Secure Pose Estimation for Autonomous Vehicles under Cyber Attacks

Qipeng Liu[1], Yilin Mo[2], Xiaoyu Mo[2], Chen Lv[2], Ehsan Mihankhah[1], and Danwei Wang[1]

[1]Nanyang Technological University, [2]Tsinghua University
2019 IEEE Intelligent Vehicles Symposium (IV)

Jonathan Lee, Secure Autonomous Systems, December 5th 2022

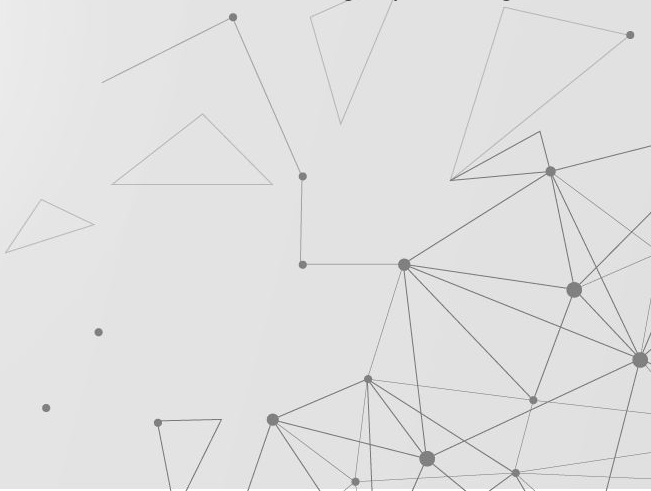
MOTIVATION

Attacks

- Network attacks - V2V
- Vehicle software - CAN bus, remote entry
- Manipulate sensor data - Adversarial signs

Defenses

- Misbehavior detection - other agents
- Cryptography - encryption, device security
- Inconsistent data - sensor fingerprinting



APPROACH

GOAL

Secure localization of an autonomous vehicle under sensor attacks.

- GPS
- LIDAR
- IMU

EKF & CUMSUM detector

Monitor inconsistency between predicted pose and sensor measurement.

- Extended Kalman filter (EKF) to fuse sensor data
- **Cumulative Sum detector** - monitor inconsistency between predicted pose and sensor measurement

POSE ESTIMATION - MODEL

- Kinematic bicycle model: inputs steering angle δ_f and acceleration α.

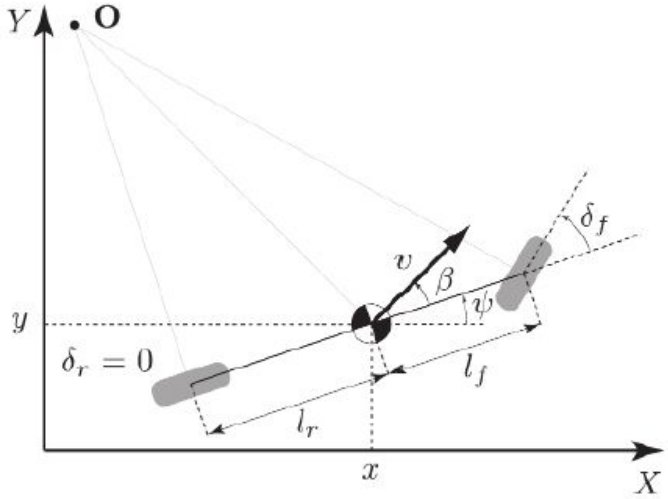


Fig. 1. Kinematic Bicycle Model

$$\dot{x} = v\cos(\psi + \beta) \tag{1a}$$

$$\dot{y} = v\sin(\psi + \beta) \tag{1b}$$

$$\dot{\psi} = \frac{v}{l_r}\sin(\beta) \tag{1c}$$

$$\dot{v} = a \tag{1d}$$

$$\beta = \tan^{-1}\left(\frac{l_r}{l_f + l_r}\tan(\delta_f)\right) \tag{1e}$$

β is the angle of the vehicle's velocity

POSE ESTIMATION - EKF

- Typical to use Kalman filter & variants for data fusion, using extended Kalman filter to handle nonlinearity
- **Step 1:** Prediction using mathematical model
  1. Predict vehicle pose at t_k, denoted by $\dot{X}$, by using equation 2.
  2. The difference between the prediction and real state is captured by $\dot{P}$

