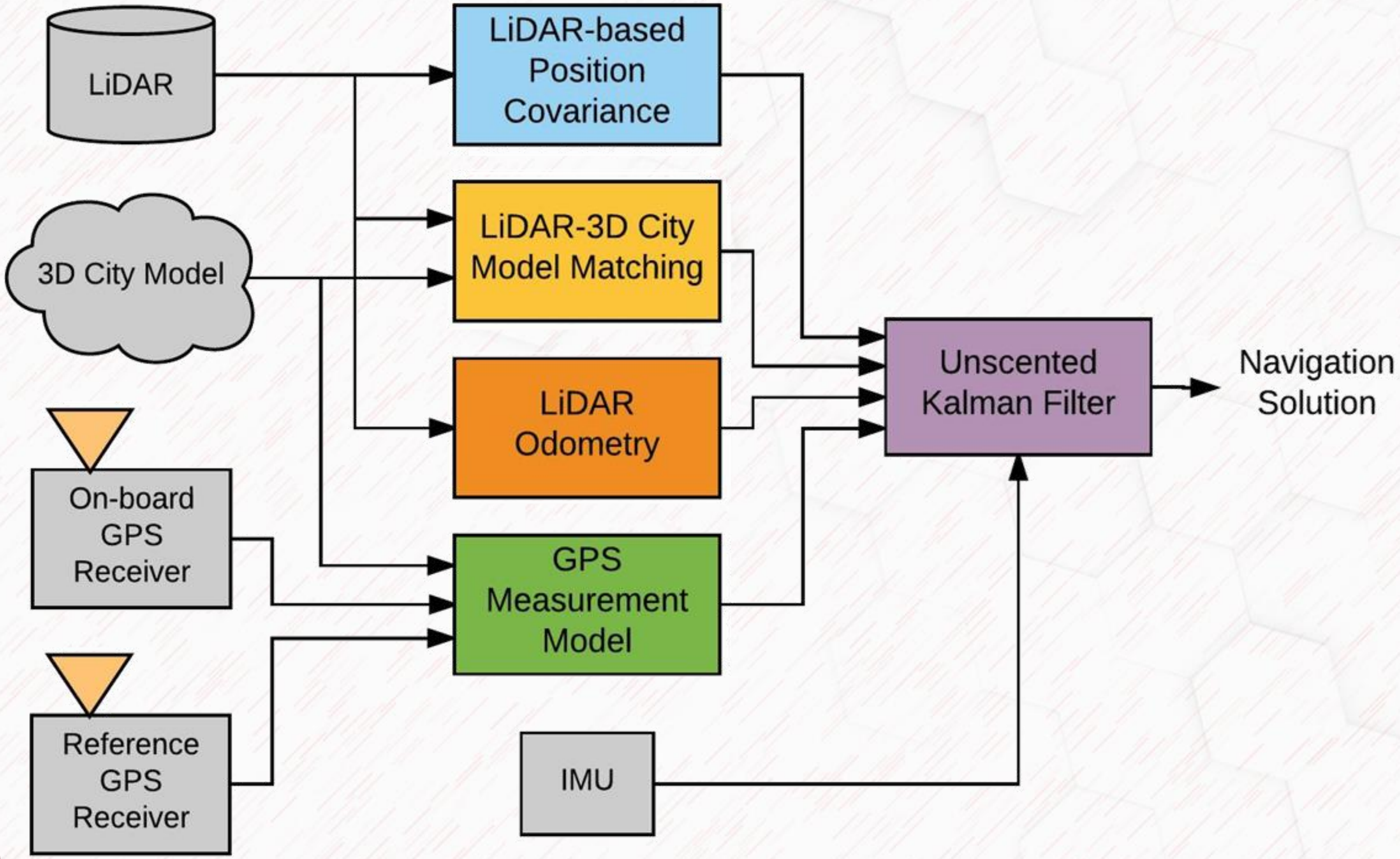
GPS spoofing can create serious problems in Autonomous systems, even life-threatening ones!

What is at risk?



LIDAR spoofing can create serious problems in Autonomous systems, even life-threatening ones!

What role does sensor fusion play in pose estimation?



Pose estimation utilizes position and orientation to predict and track the location of an AV

What question(s) does this study answer?

