Mert D. Pesé, Xiaoying Pu, and Kang G. Shin

SPy: Car Steering Reveals Your Trip Route!

Privacy Enhancing Technology Symposium (PETS 2020)
7/14/2020

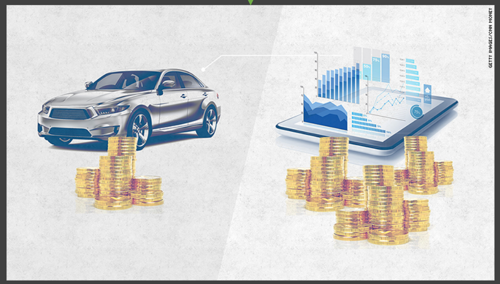
CSE COMPUTER SCIENCE AND ENGINEERING UNIVERSITY OF MICHIGAN

REAL-TIME COMPUTING LABORATORY @ UNIVERSITY OF MICHIGAN, ANN ARBOR

Vehicles are getting increasingly connected

Data Connectivity

- 2016: 20%
- 2020: 75%
- 2021: 98%



Revenue through Advertisements and Third-Party Apps

Who collects what data?

BMW CarData

Mercedes me

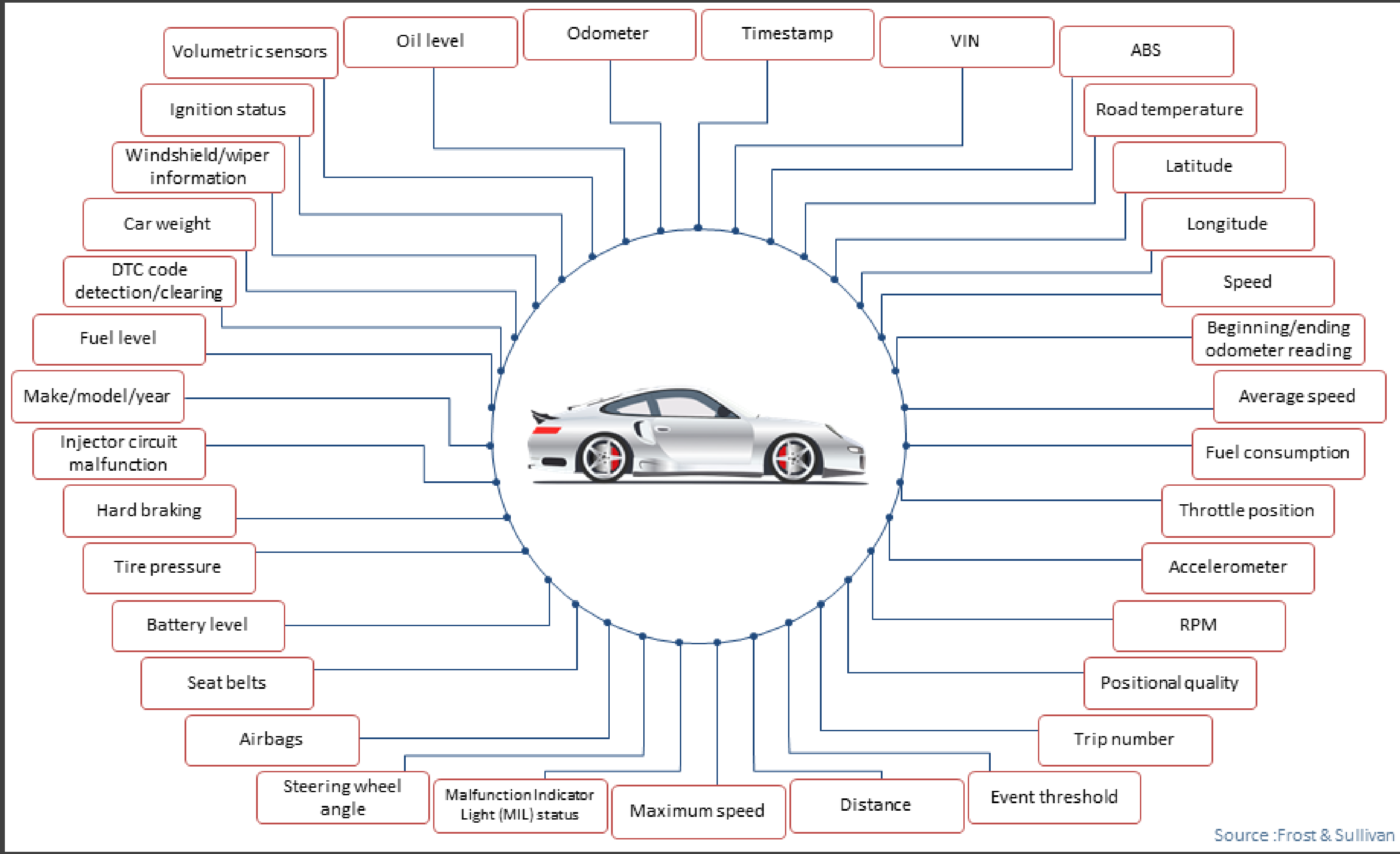
PROGRESSIVE

StateFarm

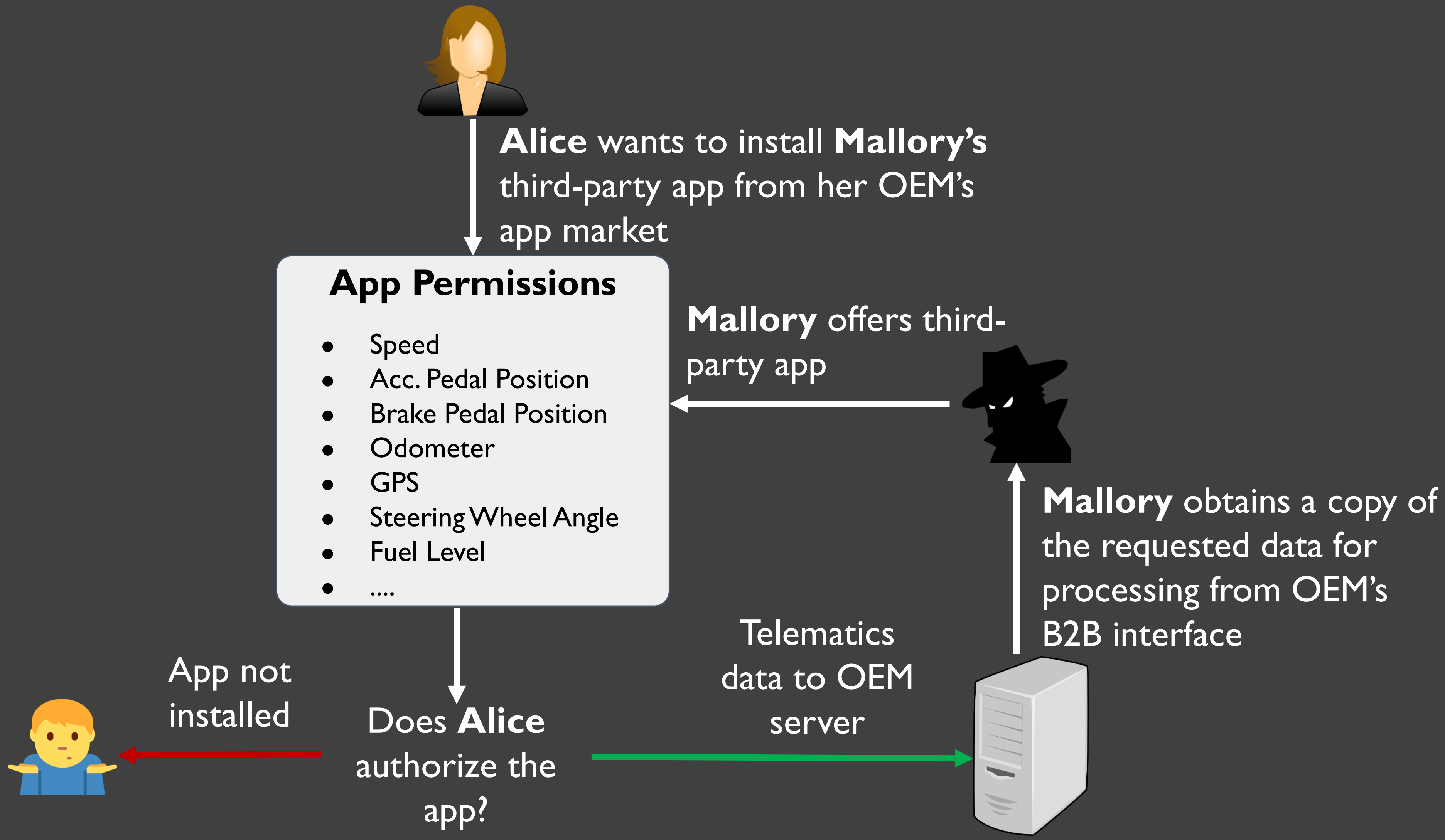
verizon

otonomo

Automotive

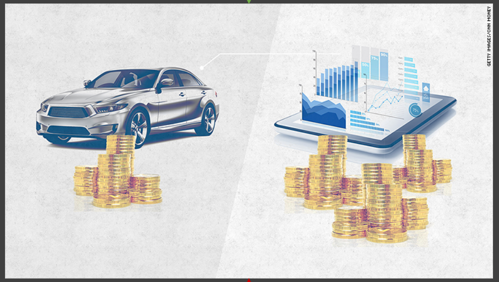


Threat Model (derived from BMW CarData)