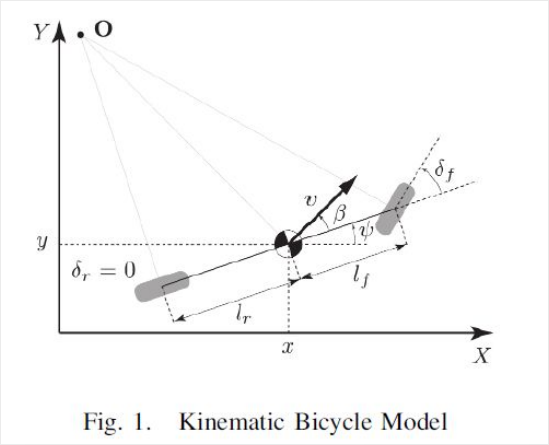


Fig. 1. Kinematic Bicycle Model

$$\dot{X}(t) = f(X(t), u(t)) \tag{2}$$

where states $X = [x, y, \psi, v]^T$, control inputs $u = [\beta, a]^T$, and f is the nonlinear function reproducing Eq. (1).

the real state can be captured by a covariance matrix $P(t_k)$ which is the solution of the following equation at time t_k

$$\dot{P}(t) = F(t)P(t) + P(t)F(t)^T + Q, \tag{3}$$

where $F(t)$ is the Jacobian matrix of f with respect to $\hat{X}(t)$, and Q is the covariance matrix of the process noise.

POSE ESTIMATION - EKF

- Typical to use Kalman filter & variants for data fusion, using extended Kalman filter to handle nonlinearity
- **Step 2:** Correction using sensor measurement
  1. Compute residual between state and sensor measurements
  2. Update the final estimation of vehicle state by adding the product of Kalman gain and residual
  3. The Kalman gain proportional to sensor data.

A variable $r(t_k)$ called residual is computed to represent the difference between the predicted and the real measurement:

$$r(t_k) = y(t_k) - C\hat{X}(t_k) \tag{4}$$

With residual $r(t_k)$ in hand, we can update our previous prediction by using the following equation:

$$\hat{X}^{+}(t_k) = \hat{X}(t_k) + K(t_k)r(t_k) \tag{8}$$

where $\hat{X}^{+}(t_k)$ is the final estimation of the vehicle pose; $K(t_k)$ is Kalman gain, which is computed by:

$$K(t_k) = P(t_k)C^T(CP(t_k)C^T + R)^{-1} \tag{9}$$

ATTACK SCENARIOS

1. **GPS Spoofing Attack:** GPS message modified by attacker to indicate fake position of the vehicle. Specifically some offset from genuine position.

2. **LIDAR Replay Attack:** Attacker continuously records LIDAR measurements and plays it back to the vehicle (position is delayed).

CUMSUM DETECTOR

Monitor EKF and find out which sensor is under attack, and reconfigure the EKF.

- Naive method: monitor the residual between state prediction and measurement
  - Might be triggered by measurement noise
- Better method: monitor residual for a period, and continuously check if it is greater than a threshold (cumulative sum).

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

IDENTIFY COMPROMISED SENSOR

Additional two EKFs and corresponding CUMSUM detectors:

- GPS + IMU
- LIDAR + IMU

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

Assume at most one of GPS and LIDAR might be attacked

EKF RECONFIGURATION

Use only good measurements in the pose estimation.