The necessity of multiple sensors correctly estimating pose in autonomous systems is clear…

But how do we guarantee a fail-safe pose estimation using sensor fusion?

What does the research propose?

- Proposed a model-based anomaly detection method.
- By comparing received sensor data to predictions based on the system mathematical model, determine if the sensor is compromised or not.
- GPS spoofing and LIDAR replay attacks are the two scenarios considered
- AV is assumed to use an extended Kalman filter (EKF) to fuse sensor measurements from GPS, LIDAR, IMU and estimate its own pose (including position and orientation).
- Designed a cumulative sum (CUSUM) detector based on the EKF residual, which can identify the exact sensor that is being attacked, and then reconfigured to estimate the secure pose of AV even in the face of cyber attacks.

Methodology

Pose Estimation by EKF

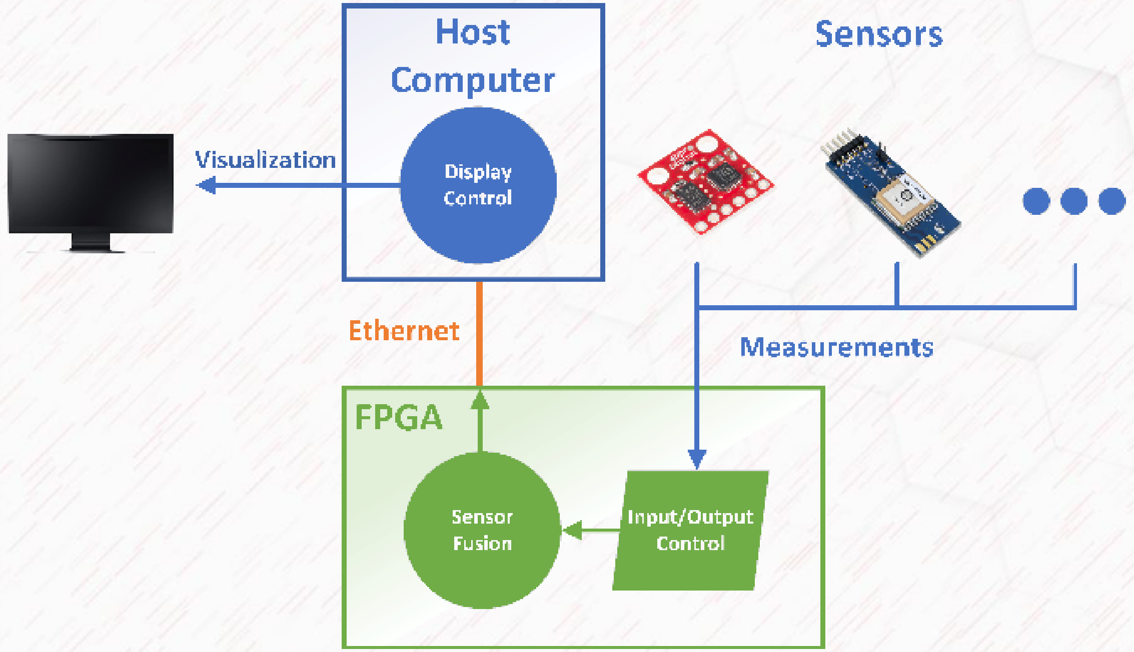
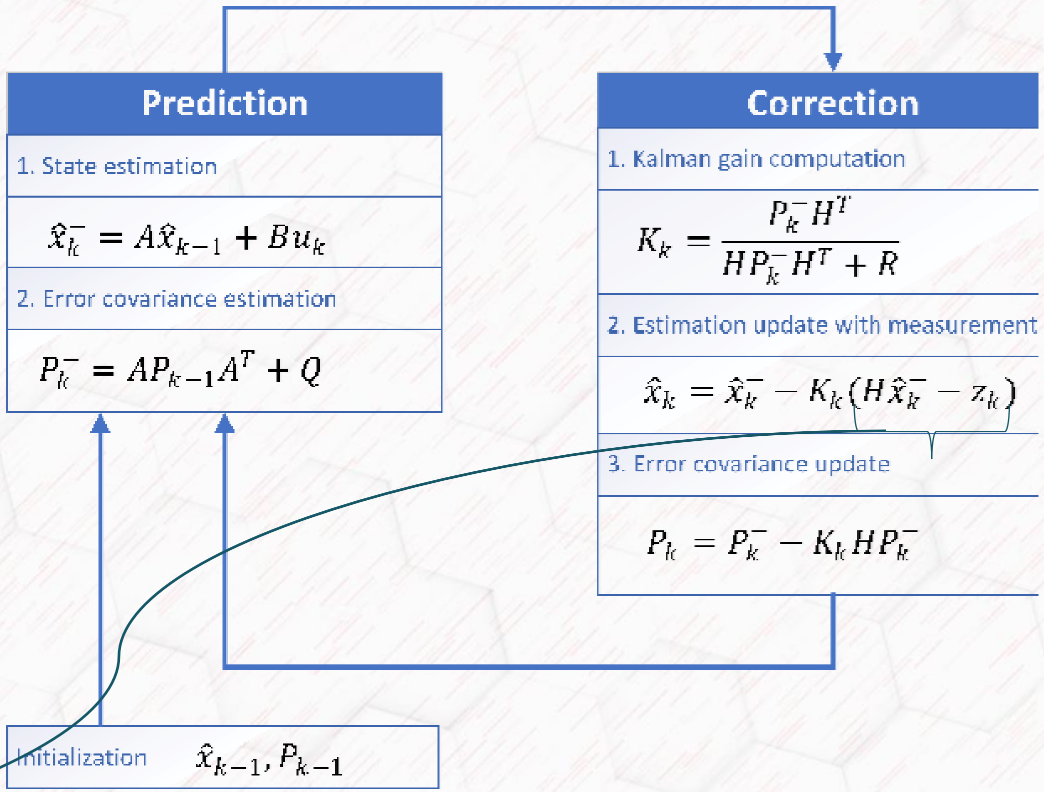