Increased connectivity comes at a price

Data Connectivity

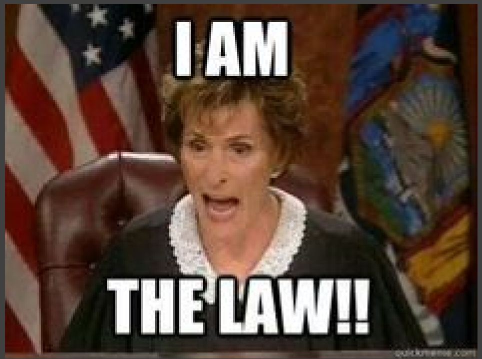


Privacy Concerns

- Facebook-Cambridge Analytica incident
- General Data Protection Regulation (GDPR)

More Regulation and Awareness?

More Regulation and Awareness?



- Voluntary guidelines from 2014
- OEMs only have to ask explicit permission for three categories:
  - Driving behavior
  - Geolocation
  - Biometrics

"covered information"

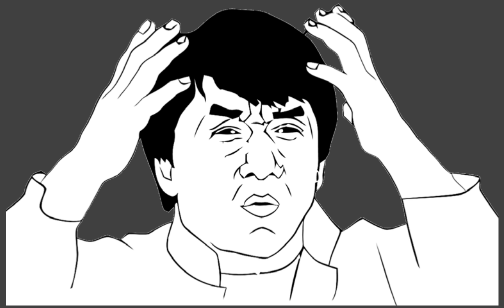
ALLIANCE OF AUTOMOBILE MANUFACTURERS, INC.
ASSOCIATION OF GLOBAL AUTOMAKERS, INC.

Consumer Privacy Protection Principles

PRIVACY PRINCIPLES FOR VEHICLE TECHNOLOGIES AND SERVICES

November 12, 2014

More Regulation and Awareness?



- How much do you agree to share the following data types with an **OEM**?

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Odometer					
Vehicle Identificat...					
Outside temperat...					
Location (GPS)					
Current speed					

...

- How much do you agree to share the following data types with a **third-party app provider**?

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Odometer					
Vehicle Identificat...					
Outside temperat...					
Location (GPS)					
Current speed					

...

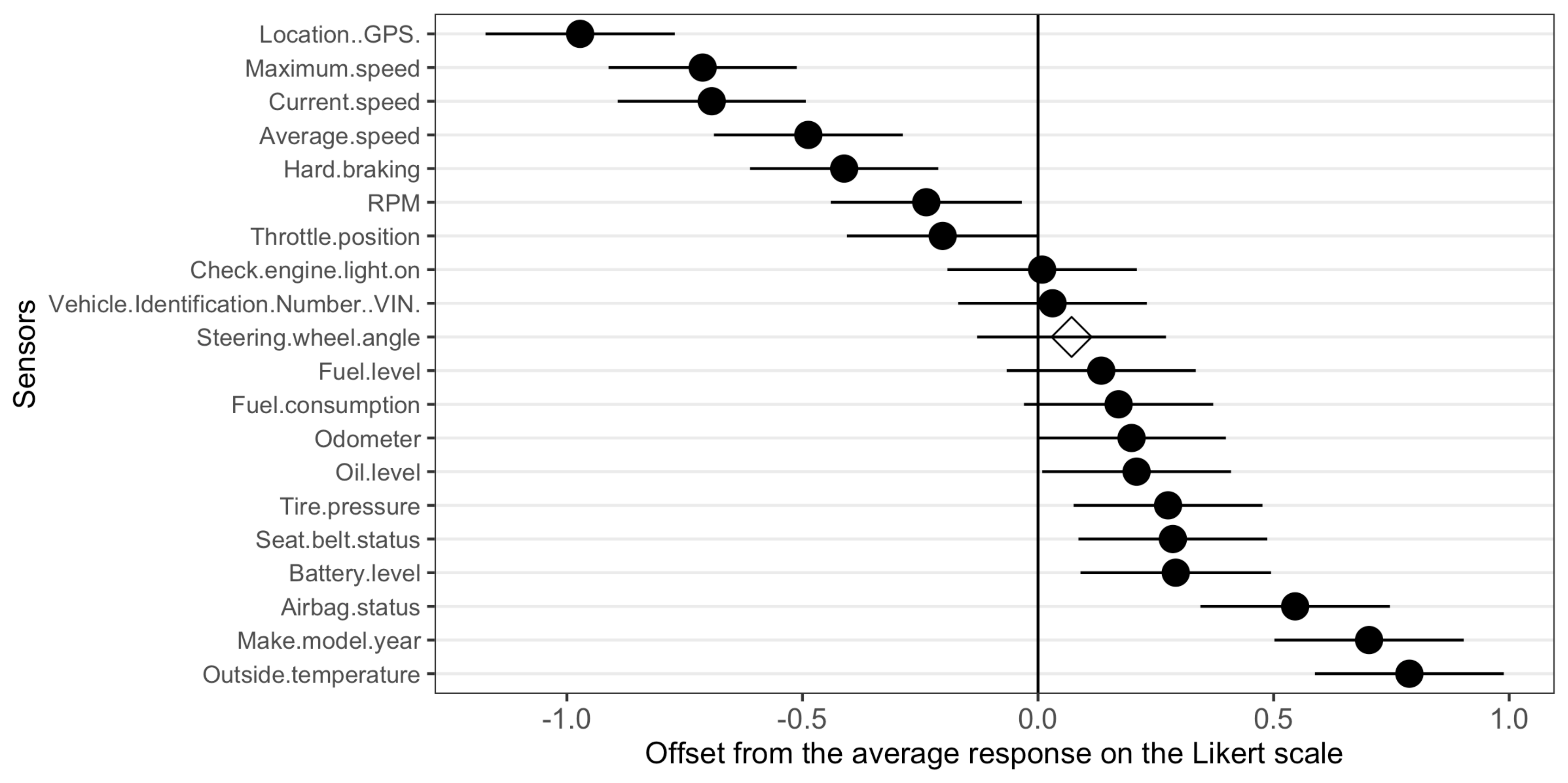
Survey Setup and Results

Participants

N=100
61% male
85% from USA
39% familiar with car telematics

Results

OEM Mean: 3.63
3rd Party Mean: 3.12



- **More comfortable sharing data with OEMs**
- **Not particularly uncomfortable sharing SWA data**

