CERIAS

The Center for Education and Research in Information Assurance and Security

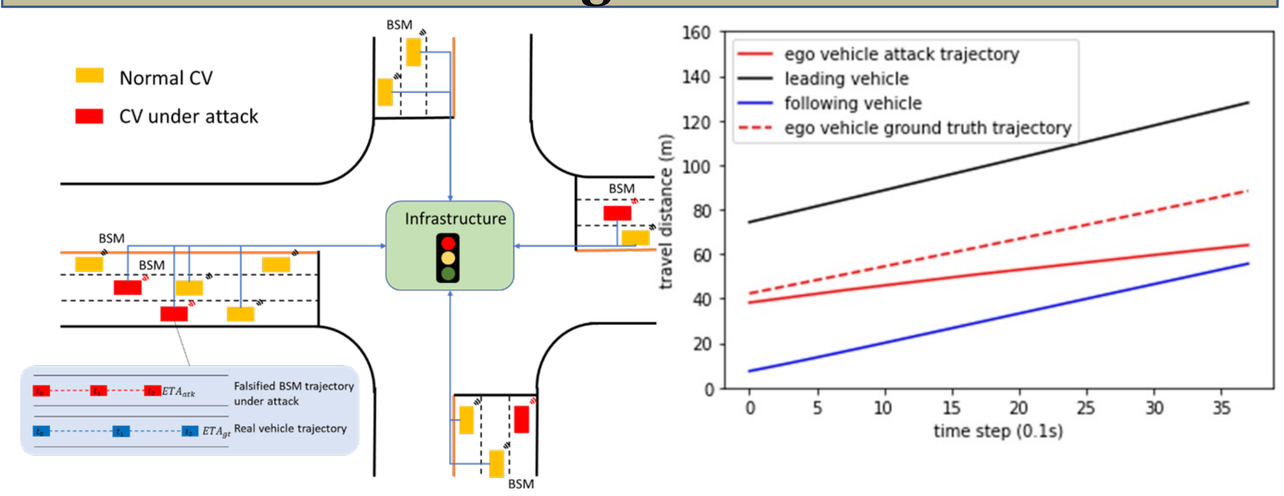
Modeling and Detecting Falsified Vehicle Trajectories Under Data Spoofing Attacks

Jun Ying[1], Yiheng Feng[1] , Qi Alfred Chen[2] , Z. Morley Mao[3]
1. Lyles School of Civil Engineering, Purdue University 2. Department of Computer Science, University of California, Irvine
3. Department of Electrical Engineering and Computer Science, University of Michigan

Introduction

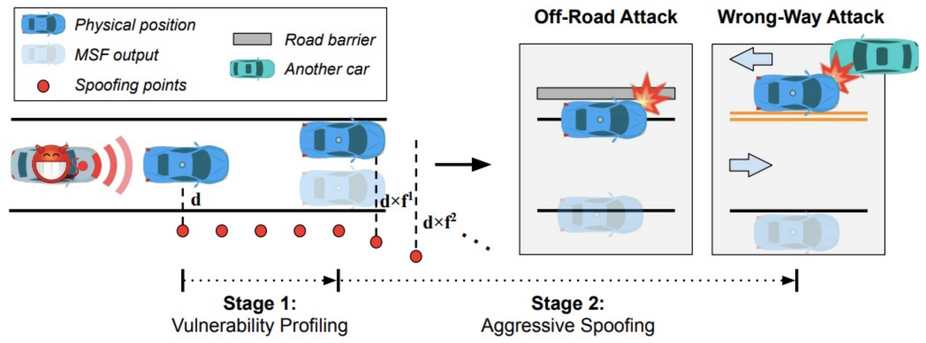
- CAV improves transportation system safety and efficiency but brings cyber risks.
- Data spoofing attack is one major threat to both CAVs and infrastructure applications.
- Existing anomaly detection algorithms are mainly designed to distinguish specific attacks.
- A generic detection framework is proposed to identify abnormal trajectories from both known and unknown attacks.
- Two representative attacks, estimated time of arrival (ETA) attack, and multi-sensor fusion (MSF) attack are modeled as known attacks.