Fig. 1. Schematic diagram of the pose estimation system



r_{t_k}

EKF Residual

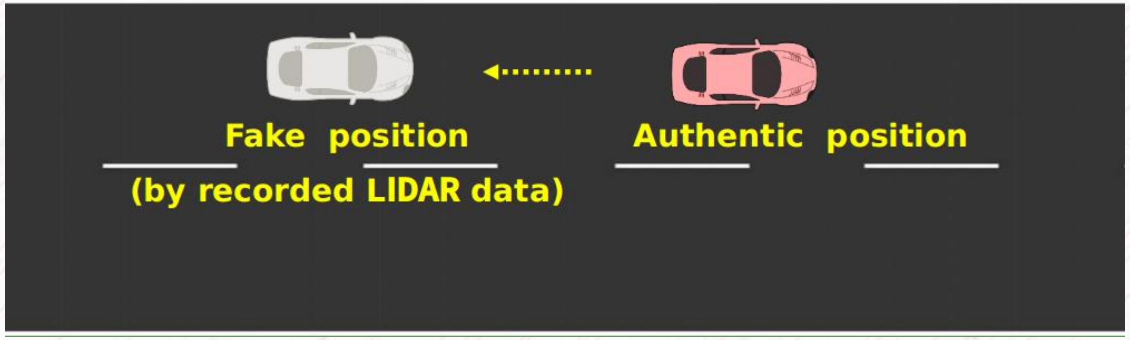
Attack Scenarios

A. *GPS Spoofing Attack*

- The attack is to add a fixed bias to the authentic GPS signal

- Assume the authentic position be $(x_a; y_a)$. By injecting a bias $(x_b; y_b)$, the final position indicated by the fake GPS signal is $(x_f ; y_f) = (x_a + x_b; y_a + y_b)$.

B. *LIDAR Replay Attack*



- The attacker continuously records the LIDAR measurements, and after T seconds, plays the measurements back to the vehicle.

- The indicated vehicle position is always later than the authentic position by T seconds.

CUSUM Detector for Sensor Attacks

- The residual $\boldsymbol{r}_{\boldsymbol{t_k}}$ serves as an indicator of the inconsistency between the state prediction and the measurement.

- The detector monitors the cumulative sum (CUSUM) of the residual for a period and see if the residual is greater than a threshold continuously.