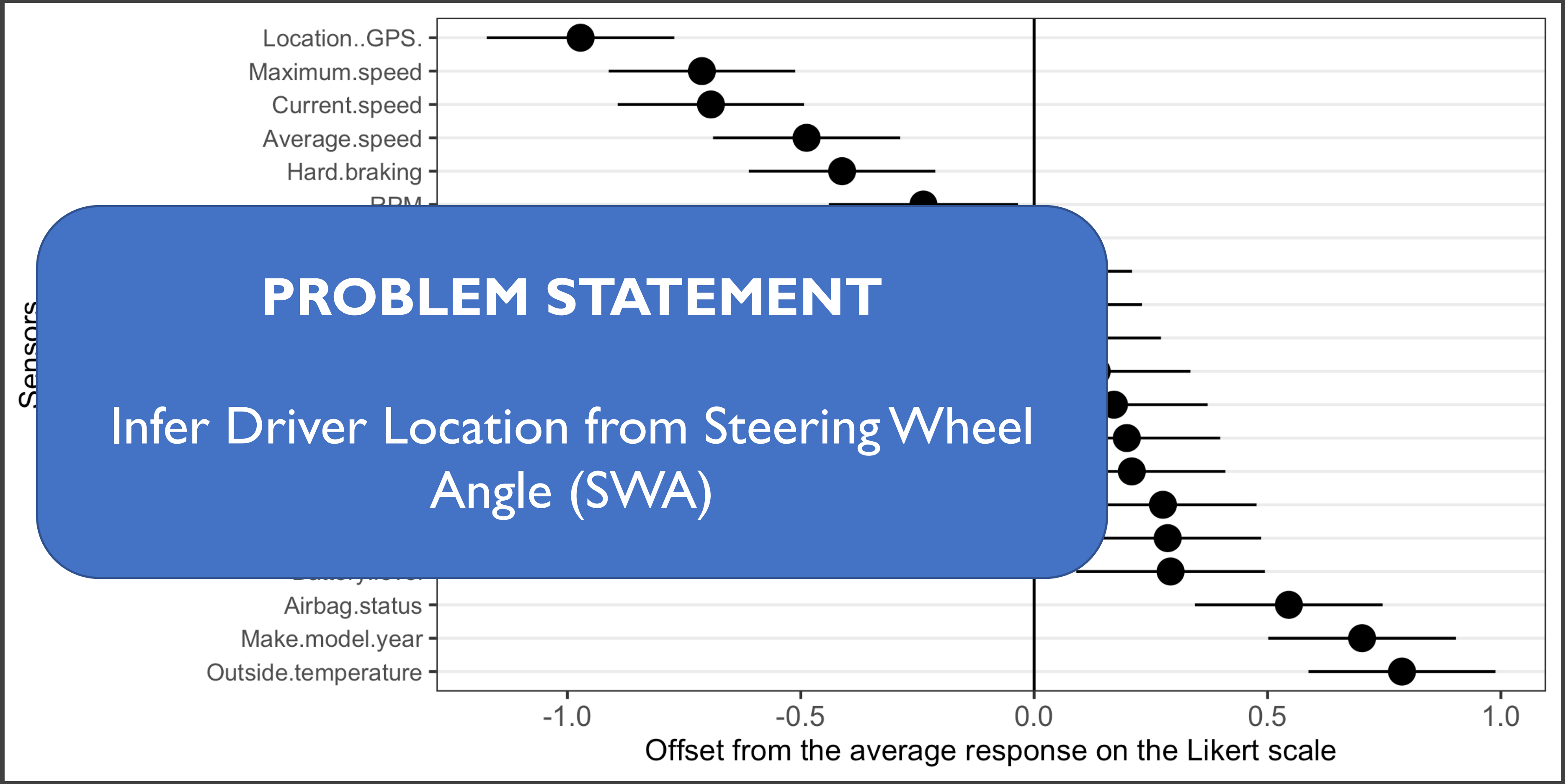
Survey Setup and Results

Participants

N=100
61% male
85% from USA
39% familiar with car telematics

Results

OEM Mean: 3.63
3rd Party Mean: 3.12



PROBLEM STATEMENT

Infer Driver Location from Steering Wheel Angle (SWA)

- **More comfortable sharing data with OEMs**
- **Not particularly uncomfortable sharing SWA data**

Attack Feasibility

Weak Architecture Design

- Permission Model (e.g., Android Automotive [Pe20])
- OEM Review Process

Lax Privacy Regulation

- Voluntary Guidelines with Vague Recommendations
- Lacking Study of GDPR Application

Lacking User Awareness

- Survey shows Steering Wheel Angle (SWA) not Sensitive enough

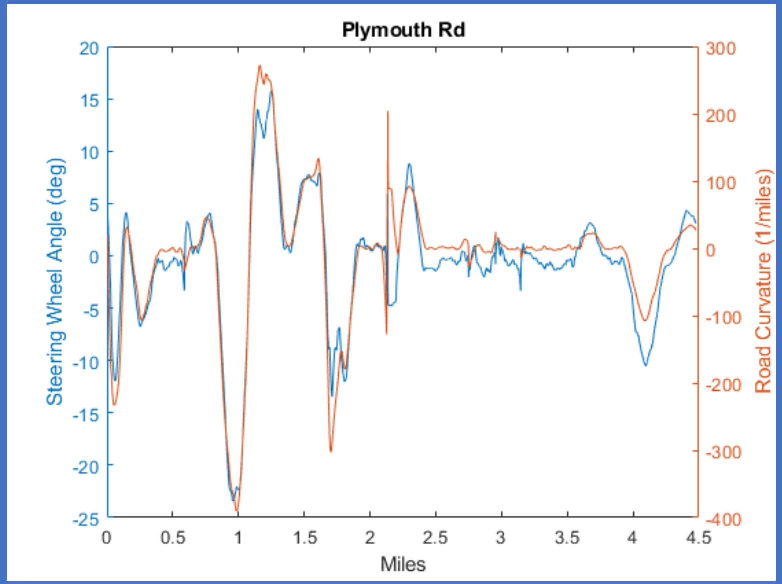
Location Inference / Travel Route Reconstruction through SWA Traces is Extremely Tempting!

Attack Feasibility

Weak Architect
Design

- Permission Mod
(e.g., Android Auton
[Pe20])
- OEM Review Proc

SOLUTION



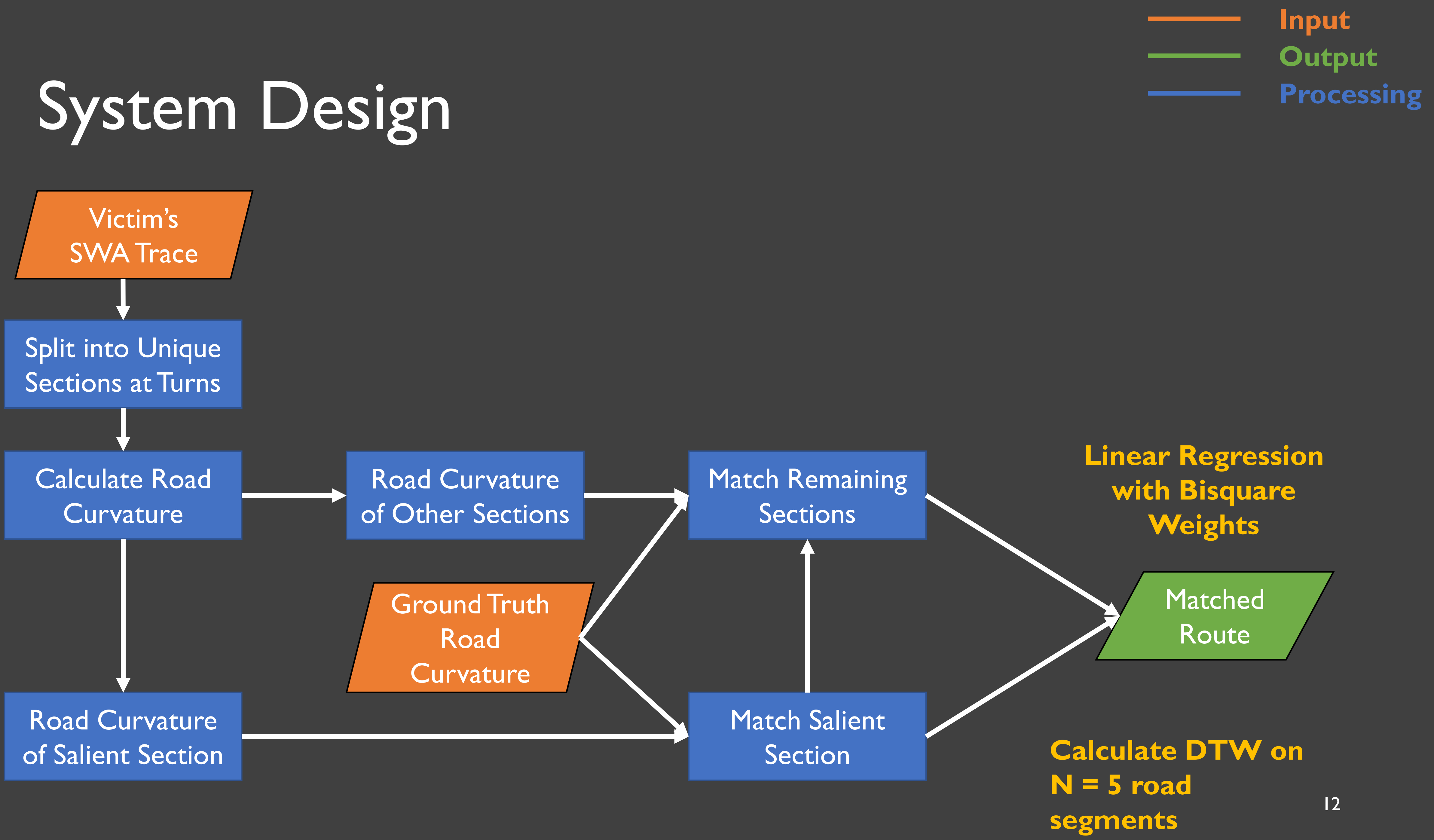
RoCuMa
(Road Curvature Matching)

