

# MCC-EKF for Autonomous Car Security

Authors: Ashutosh Singandhupe, Hung Manh La

# MCC-EKF for Autonomous Car Security

- ◇ 2020 Fourth IEEE International Conference on Robotic Computing (IRC)
- ◇ Authors: Ashutosh Singandhupe (PhD Fall 2021), Hung Manh La (Associate Professor)
- ◇ Advanced Robotics and Automation (ARA) Lab, Department of Computer Science and Engineering, University of Nevada, Reno

# General Overview

- ◇ Motivation: Prevent the autonomous system to change its estimated trajectory when an attack happens
- ◇ Introduce MCC-EKF as a defense against attacks or shot noise
- ◇ Sensors: LiDAR and stereo camera
- ◇ Simulated in Gazebo
- ◇ Benchmarked using the KITTI dataset

# Problems

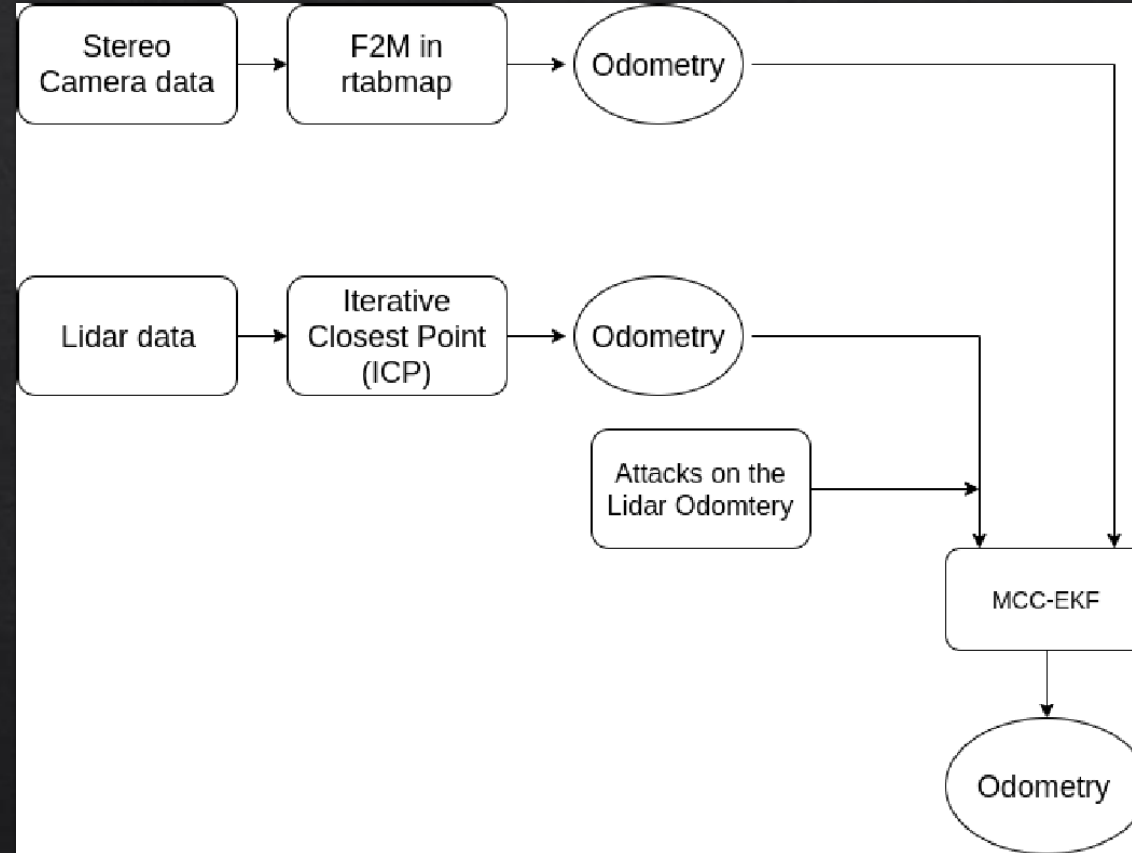
“Can we use the odometry information from two different Simultaneous Localization And Mapping (SLAM) algorithms to get a better estimate of the odometry?”

◇ “We focus on fusing odometries from Lidar-based SLAM and Visual based SLAM using the Extended Kalman Filter (EKF) algorithm”

“What if one of the SLAM algorithms gets affected by shot noise or by attack vectors, and can we resolve this situation?”

◇ “Introducing the Maximum Correntropy Criterion - Extended Kalman Filter (MCC-EKF), which assists in removing/minimizing shot noise or attack vectors injected into the system.”