- If the value is greater than a given threshold, it indicates that the predicted pose of the vehicle is inconsistent with the measurement.

$$\begin{cases} \text{Alarm} & \text{if } s(t_k) \geq \tau \\ \text{No Alarm} & \text{if } s(t_k) < \tau \end{cases}$$

Identification of the Compromised Sensor

DECISION MECHANISM OF SENSOR ATTACK SCENARIOS

CUSUM 1 (LIDAR+IMU)	CUSUM 2 (GPS+IMU)	CUSUM 3 (LIDAR+GPS+IMU)	Scenario
No Alarm	No Alarm	No Alarm	No Attack
No Alarm	No Alarm	Alarm	GPS Attack
No Alarm	Alarm	No Alarm	Impractical
No Alarm	Alarm	Alarm	GPS Attack
Alarm	No Alarm	No Alarm	Impractical
Alarm	No Alarm	Alarm	LIDAR Attack
Alarm	Alarm	No Alarm	Impractical
Alarm	Alarm	Alarm	Model Error

- To identify which sensor is attacked, they proposed three EKFs and their corresponding CUSUM detectors: one comprise of the three sensors, one only uses GPS and IMU measurements, and the third only uses LIDAR and IMU.

- For these three CUSUM detectors, they consider all possible alarm combinations and their corresponding attack scenarios

Identification of the Compromised Sensor

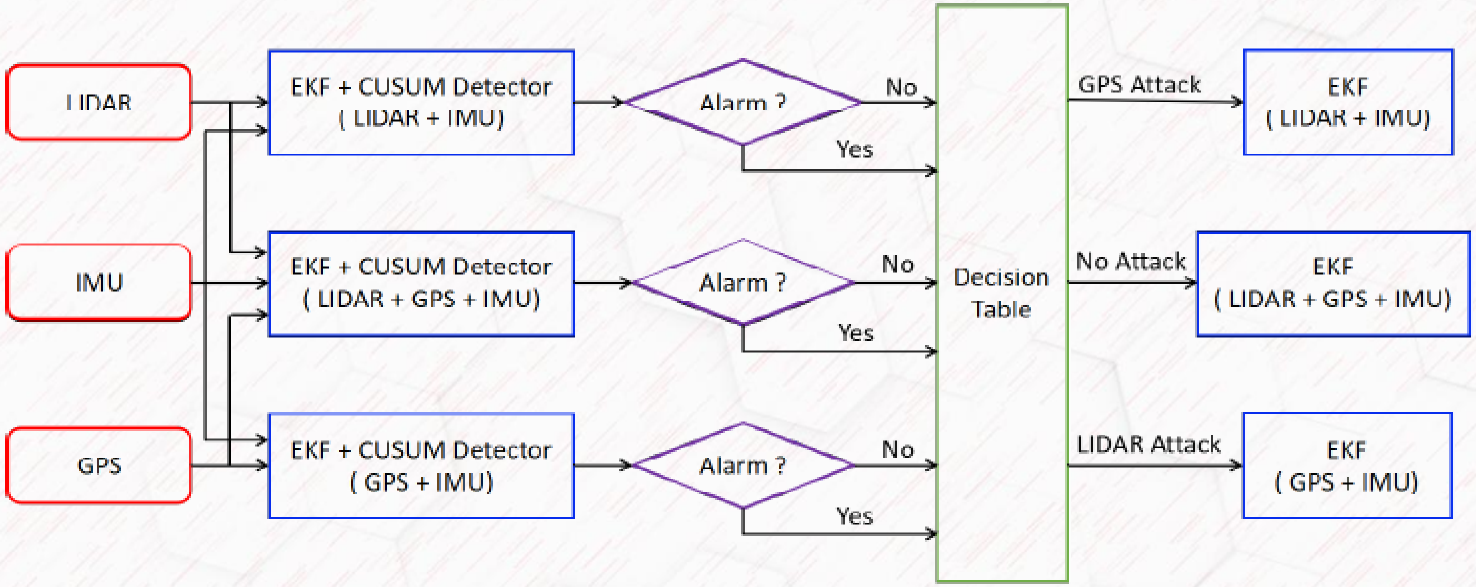


Fig. 4. Attack detection and EKF reconfiguration scheme

- If all CUSUM detector do not trigger any alarm, i.e., no attack occurs, use all measurements from the three sensors for pose estimation.
- If GPS attack is detected, discard measurements from GPS, and only LIDAR and IMU are used to estimate vehicle pose.
- If LIDAR attack is detected, discard measurements from LIDAR, and only GPS and IMU are used to estimate vehicle pose.