Lacking User
Awareness

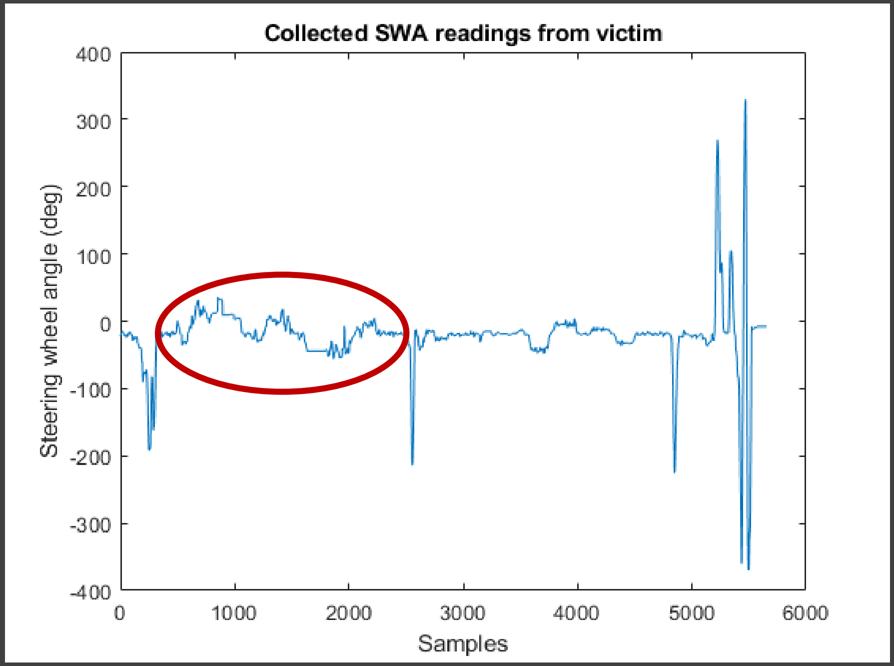
urvey shows Steering
/heel Angle (SWA) not
Sensitive enough

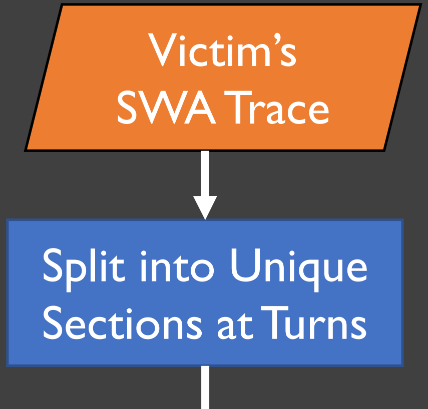
Location Inference / Travel Route Reconstruction through SWA Traces is Extremely Tempting!