# Concepts



\*F2M =Frame-To-Map

System Architecture

# Concepts

◇ MCC-EKF = Maximum Correntropy Criterion - Extended Kalman Filter

◇ Correntropy

◇  $X$  and  $y$  are 2 scalar variables

◇ Kernel function:  $\kappa\sigma$

$$V_\sigma(X, Y) = E[\kappa_\sigma(X - Y)].$$

◇ Correntropy with Kalman Filtering

◇ State vector:  $x_k$

◇ Measurement vector:  $y_k$

◇ System Noise:  $w_k$

◇ Measurement Noise:  $v_k$

◇  $F$  and  $H$  are the system matrix and the observation matrix

$$x_k = F * x_{k-1} + w_k$$

$$y_k = H * x_k + v_k$$

# Concepts

For initialization:

$$\hat{x}_0 = E[x_0] \quad (13)$$

$$P_0 = E[e_0 e_0^T] \quad (14)$$

where,  $e_0 = x_0 - \hat{x}_0$  is the error term, and  $E(\cdot)$  is the expected value operation. Prior estimation can be calculated as

$$\hat{x}_k^- = F \hat{x}_{k-1} \quad (15)$$

$$P_{k|k-1} = F P_{k-1|k-1} F^T + Q_k. \quad (16)$$

$$K_k = (P_{k|k-1}^{-1} + L_k * H^T * R_k^{-1} * H)^{-1} * L_k * H^T * R_k^{-1} \quad (18)$$

$$\hat{x}_k = \hat{x}_k^- + K_k (y_k - H * \hat{x}_k^-) \quad (19)$$

$$P_{k|k} = (I - K_k * H) * P_{k|k-1} * (I - K_k * H)^T + K_k * R_k * K_k^T. \quad (20)$$

$$L_k = \frac{G_\sigma(\|y_k' - H * \hat{x}_k\|_{R_k^{-1}})}{G_\sigma(\|\hat{x}_k - F * \hat{x}_{k-1}\|_{P_{k|k-1}^{-1}})}. \quad (24)$$

- ◇ “So when  $y_k$  is large as defined by the kernel bandwidth,  $L_k$  is 0, which forces the Kalman Gain  $K$  to be 0. So the next updated state is updated by the system state as given in Equ. (15). This process, as one can see, can reject the attacks/outliers thus securing the system”

# Concepts

---

**Result:** Computed odometry from MCC-EKF SLAM

Lidar Odom (ICP)  $\rightarrow L_o(x, y, z, r, p, y)$

Stereo Odom (F2M)  $\rightarrow S_o(x, y, z, r, p, y)$

Initialization;

Lidar odom  $\rightarrow (L_o)$

Stereo odom  $\rightarrow (S_o)$

Compute  $x_0$  from Equ. (13)

Compute  $P_0$  from Equ. (14)

Prior Estimation;

Compute  $\hat{x}_k^-$  from Equ. (15)

Compute  $P_{k|k-1}$  from Equ. (16)

**while** get  $L_o$  and  $S_o$ ;

**do**

    Compute  $L_k$  from Equ. (24)

    Compute Gain  $K_k$  from Equ. (18)

    Update state  $x_k$  from Equ. (19)

    Update  $P_{k|k}$  from Equ. (20)