Evaluation/ Results

Evaluation tools

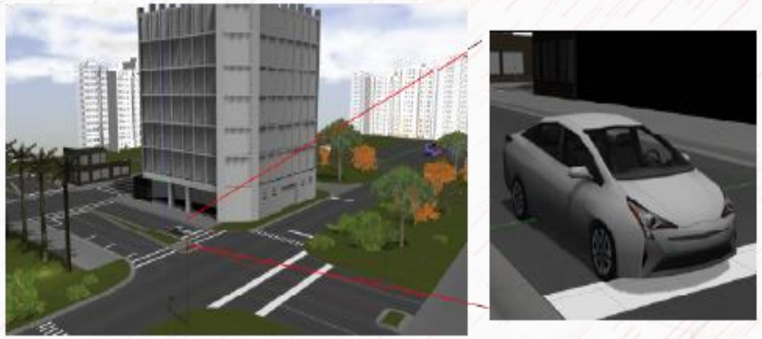


Fig. 5. Simulation platform. Left: simulated city. Right: simulated autonomous driving car

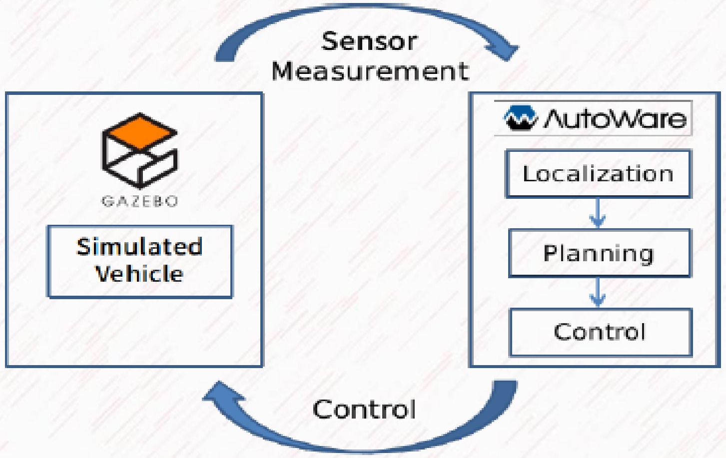


Fig. 6. Closed-loop test platform.

SIMULATION PARAMETERS

Parameters		Values	Units
Dist. from front wheel to c.g.	l_f	1.73	m
Dist. from rear wheel to c.g.	l_r	1.12	m
GPS spoofing bias	x_b	5	m
	y_b	0	m
LIDAR delay time	T^*	2	s
CUSUM detector 1	w	0.2	null
	τ	5	null
CUSUM detector 2	w	0.8	null
	τ	10	null
CUSUM detector 3	w	1	null
	τ	5	null

Results

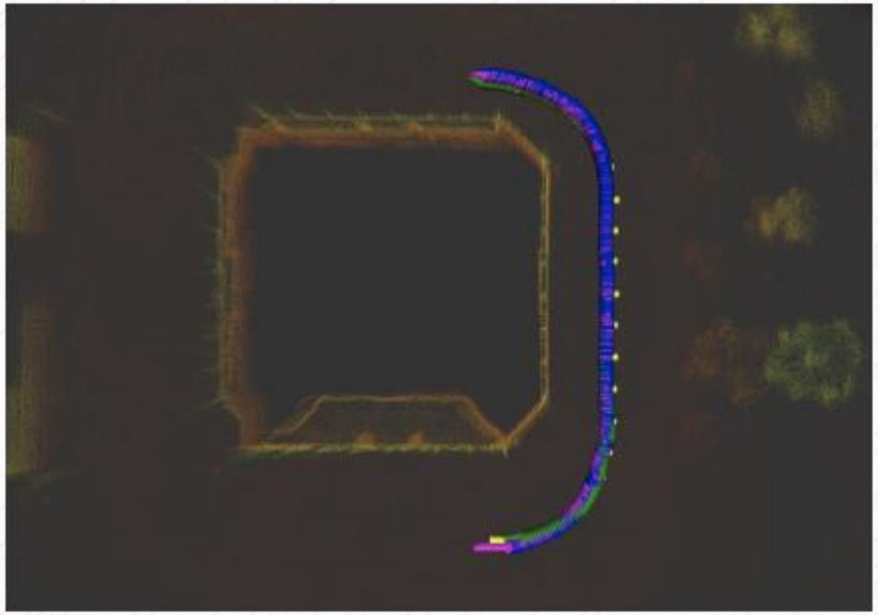


Fig. 8. Normal situation without any attack.