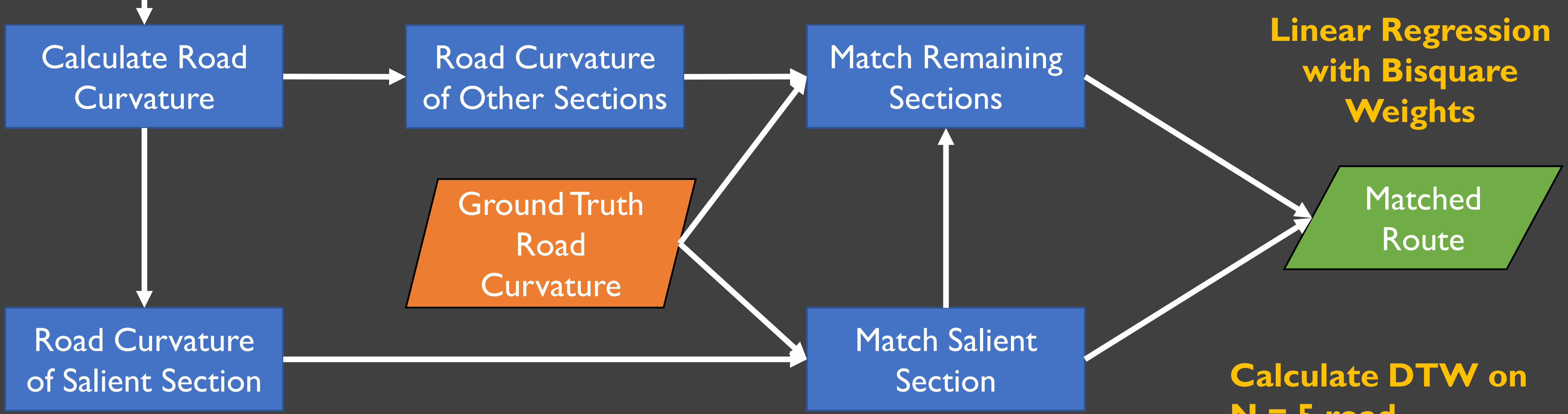
System Design



System Design

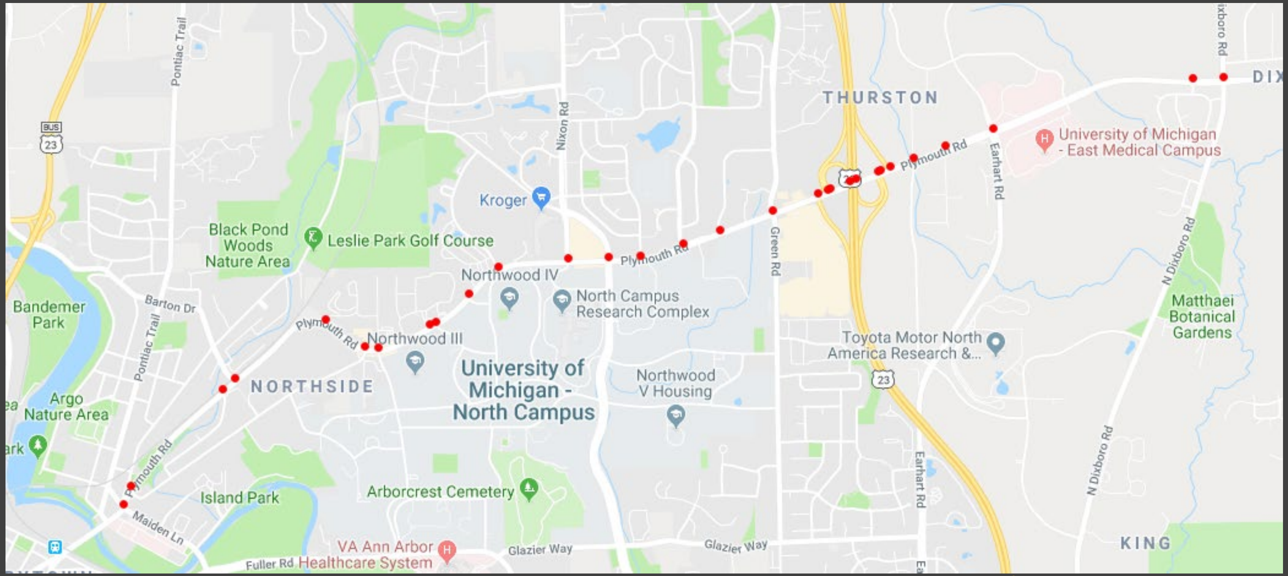






System Design

Input
Output
Processing



Victim's SWA Trace

Split into Unique Sections at Turns

Calculate Road Curvature

Road Curvature of Other Sections

Match Remaining Sections

Linear Regression with Bisquare Weights

Ground Truth Road Curvature

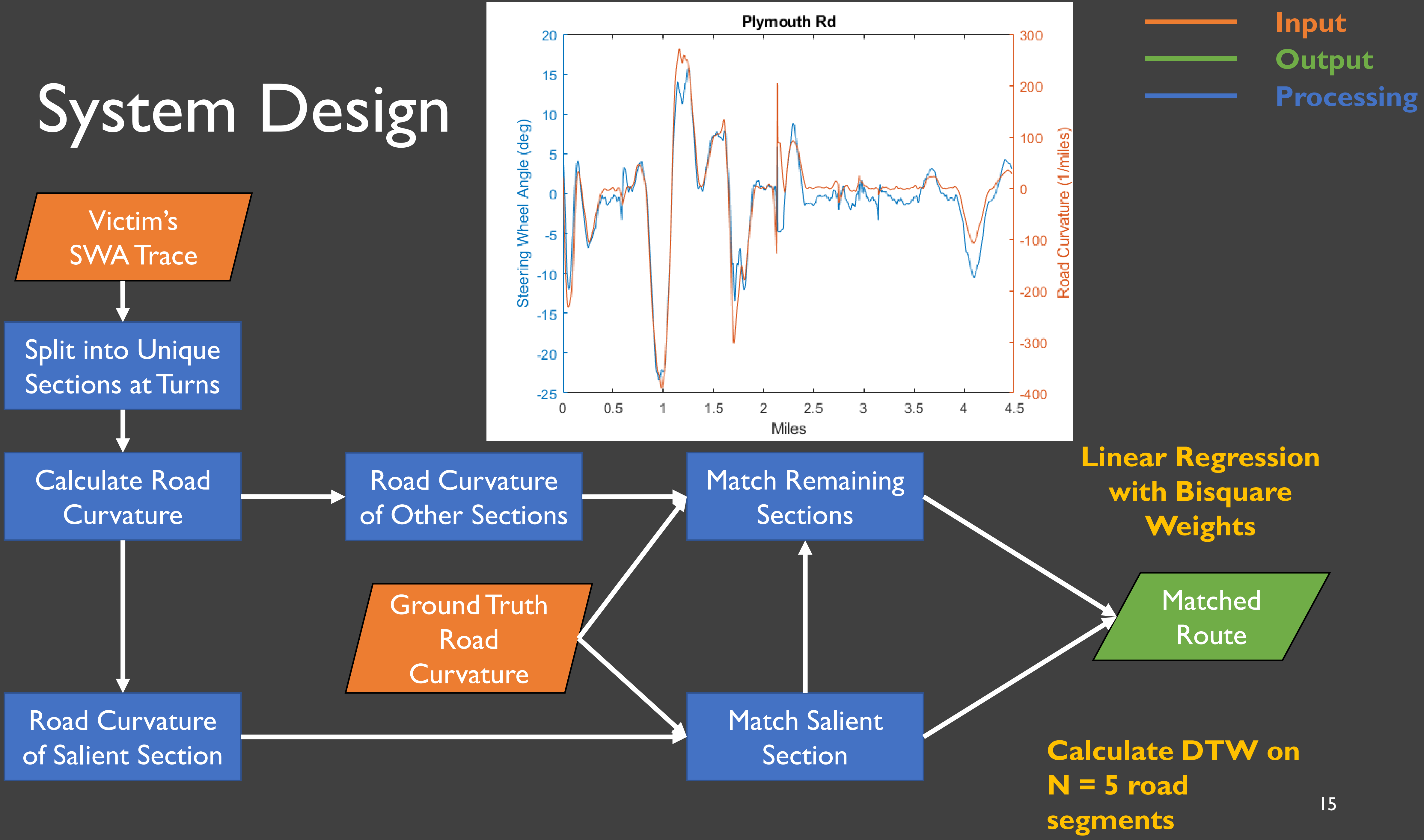
Matched Route

Road Curvature of Salient Section

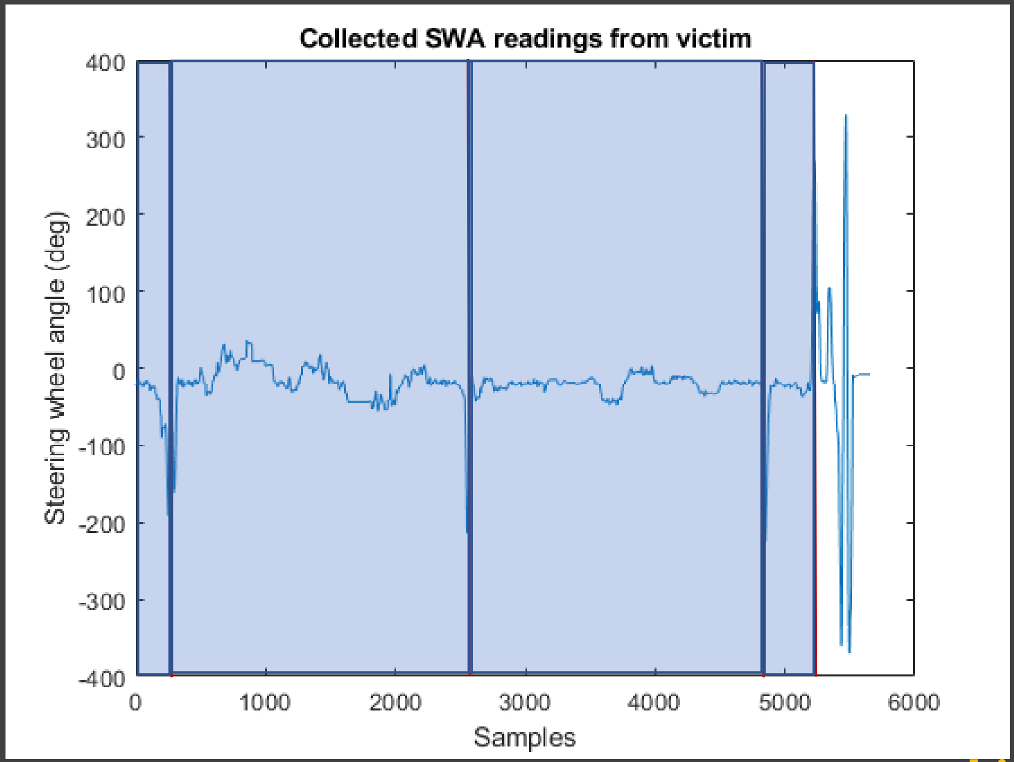
Match Salient Section

Calculate DTW on N = 5 road segments

System Design



System Design



Input
Output
Processing

Victim's SWA Trace
Split into Unique Sections at Turns
Calculate Road Curvature
Road Curvature of Other Sections
Road Curvature of Salient Section
Ground Truth Road Curvature
Match Remaining Sections
Match Salient Section
Matched Route
Linear Regression with Bisquare Weights
Calculate DTW on N = 5 road segments

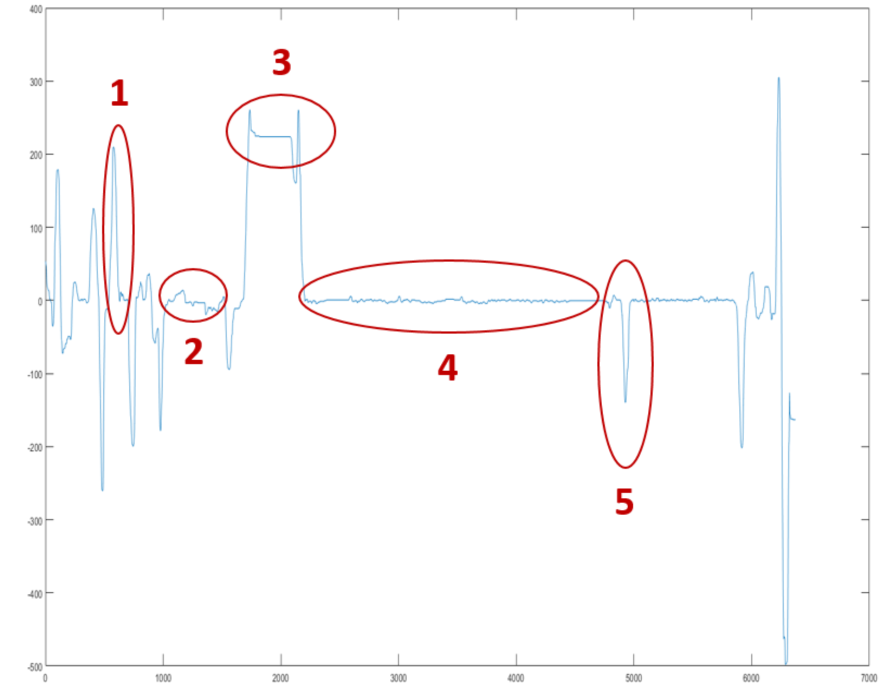
System Design

SY

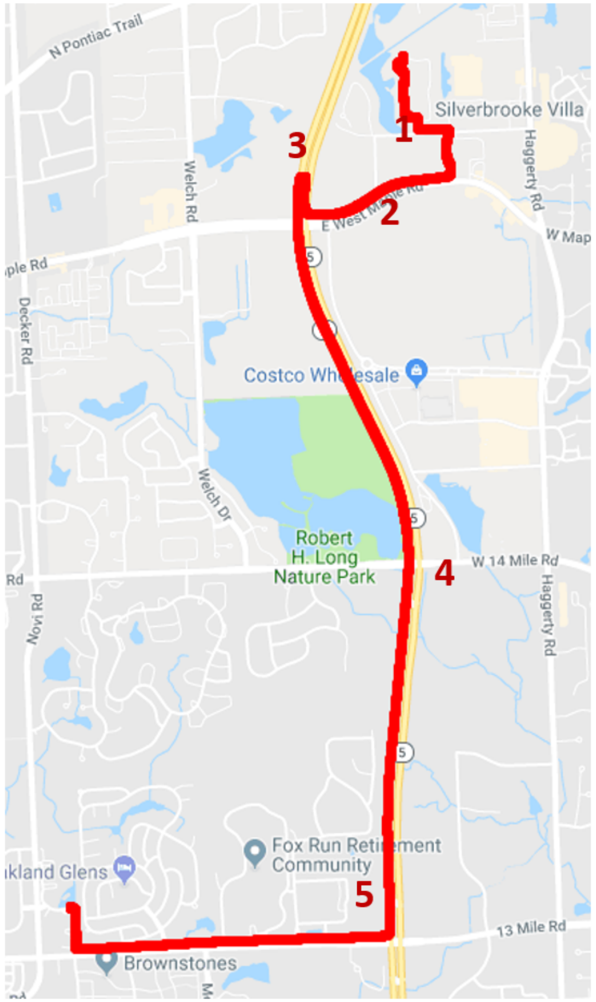
Split i
Sectio

Calc
Cu

Road
of Sal



(1) Spike to positive over 90°: Left turn
(2) Deviations around 0° larger than 10°: Relatively curvy road
(3) Spike with two peaks and flat shape in between peaks: U-turn
(4) Deviations around 0° smaller than 10°: Relatively straight road
(5) Spike to negative over 90°: Right turn