Modeling ETA Attack



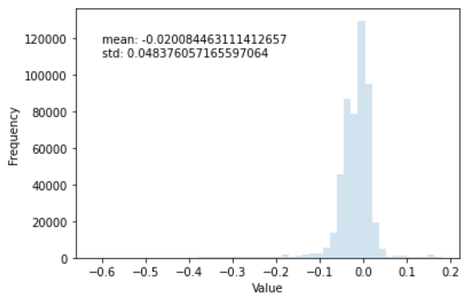
- ETA attack generates falsified vehicle trajectories that have abnormal longitudinal behaviors.
- Vehicle under attack sends out falsified BSMs with longer ETAs.
- ETA attack leads to nonoptimal signal timing plans and increases vehicle delay at intersections.
- ETA attack is modeled as an optimization problem.

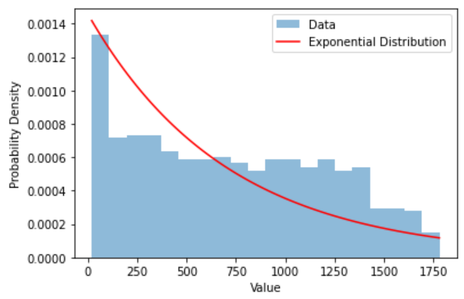
Modeling MSF Attack



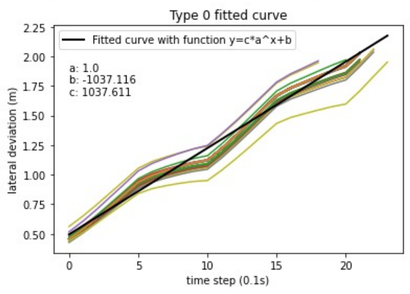
- MSF attack leads to vehicle's lateral abnormal behaviors (e.g., deviation from the lane center)
- The original MSF attack is time-consuming and complicated.
- Only trajectory-level attack behavior is needed to model the attack's impact on traffic safety and mobility.