- Green arrow: the ground truth of the vehicle pose;
- Blue arrow: the pose indicated by LIDAR;
- Yellow points: the pose indicated by GPS. Note that GPS has no information about orientation. We only need to show its position.
- Purple arrow: the estimated pose by EKF.

The expected trajectory of the vehicle is a half circle from the bottom right to the top right. We can see that on the trajectory, poses from LIDAR, GPS, and EKF are all very close to the ground truth, which means that in the normal situation, the vehicle pose measurements and estimations are very accurate.

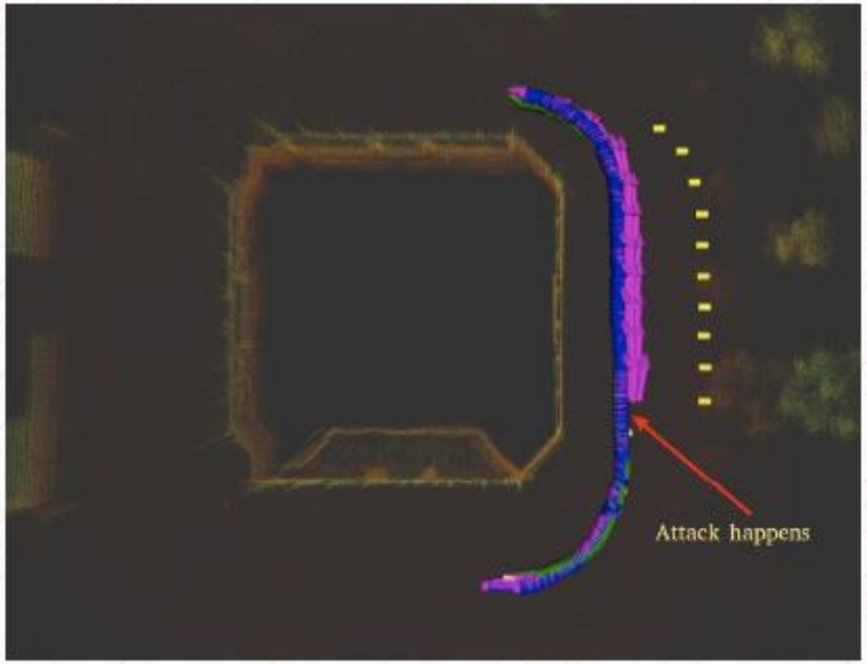


Fig. 9. GPS spoofing attack without CUSUM detection.

- Green arrow: the ground truth of the vehicle pose;
- Blue arrow: the pose indicated by LIDAR;
- Yellow points: the pose indicated by GPS. Note that GPS has no information about orientation. We only need to show its position.
- Purple arrow: the estimated pose by EKF.

The GPS measurements (yellow points) deviate from the ground truth by a fixed bias to the right. As a result, the estimated poses from EKF (purple arrows) also deviate from the ground truth. Since there is more weight on LIDAR measurements than GPS in the algorithm, the deviation of EKF estimation is not very large due to the correction effect of LIDAR measurements.