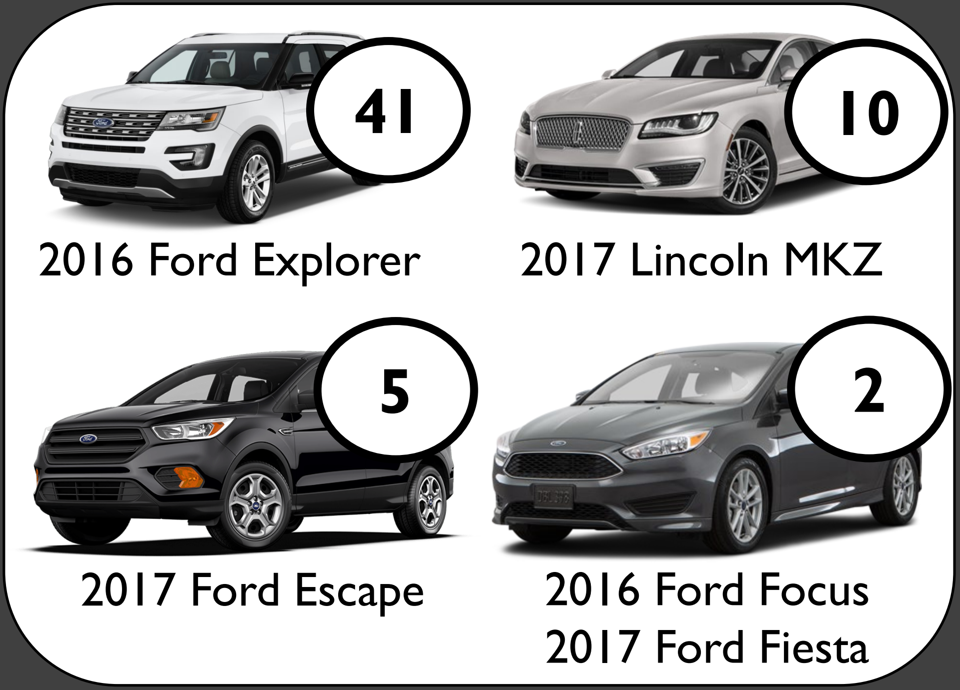
Linear Regression with Bisquare Weights

Matched Route

Calculate DTW on N = 5 road segments

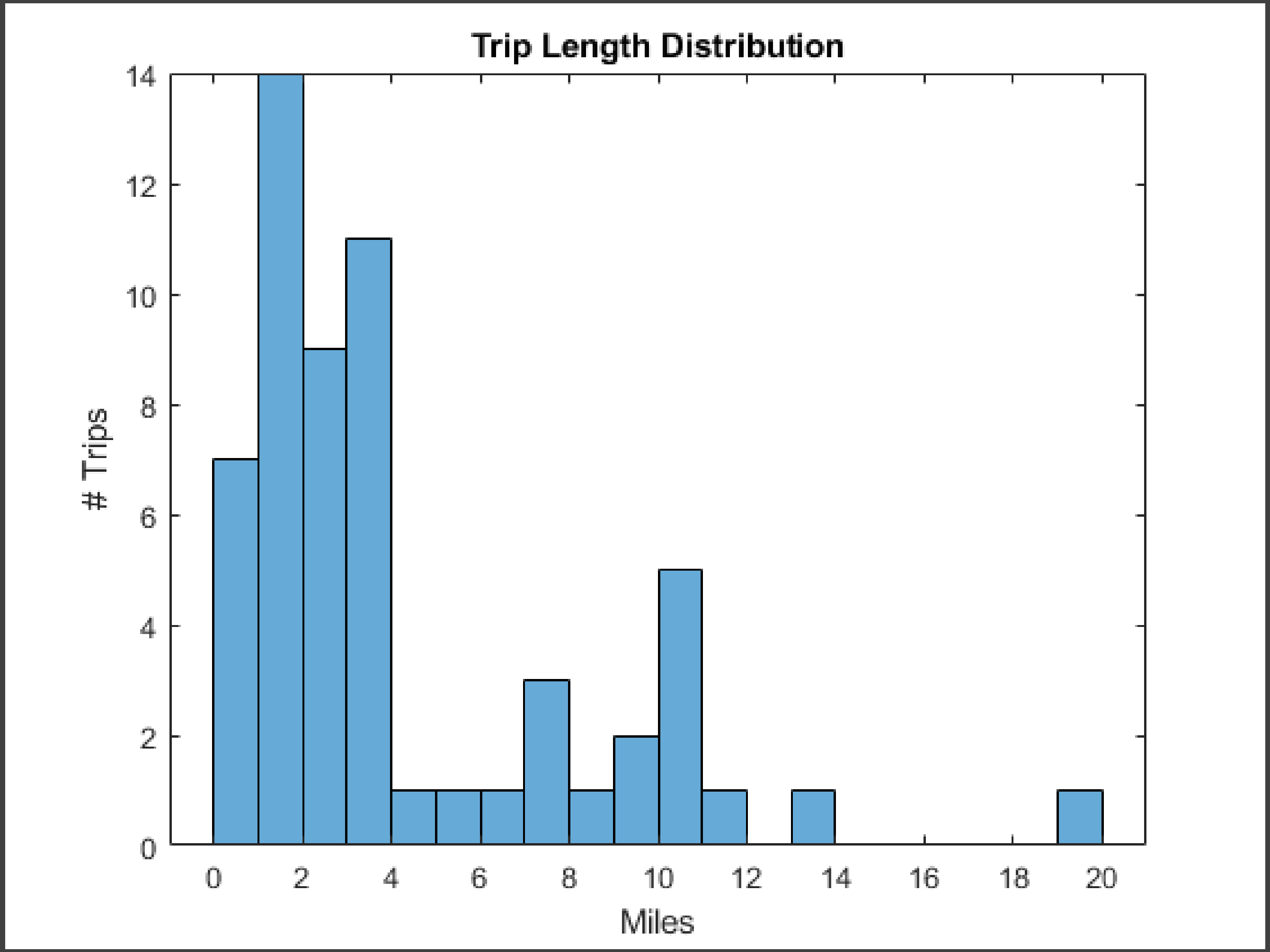
Experimental Setup

- Five different models of same OEM
  - 58 traces in total
- Vehicle Data Collection
  - OpenXC Platform
- Road Curvature Acquisition
  - OpenStreetMap