**end**

---

MCC-EKF Algorithm



# Testing Environment

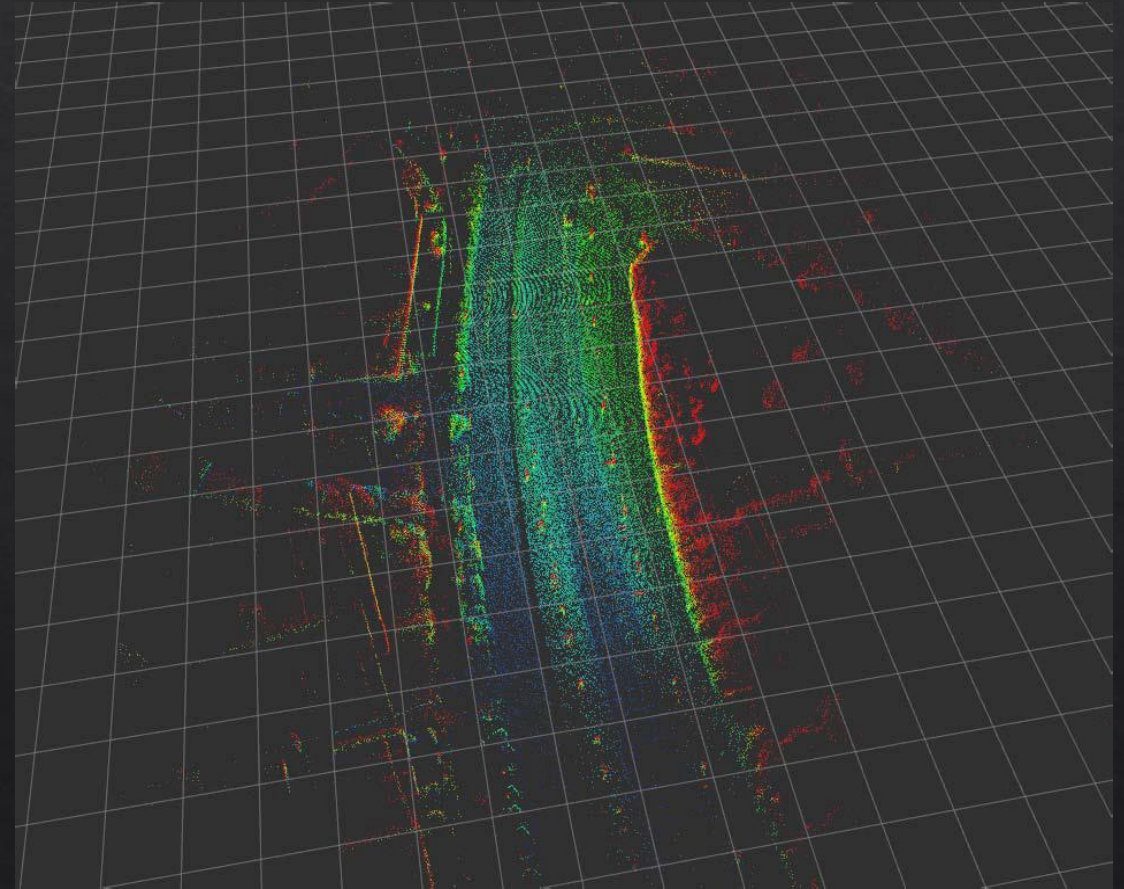


Gazebo Simulation Environment

# Testing Environment



KITTI dataset data (SEQ 11) Environment

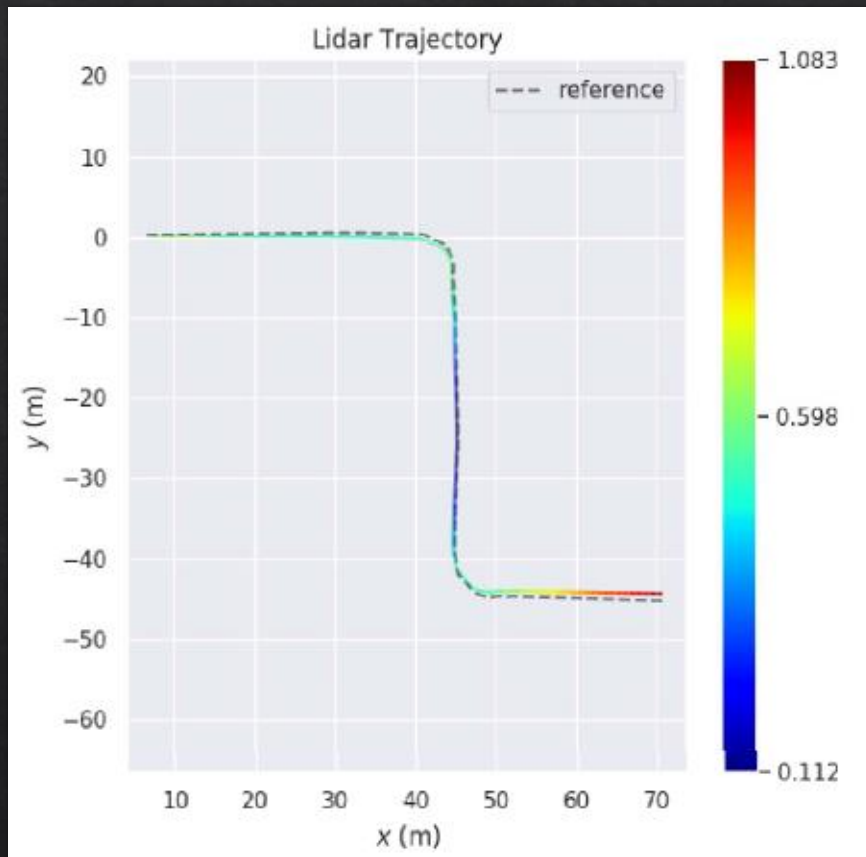


KITTI dataset data (SEQ 11) 3D Lidar Map