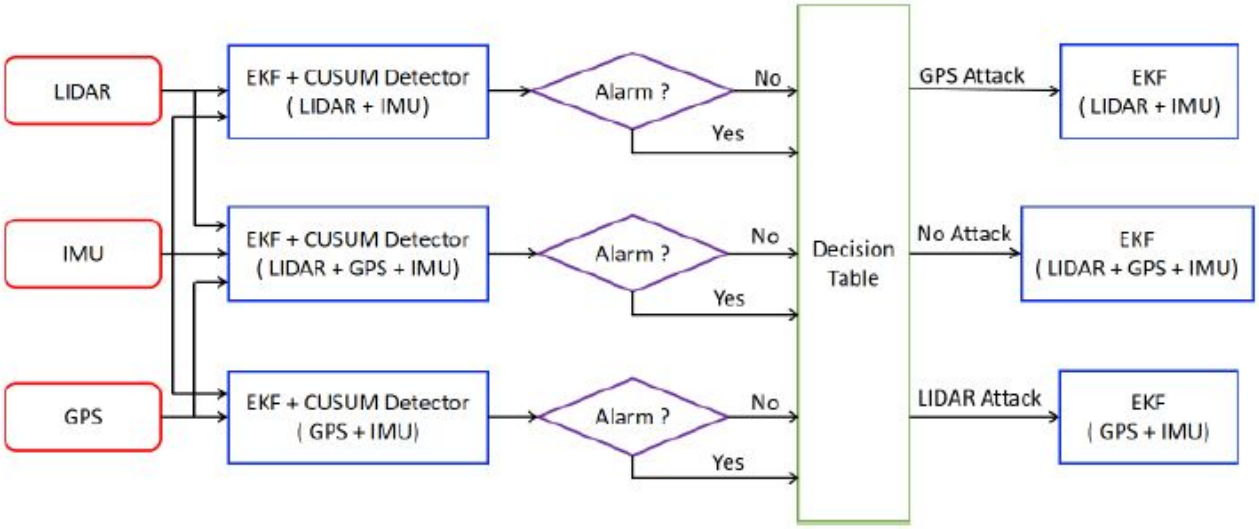


Fig. 4. Attack detection and EKF reconfiguration scheme

EXPERIMENTS

Test platform:

- Autoware: ROS-based open-source platform for testing self-driving in cities.
- Gazebo: robot simulation platform
- Equip simulated car with GPS, LIDAR, and IMU plugins
- Gazebo provides sensor measurements to Autoware, Autoware sends control commands back to Gazebo to simulate driving.

RESULTS

Experiment on scene with a building and trees.

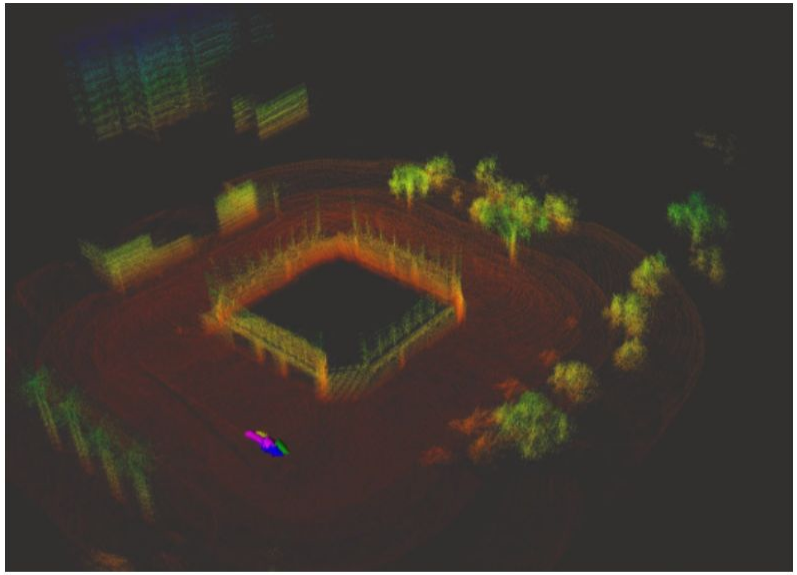


Fig. 7. Test environment shown in Rviz.