Dataset

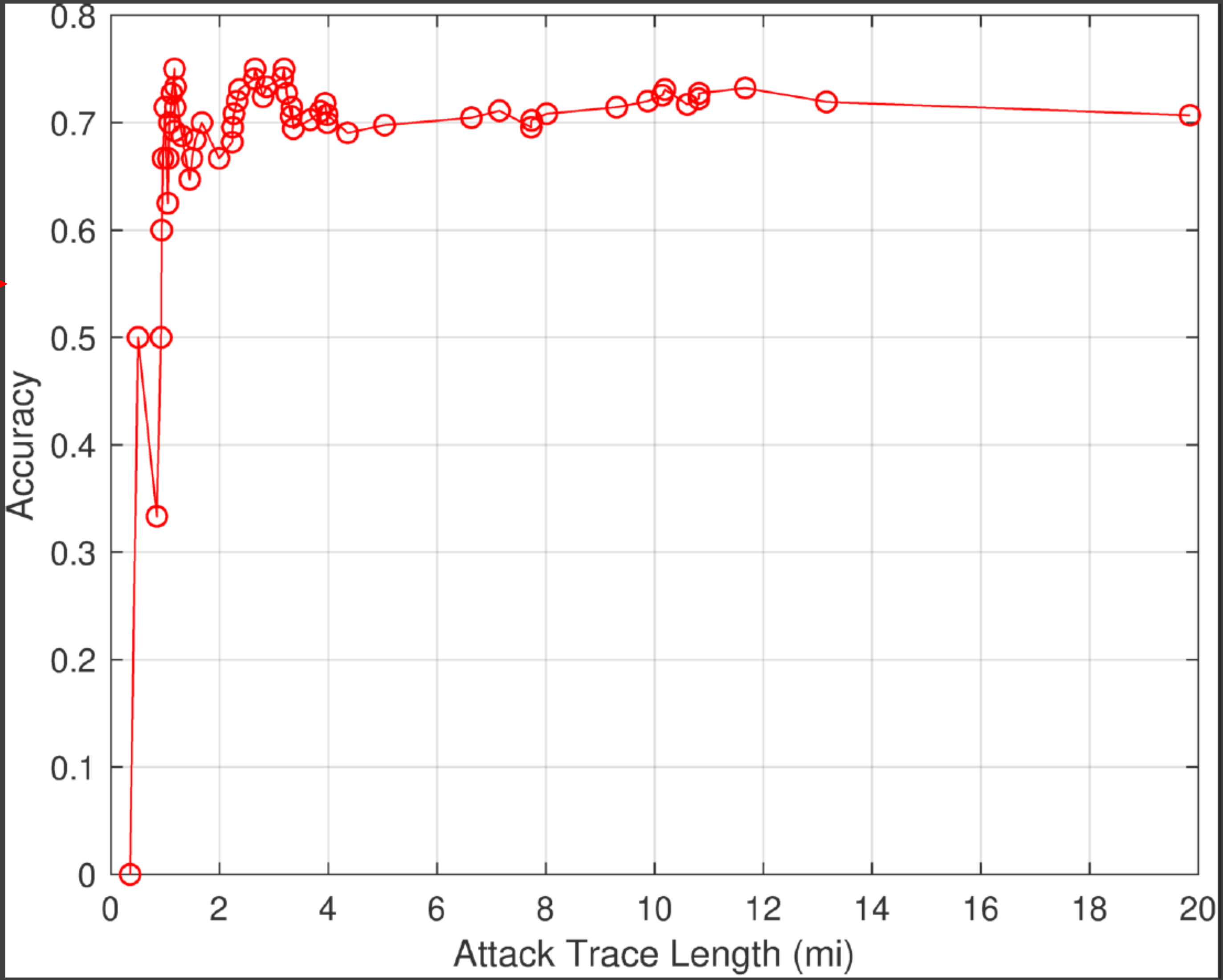
- Ground truth database in Ann Arbor, MI
  - 236 roads, 2776 road segments
- 58 attack SWA traces collected
  - Mean length 4.28 mi
  - Median length 2.83 mi
  - Minimum length 0.35 mi
  - Maximum length 19.85 mi



Accuracy

Full Route Match
41/58 = 71%

Initial Section Match
44/58 = 76%

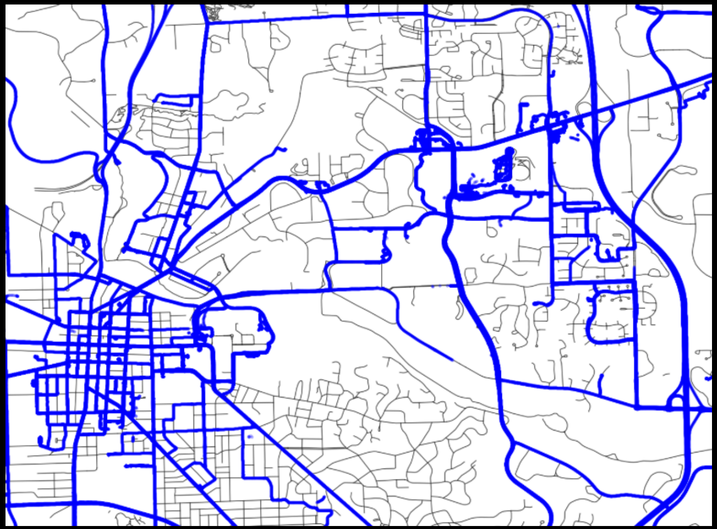


- Success heavily depends on initial section
- Straight final segments cause issues

Other Metrics

Memory Footprint

Total Ground Truth: 29.8 MB
Per Mile: 55.2 kB
Per Road Segment: 10.6 kB



Detroit Metro Area: ~26 GB

Computation Time & Complexity

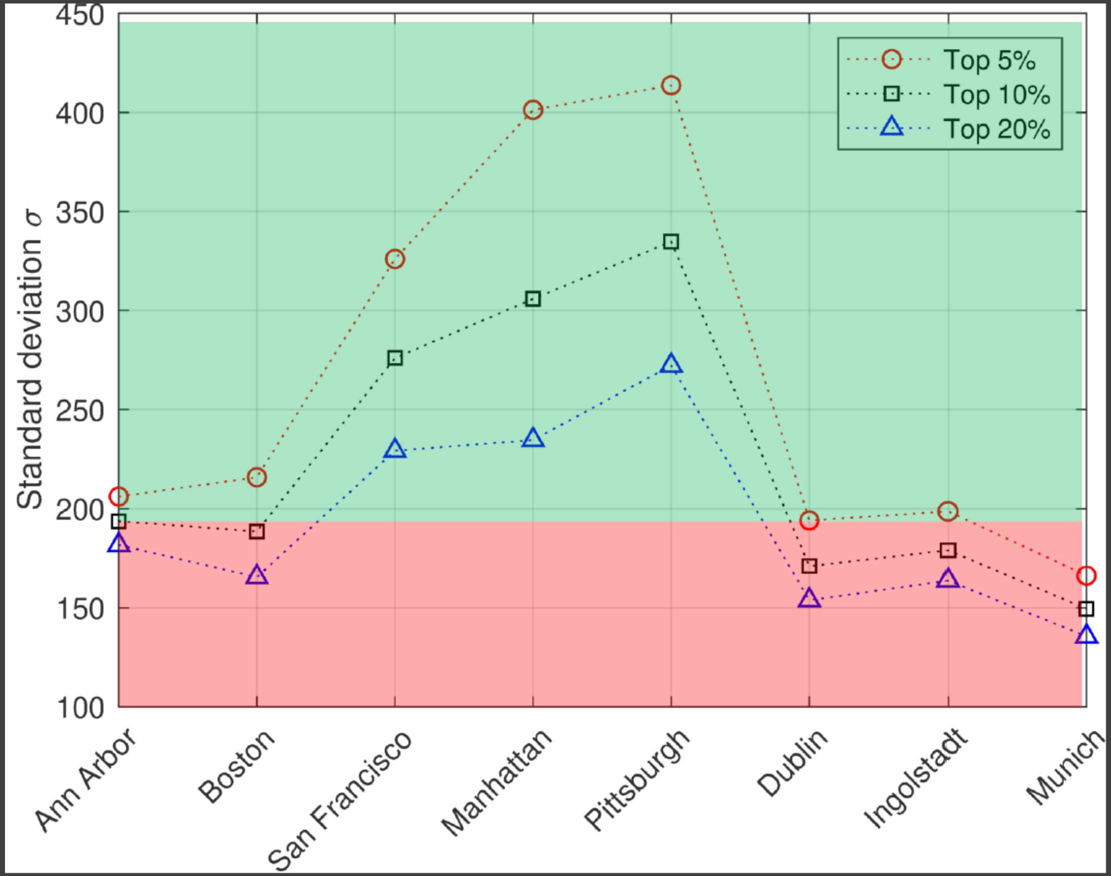
Intel Core i7-8650U CPU
16 GB RAM
Windows 10 + MATLAB R2018a

- Max. time: <19 minutes
- DTW: >90%
- Initial Section Matching: >99%
- Initial Section Complexity: $O(N^2)$
- Remaining Section Complexity: $O(N)$

Applicability to Other Cities

City	# Road Segments	Avg. Curvature Index
Ann Arbor, MI	2776	207.82
Boston, MA	9539	195.25
San Francisco, CA	7515	158.73
Manhattan, NY	1920	92.51
Pittsburgh, PA	10692	248.61
Dublin, Ireland	12977	221.42
Ingolstadt, Germany	2338	225.17
Munich, Germany	15071	152.30

$$avg\_curv\_index = \frac{\sum_{i=1}^{\#segments} curv(i)length(i)}{\sum_{j=1}^{\#segments} length(j)}$$