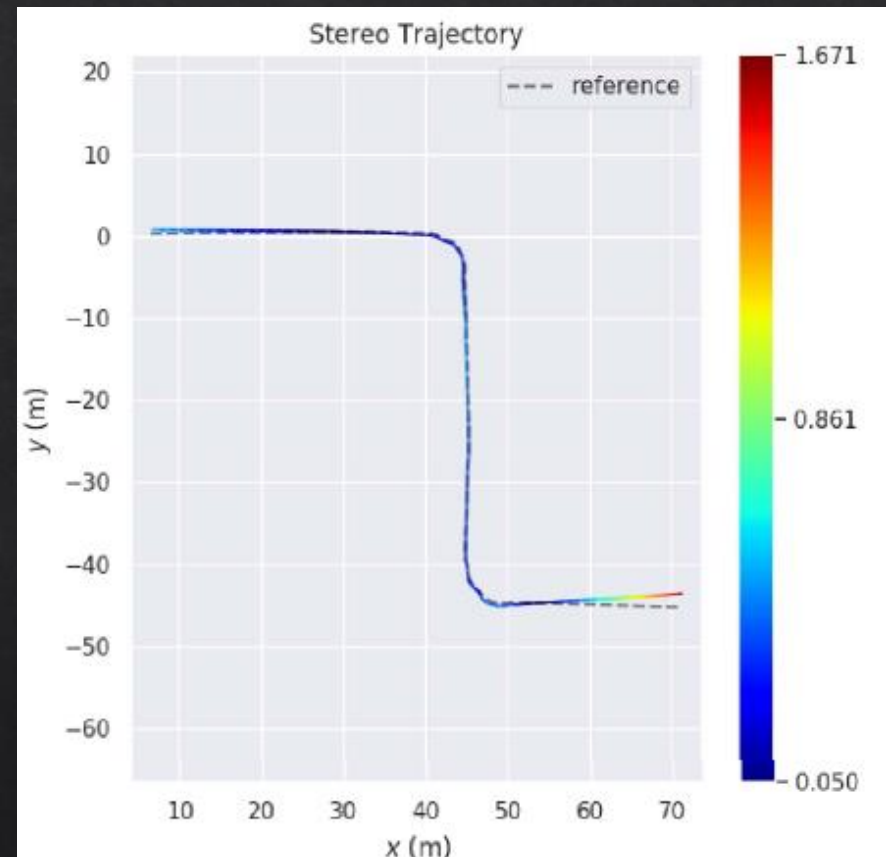
## KITTI Dataset Project:

- Karlsruhe Institute of Technology (KIT) and Toyota Technological Institute at Chicago (TTI-C)
- Datasets are captured by driving around the mid-size city of Karlsruhe
- <http://www.cvlibs.net/datasets/kitti/>