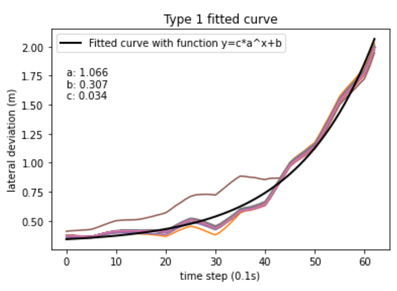
- Vulnerability profiling stage

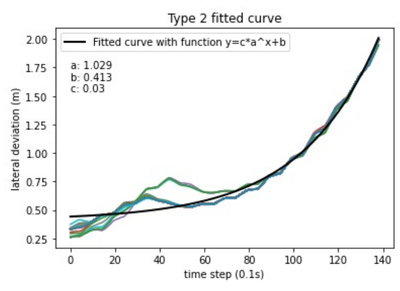


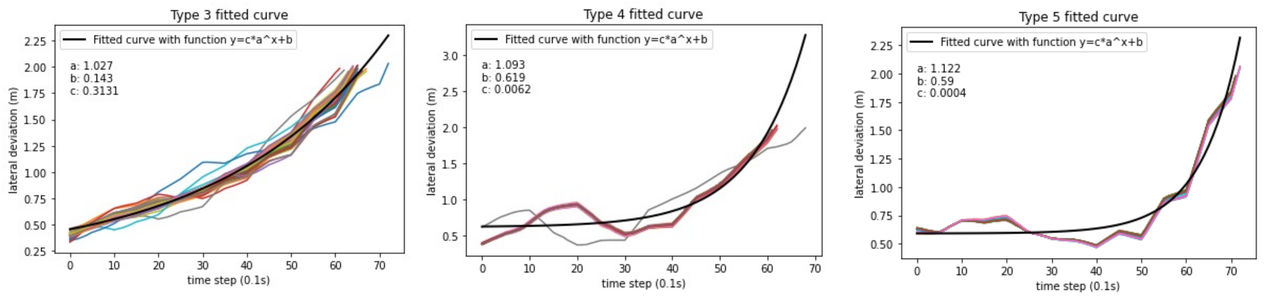


Aggressive spoofing stage

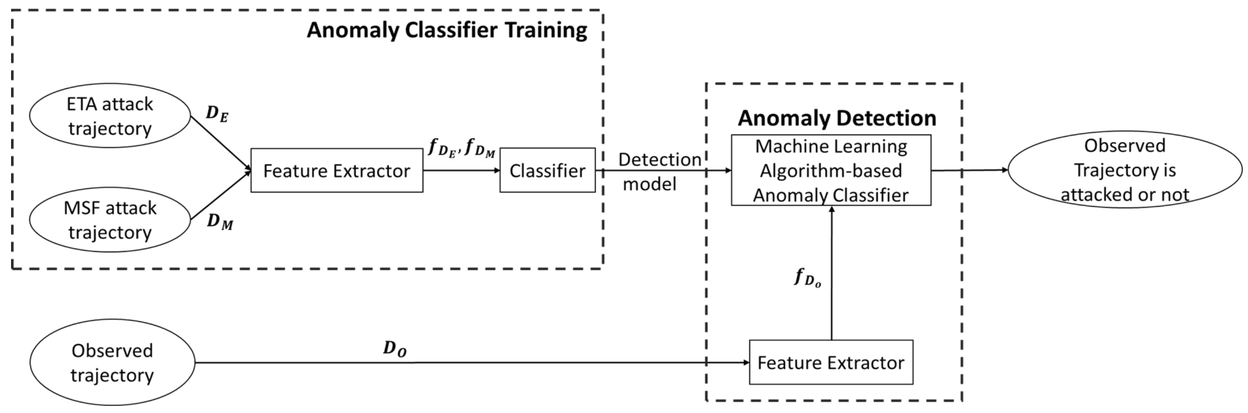








Detection Methodology



- Domain knowledge-based feature extraction is applied to extract 13 features from vehicle trajectories, including both car-following and lane changing related features.

Numerical Study

- The anomaly detection algorithm is tested on the V2X Application Spoofing Platform (VASP).

Detection Performance on two known attacks

	FP	FN	TP	TN	Detection rate	False alarm rate
SVM	7	1	144	196	144/145	7/203
Random Forest	0	0	145	203	145/145	0/203
Decision Tree	0	0	145	203	145/145	0/203

Detection Performance on six unknown attacks

Attack Type	Traj. Count	Accuracy (Avg.)		
		SVM	Decision Tree	Random Forest
Random position	246	1.0	1.0	1.0
Random position offset	216	1.0	1.0	1.0
High acceleration	225	1.0	1.0	1.0
Low speed	225	1.0	1.0	1.0
Braking from communication range	990	1.0	1.0	1.0
EEBL	1055	1.0	1.0	1.0

- The anomaly detection algorithm performs well in detecting both known and unknown attacks.
- Other baseline models: plausibility check based anomaly detection, neural network classifier with linear connected layer, convolution neural network classifier.

Attack Type	Traj. Count	Accuracy (Avg.)		
		Plausibility check	NN	CNN
MSF and ETA	348	0.72	0.96	0.96
Random position	246	1.0	0.99	0.99
Random position offset	216	1.0	1.0	0.95
High acceleration	225	1.0	1.0	0.95
Low speed	225	1.0	1.0	0.95
Braking from communication range	990	1.0	0.77	0.83
EEBL	1055	1.0	0.82	0.82

- The proposed anomaly detection algorithm outperforms the baseline models.

Acknowledgement: This research is supported in part by the U.S. National Science Foundation (NSF) through Grant SaTC. #1930041.

Contact Info.: Yiheng Feng feng333@purdue.edu