Results

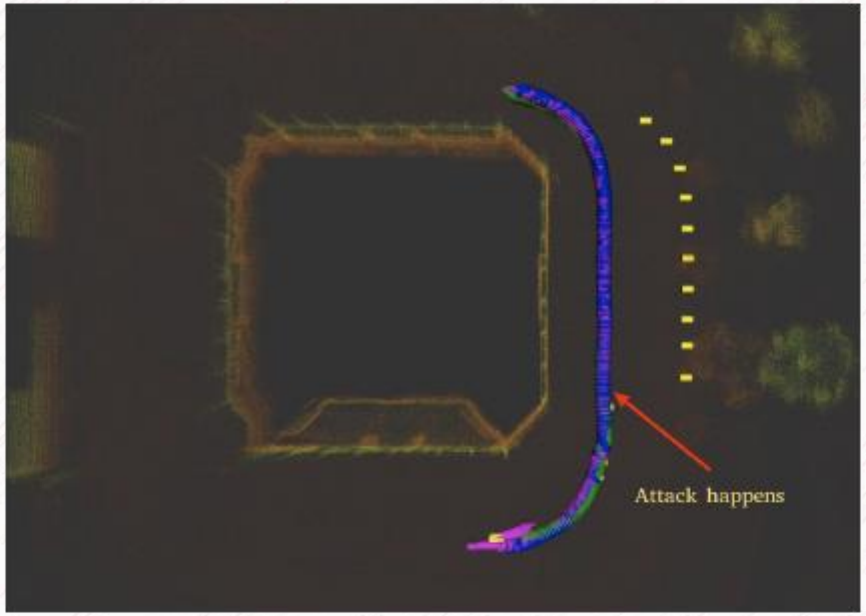


Fig. 10. GPS spoofing attack with CUSUM detection.

- Green arrow: the ground truth of the vehicle pose;
- Blue arrow: the pose indicated by LIDAR;
- Yellow points: the pose indicated by GPS. Note that GPS has no information about orientation. We only need to show its position.
- Purple arrow: the estimated pose by EKF.

- Even though GPS measurements (yellow points) deviate from the ground truth, the estimated poses by EKF (purple arrows) are not influenced by the attack. In fact, once the attack happens, an alarm is triggered indicating that GPS is being attacked. Thus, EKF ignores GPS measurements, and only uses LIDAR and IMU to estimate the vehicle pose

Results

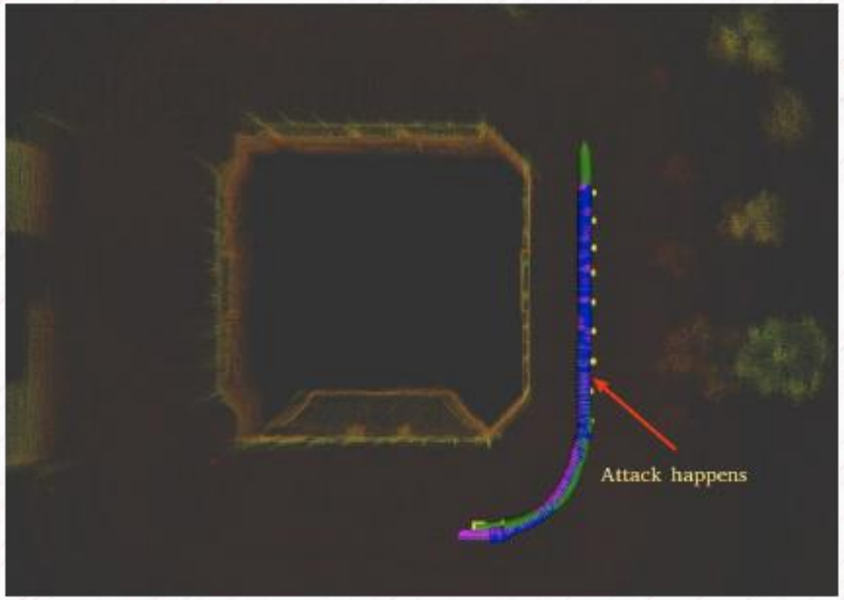


Fig. 11. LIDAR replay attack without CUSUM detection.

- Green arrow: the ground truth of the vehicle pose;
- Blue arrow: the pose indicated by LIDAR;
- Yellow points: the pose indicated by GPS. Note that GPS has no information about orientation. We only need to show its position.
- Purple arrow: the estimated pose by EKF.

LIDAR replay attack causes delay of the EKF estimated pose (purple arrow). From the figure we can see that the poses from LIDAR and EKF are apparently behind the ground truth (green arrow).