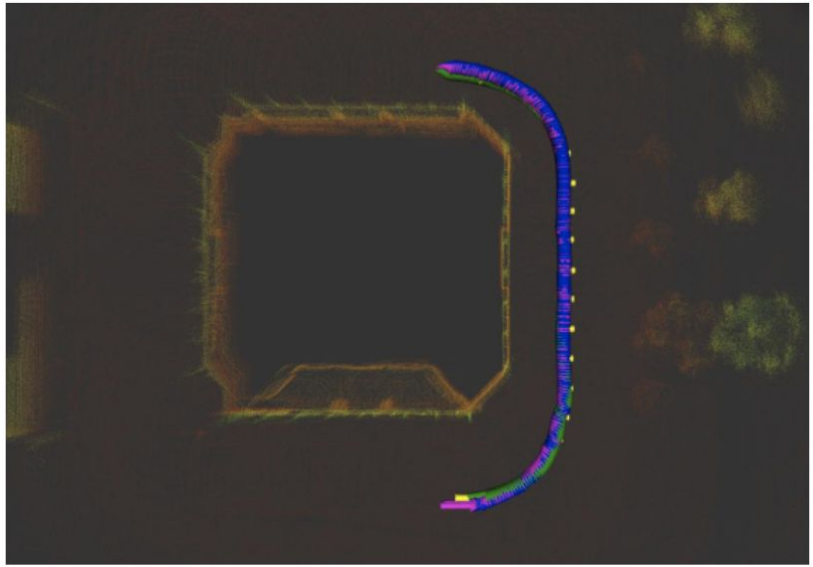
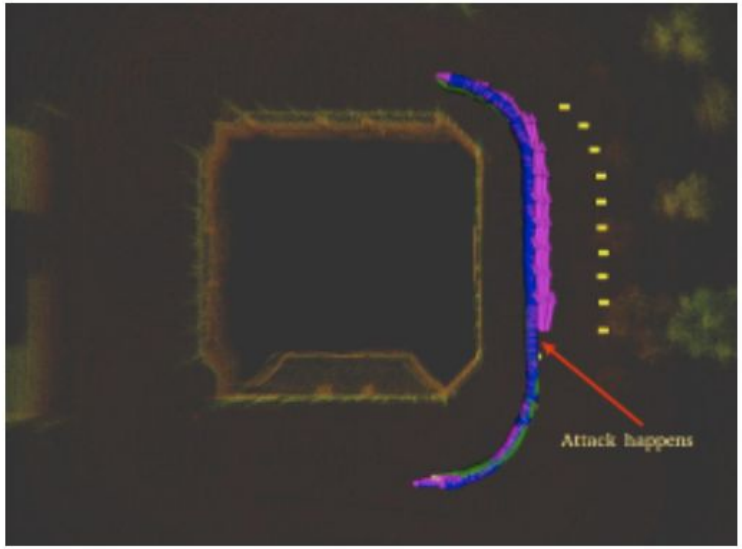


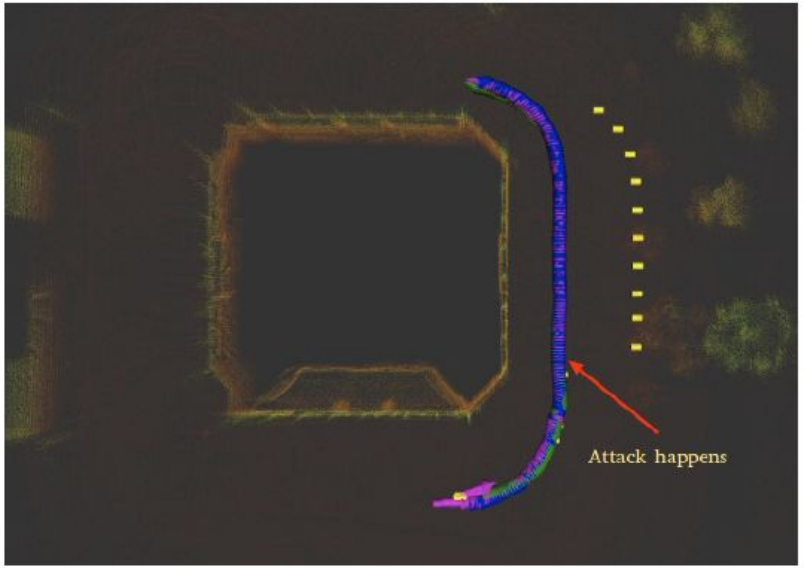
Fig. 8. Normal situation without any attack.