# Results

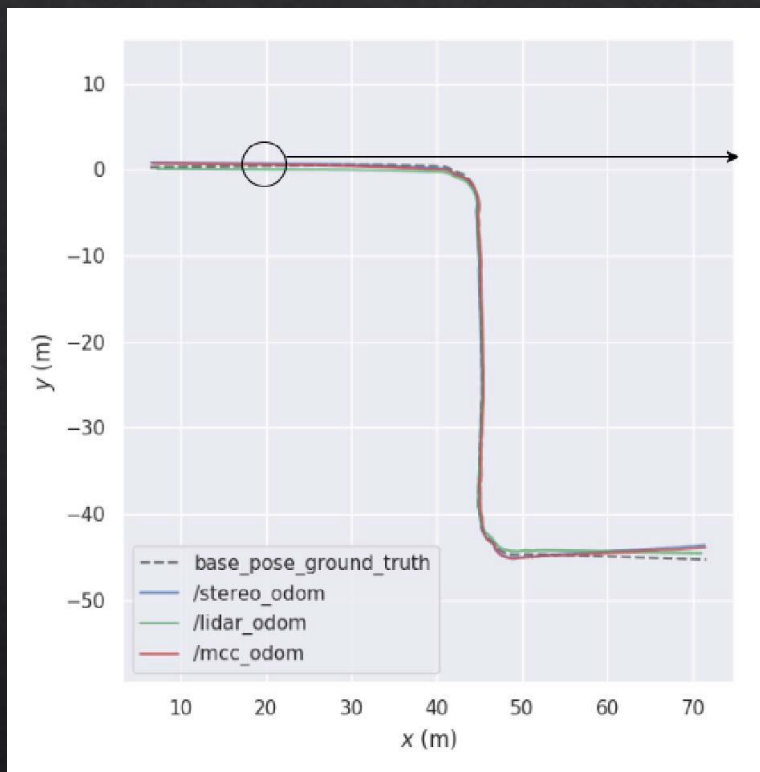


Lidar odometry

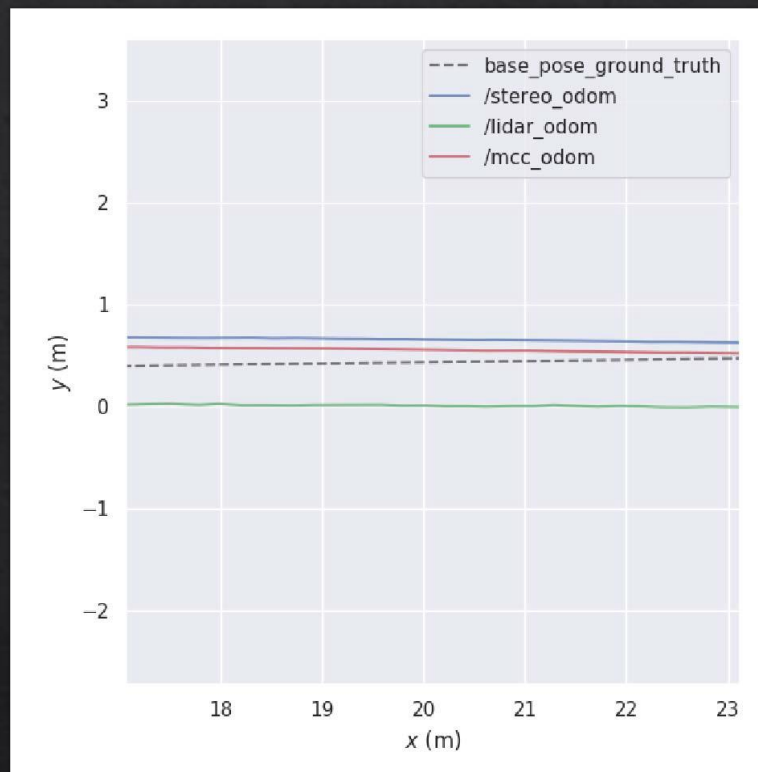


Stereo odometry

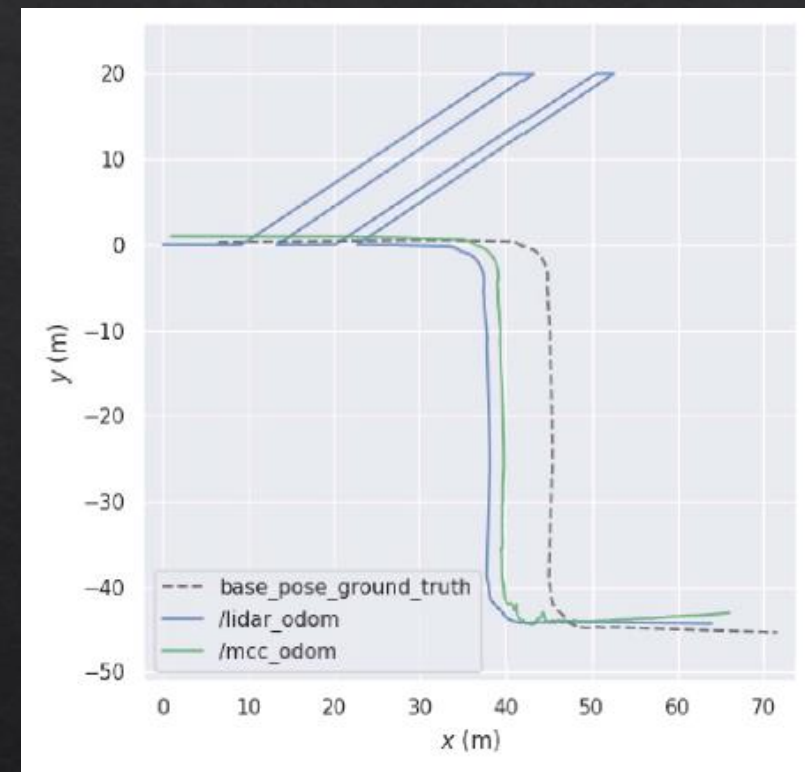
# Results



Odometry



Odometry (Zoom-in)



MCC-EKF response to attacks on Lidar data

# Results

	Traj 1	Traj 2
Stereo (RMSE)1	0.478404	1.840472
Lidar (RMSE)	0.557076	0.505731
MCC-EKF (RMSE)	0.419823	0.49761