Results

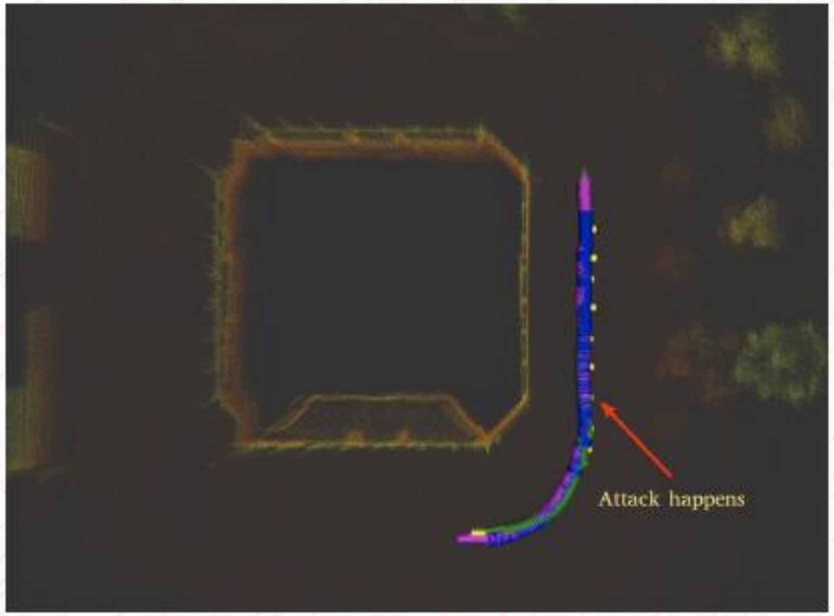


Fig. 12. LIDAR replay attack with CUSUM detection.

- Green arrow: the ground truth of the vehicle pose;
- Blue arrow: the pose indicated by LIDAR;
- Yellow points: the pose indicated by GPS. Note that GPS has no information about orientation. We only need to show its position.
- Purple arrow: the estimated pose by EKF.

This time even though the LIDAR measurements (blue arrow) are still behind the ground truth (green arrow) due to the replay attack, there is no delay in EKF estimated pose (purple arrow), because the detector finds out the LIDAR attack and discard the compromised measurements in pose estimation.

Conclusion and related works

Related works

Author(date)	Title	Summary of contribution	Implication
Wang Y. et al. (2021)	Detection and Isolation of Sensor Attacks for Autonomous Vehicles: Framework, Algorithms, and Validation	A model-based framework is proposed which can detect sensor attacks and identify their sources in order to achieve the secure localization of self-driving vehicles.	The authors improved on their previous work by considering more attack surfaces as well as introducing an auxiliary detector to monitor the inconsistences amongst multiple sensor measurements.
van Wyk F. et al. (2020)	Real-Time Sensor Anomaly Detection and Identification in Automated Vehicles	Developed an anomaly detection approach through combining a deep learning method, namely convolutional neural network (CNN), and Kalman filtering with a chi-square test detector, to detect and identify anomalous behavior in CAVs.	The data driven approach is unable to identify the sensor(s) under attack.
Yang T. (2020)	A Secure Sensor Fusion Framework for Connected and Automated Vehicles under Sensor Attacks	They proposed a sensor fusion algorithm for providing a robust estimate of the correct sensor information with bounded errors independent of the attack signals, and for attack detection and isolation.	The proposed sensor fusion framework is applicable to a large class of security-critical CPSs.

Conclusion

- The authors conducted an investigation to address the vulnerability of EKF to sensor attacks, such as GPS spoofing attack and LIDAR replay attack, which can seriously mislead the estimated vehicle Pose while fusing the different inputs.

- They ascertained the feasibility and effectiveness of the proposed approach through experiments on a simulation platform with different types of attack scenarios.

Paper Critique/Discussions

Any loopholes in the proposed scheme?

What are the ways this work can be extended?

How can we attack the proposed system?

1. No more than 1 sensor can be attacked at a time. How true can this assumption be?

2. Using only a single threshold could lead to false alarms? How is the threshold even determined?

3. The issue of mitigating the effects of the attack is not investigated?

4. How will the system deal with stealthy attacks?

   Attackers could inject a sequence of false information into the authentic GPS measurements; each piece of false information alone may not lead to a large enough difference to trigger the alarm, but these errors together could successfully deviate the vehicle.

5. Conducting a real-time implementation of the proposed attack detection scheme in a real AV?