GPS SPOOFING ATTACK

Attacker adds a constant offset/bias to the GPS measurements.



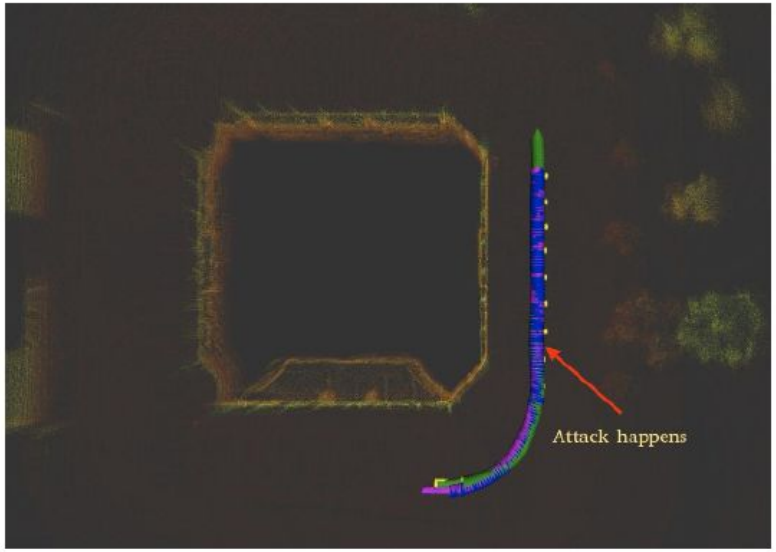
GPS spoofing attack without CUSUM detection.



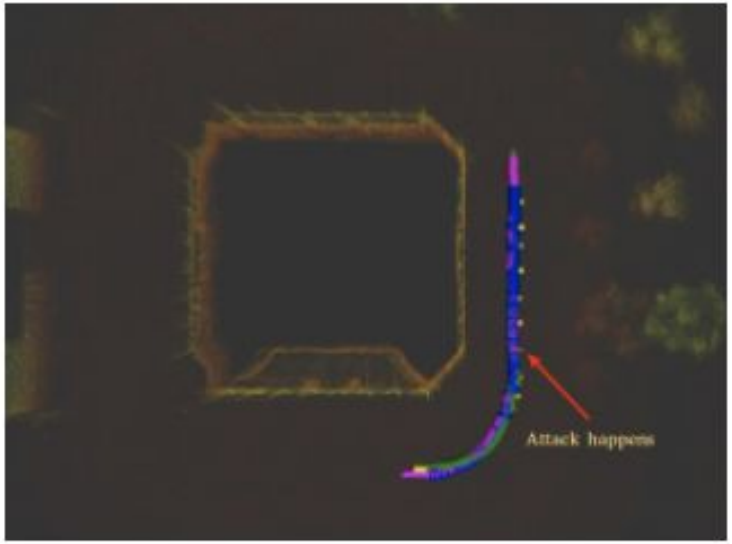
0. GPS spoofing attack with CUSUM detection

LIDAR REPLAY ATTACK

Attacker delays LIDAR measurements by 2 seconds.



1. LIDAR replay attack without CUSUM detection.



2. LIDAR replay attack with CUSUM detection.

Questions?

DISCUSSION

- The authors consider only GPS offset and LIDAR replay attacks. What other attacks might be effective using these sensors?
- The authors assume the car is equipped with GPS, LiDAR, and IMU. Tesla does not use LiDAR in their cars. Do you think the absence of LiDAR and RADAR makes cars more vulnerable or more resilient to attacks?

CLOSING THOUGHTS

Reject

- Limited testing/results presented.
  - Only one scenario of each type of attack.
  - One experiment is not statistically significant
- No related work section.
  - How does this compare to other approaches?
  - What is the metric for success?
- Strong assumptions.
  - Only one sensor attacked at a time
  - GPS, LIDAR, IMU required