RSME Comparison

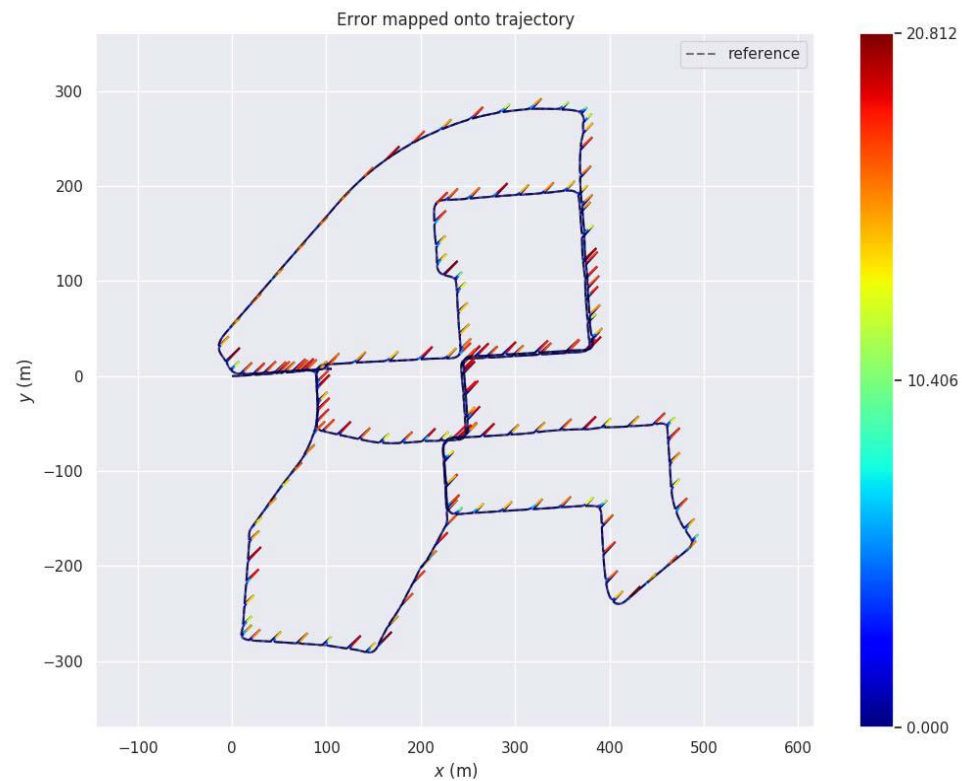
	Traj 1	Traj 2
Random attacks 1		
Normal EKF (RMSE)	3.624596	5.01472
MCC-EKF (RMSE)	0.420437	0.81037
Random attacks 2		
Normal EKF (RMSE)	4.624596	7.01472
MCC-EKF (RMSE)	0.43317	0.85132

RSME Comparison (after attack)

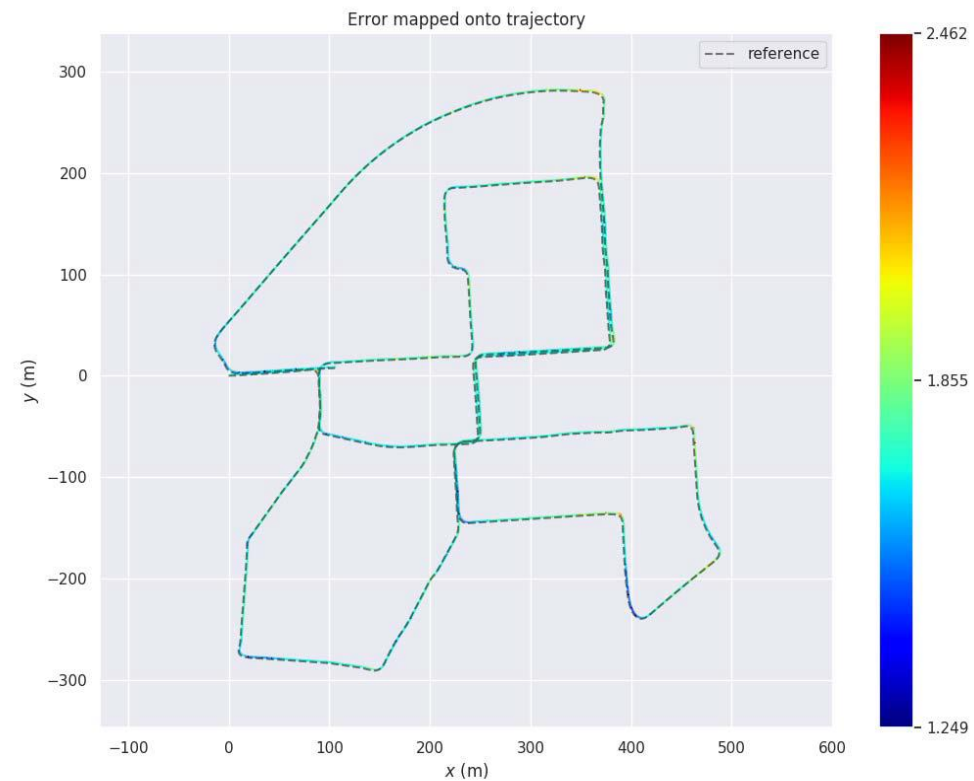
	SEQ 01	SEQ 05	SEQ 11	SEQ 27
Random attacks 1				
EKF	2.04	2.42	1.475	3.193625
MCC-EKF	0.0198	0.0073	0.110	0.142083
Random attacks 2				
EKF	3.79	7.0685	2.1875	4.1989
MCC-EKF	0.0198	0.092263	0.1842	0.1693

RSME Comparison on  
KITTI Dataset (after attack)