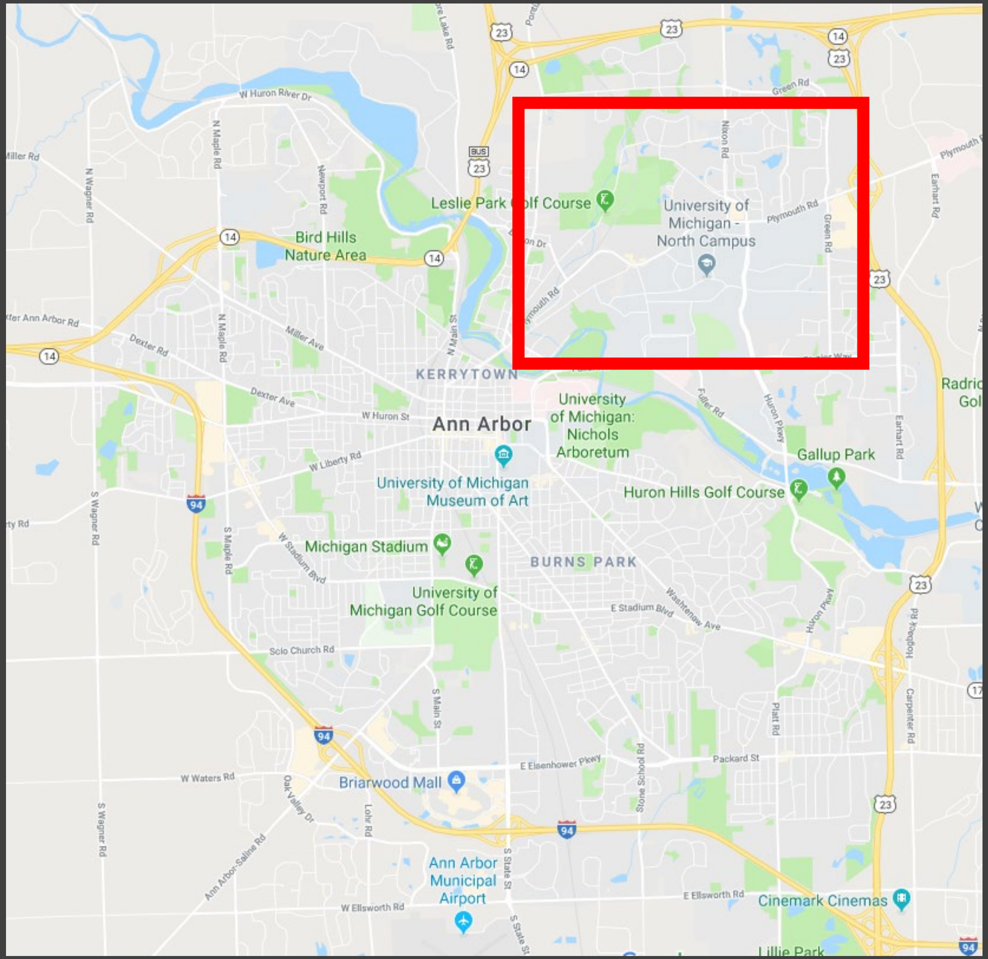


σ↑ less similar roads

σ↓ more similar roads

Applicability to Other Cities

- New Area with higher Avg. Curvature Index
  - 268.73 > 207.82
- 15/58 traces evaluated in this area
  - 550 < 2776 road segments
  - Mean trip length 2.2 mi < 4.28 mi
- Accuracy
  - 13/15 = 87% > 71%



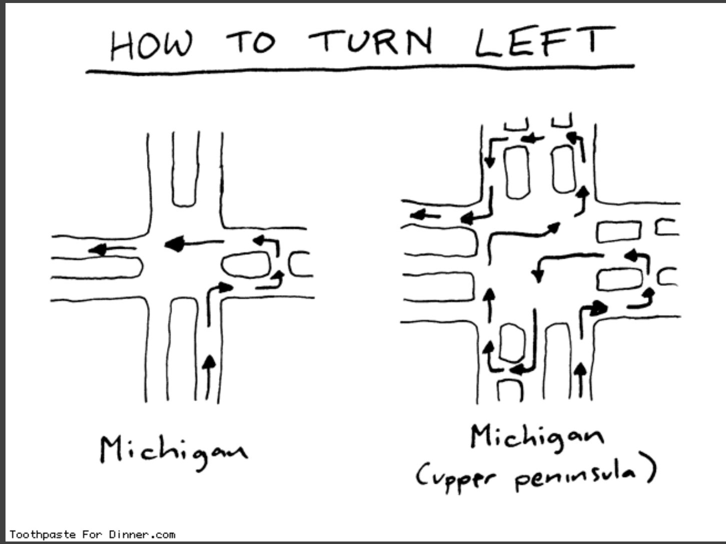
Area with higher avg. curvature yields higher accuracy!

Comparison with Related Work

	Na16	Mi15	Zh17	Ga14	De13	SPy
Data Source	Phone IMU Sensors	Phone Power Consumption	Speed from OBD-II Device	Speed from OBD-II Device	Speed from GPS Tracking Unit	Vehicular Data Collection Systems
Reference Source	Maps	Prerecorded Power Profiles for Each Phone	Maps	Maps	Time Stamp + Speed + Distance Traveled	Maps
Pre-processing	**Easy**	Hard	**Easy**	**Easy**	Medium	**Easy**
# Apps in App Market	Android: 3.5M (Dec 2017) iOS: 2.2M (Jan 2017)	Android: 3.5M (Dec 2017) iOS: 2.2M (Jan 2017)	N/A	N/A	N/A	**BMW: 90 (Jan 2018)**
Matching Method	Turn Angle Similarity + Curve Similarity + Travel Time Similarity	HMM	HMM, DFS	Elastic Pathing	DFS	Road Curvature Matching (RoCuMa)
No Starting Point Assumption	✔	✗	✗	✗	✗	✔
Accuracy of Estimating Entire Road	13-38%	45% (of full route)	70% in Top 30 Candidate Routes	14% (less than 250m error)	37%	**71%**

Limitations

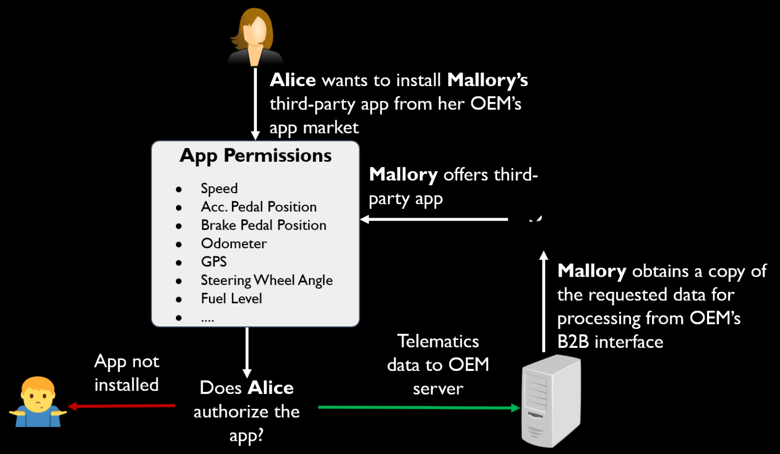
- Works for most European cities with similar or higher curvature than Ann Arbor, but not for particular US cities on the grid (e.g., Manhattan)
- Rough knowledge of city/area required
- Did not consider lane changes, U-turns or roundabouts



Conclusion

Driver Location can be Viably Inferred by Steering Wheel Angle Data!

New Threat Model



Vehicular telematics systems are on the rise and allow third-party apps to access sensitive vehicular data

Awareness Survey

Drivers are not aware of sensitivity and privacy consequences of most automotive sensors

Accuracy

RoCuMa offers better accuracy compared to existing related location inference approaches

Q & A

Mert D. Pesé

Xiaoying Pu

Kang G. Shin

References

[Pe20] Pese, M., Shin, K., Bruner, J., and Chu, A., "Security Analysis of Android Automotive," SAE Technical Paper 2020-01-1295, 2020

[Na16] Sashank Narain, Triet D. Vo-Huu, Kenneth Block, and Guevara Noubir. Inferring User Routes and Locations Using Zero-Permission Mobile Sensors. Proceedings - 2016 IEEE Symposium on Security and Privacy, SP 2016, pages 397–413, 2016

[Mi15] Yan Michalevsky, Gabi Nakibly, Aaron Schulman, Gunaa Arumugam Veerapandian, and Dan Boneh. PowerSpy: Location Tracking using Mobile Device Power Analysis. 24th USENIX Security

References

[Zh17] Lu Zhou, Qingrong Chen, Zutian Luo, Haojin Zhu, and Cailian Chen. Speed-Based Location Tracking in Usage-Based Automotive Insurance. Proceedings - International Conference on Distributed Computing Systems, pages 2252–2257, 2017

[Ga14] Xianyi Gao, Bernhard Firner, Shridatt Sugrim, Victor Kaiser-Pendergrast, Yulong Yang, and Janne Lindqvist. Elastic pathing. In Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing - UbiComp '14 Adjunct, pages 975–986, New York, New York, USA, 2014

[De13]] Rinku Dewri, Prasad Annadata, Wisam Eltarjaman, and Ramakrishna Thurimella. Inferring trip destinations from driving habits data. Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society – WPES '13, pages 267–272, 2013