# Results

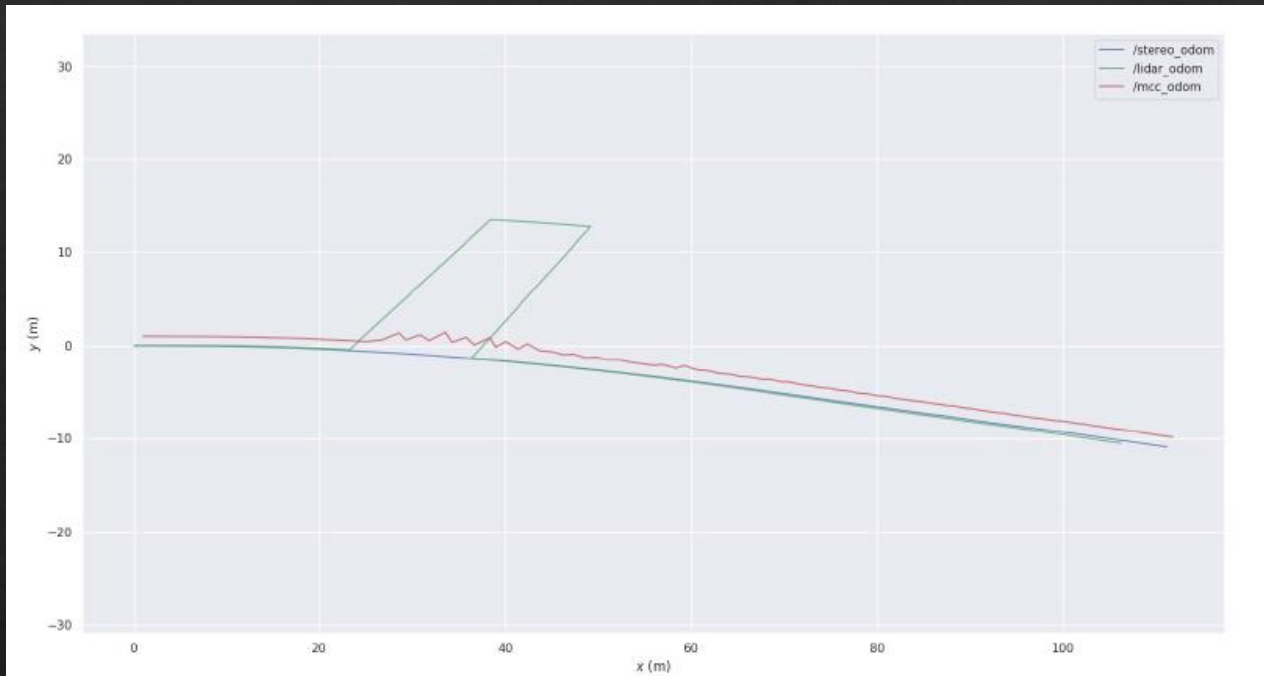


Normal EKF on KITTI dataset SEQ 27

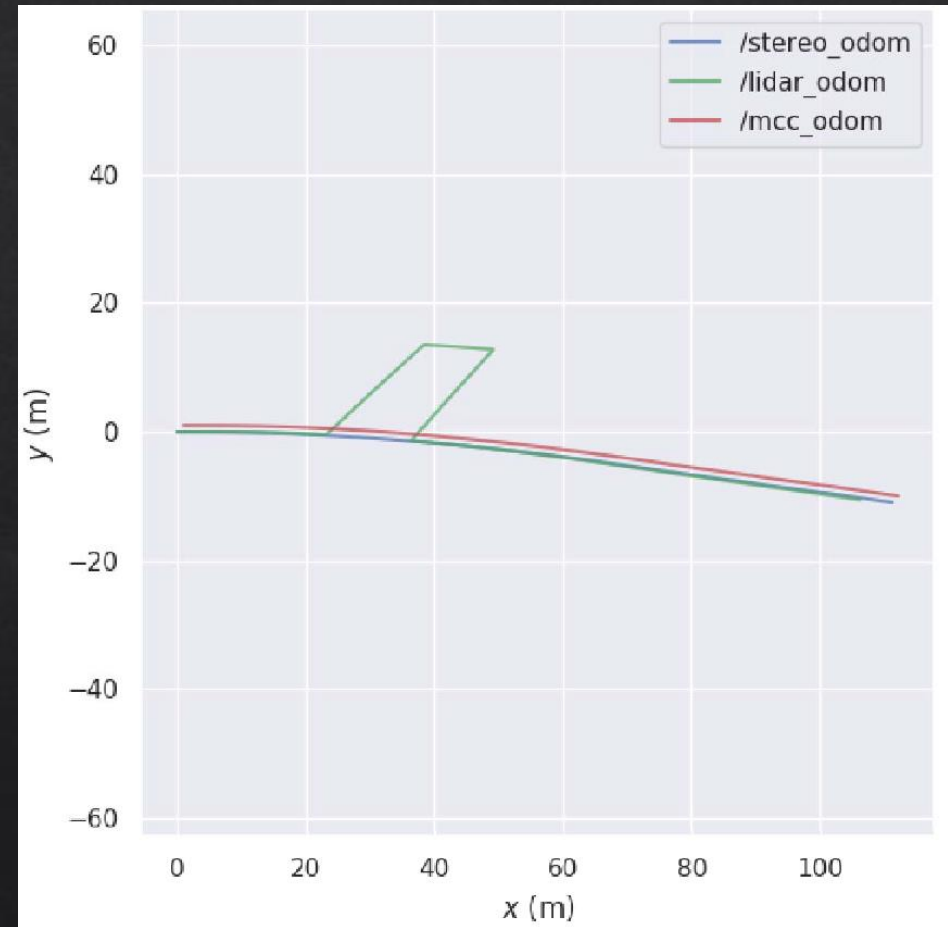


MCC-EKF on KITTI dataset SEQ 27

# Results



EKF response on KITTI dataset SEQ 01 (with attack)



MCC-EKF response on KITTI dataset SEQ 01 (with attack)

# Video



Advanced Robotics and Automation Lab

115 subscribers

SUBSCRIBE

HOME

VIDEOS

PLAYLISTS

CHANNELS

ABOUT



## Description

The Advanced Robotics and Automation (ARA) was established in July 2014 by Dr. Hung La. ARA Lab's mission statement is to discover, develop, implement innovative algorithms and methodologies as well as prototypes for robotics and automation systems, and their applications.

ARA Lab is located at the Advanced Research Facility (ARF) Building: ARF 118, ARF 120; and Edmund Cain Hall: CAIN 253A.

ARA Lab has various state-of-the-art equipment including motion capture system (from Motion Analysis), drones, mobile robots, Seekur Jr robot, steel bridge climbing robots, ground penetrating radar (GPR), Electrical Resistivity Probes, Laser scanners, LIDAR, Humanoid robots, Cameras, High Accuracy Novatel DGPS, IMUs, PCs, etc.

ARA Lab's research focus on the areas of autonomous systems, multi-robot systems, control systems, human-robot collaboration, and wearable computing. We would like to welcome any students who are interested in these exciting research areas.

Dr. Hung La, Computer Science, UNR

## Stats

Joined Jul 31, 2008

21,582 views



KITTI Sequence 27

Yellow Path shows the Lidar Odometry with attacks  
 Red Path shows the Normal EKF Odometry  
 Green Path shows the MCC-EKF Odometry

Displays

- Global Options
  - Fixed Frame: paths
  - Background Color: 48; 48; 48
  - Frame Rate: 30
  - Default Light:
- Global Status: ...
  - Fixed Frame: No tf data. Actual err...
- Grid
  -
- Path
  - 
  - Status: Ok
  - Topic: /lidar\_path
  - Unreliable:
  - Line Style: Lines
  - Color: 252; 233; 79
  - Alpha: 1
  - Buffer Length: 1
  - Offset: 0; 0; 0
  - Pose Style: None
  - Path
    - 
    - Topic: /stereo\_path

Image

No Image

Image

No Image

Views

Type: Orbit (rviz) Zero

Current View	Orbit (rviz)
Near Clip ...	0.01
Invert Z Axis	<input type="checkbox"/>
Target Fra...	<Fixed Frame>
Distance	79.607
Focal Shap...	0.05
Focal Shap...	<input checked="" type="checkbox"/>
Yaw	0.375396
Pitch	0.674796
Focal Point	0; 0; 0

Time

ROS Time: 1575084175.95    ROS Elapsed: 12.50    Wall Time: 1575084175.98    Wall Elapsed: 12.41

Reset

Experimental     31 fps

# Related Publications

- ◇ Sehgal, A. *et al.* (2019) 'Lidar-Monocular Visual Odometry with Genetic Algorithm for Parameter Optimization', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 11845 LNCS, pp. 358–370. doi: 10.1007/978-3-030-33723-0\_29.
- ◇ Singandhupe, A. and La, H. (2019) 'A Review of SLAM Techniques and Security in Autonomous Driving', *Proceedings - 3rd IEEE International Conference on Robotic Computing, IRC 2019*, (19), pp. 602–607. doi: 10.1109/IRC.2019.00122.

# Discussion

- ◇ Is the upgrade from normal EKF to MCC-EKF worth it?
- ◇ Would it still be an improvement (from EKF to MCC-EKF) if the GPS was used in the KITTI benchmark?
- ◇ Is there a better data fusion method for this scenario?

# Links

- ◇ Paper Link: [https://ara.cse.unr.edu/wp-content/uploads/2014/12/IEEE\\_IRC2020\\_Ashu.pdf](https://ara.cse.unr.edu/wp-content/uploads/2014/12/IEEE_IRC2020_Ashu.pdf)
- ◇ YouTube Video: <https://www.youtube.com/watch?v=bKzN8NdQnaE>
- ◇ ARA Lab Website: <https://ara.cse.unr.edu/>
- ◇ GitHub: <https://github.com/aralab-unr/MCC-EKF-SLAM>
- ◇ Gazebo: <http://gazebo.org/>
- ◇ KITTI database: <http://www.cvlibs.net/datasets/kitti/>