Deep-Learning-Based Anomaly Detection for Connected and Autonomous Vehicles in Lane-Changing Scenarios

Chien Lin

Advisor: Chung-Wei Lin, Ph.D.

National Taiwan University
Taipei, Taiwan

Outline

- **Introduction**
- Problem Formulation
- Proposed Approaches
- Experimental Results
- Conclusion

Introduction

- Advanced Driver Assistance Systems (ADAS)
  - Cooperative Adaptive Cruise Control (CACC), Lane Keeping Assistance System (LKA) and so on
  - Use vehicular communication to receive the environmental information like the position, velocity, and acceleration from the surrounding vehicles
- Wireless channels are vulnerable to security attacks
  - Attackers can modify data transmitted from other vehicles
- Mitigation approaches should be provided to protect against attacks
  - Intrusion Detection Systems (IDS)

Related Work

- Rule-based model [1]
  - Based on the rules of human knowledge
- Probabilistic model [2]
  - Using multiple statistical techniques
- Deep-learning-based model [3]
  - Iterated computation

[1] "Lane-changing prediction in highway: Comparing empirically rule-based model mobil and a naıve bayes algorithm," ITSC'21
[2] "Highway discretionary lane changing behavior recognition using continuous and discrete hidden Markov model," ITSC'21
[3] "An ensemble deep learning approach for driver lane change intention inference," Transportation Research Part C: Emerging Technologies '20

Contributions

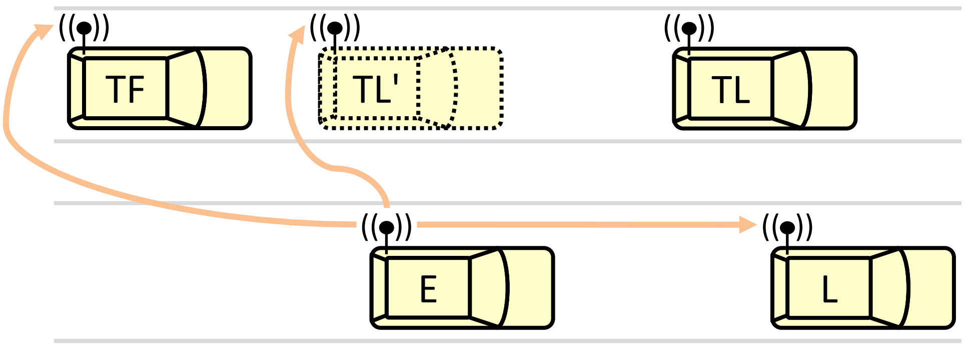
- Propose stealthy attacks
  - Cannot be detected by a rule-based model
- Propose deep-learning-based models for anomaly detection
  - The models achieve decent detection performances against the anomaly
- Have a general anomaly detection workflow
  - The workflow can be used in different lane-changing environments
  - Highway, roundabout, and opposite overtaking
- Deploy the attacks directly into SUMO during the simulation
  - Generate data to better reflect the real-world scenarios
  - Establish the standards and specifications for the operations in SUMO

Outline

- ❑ Introduction
- ❑ **Problem Formulation**
- ❑ Proposed Approaches
- ❑ Experimental Results
- ❑ Conclusion

System Overview

- Information which assists lane changing can be compromised
- Detect whether a vehicle is attacked when it has a lane-changing intention
- Example:
  - Anomalous vehicle TL indicate itself as TL'



Definitions: Feature Vector

- Consider 4 vehicles
  - Ego vehicle
  - Leading vehicle on the source lane
  - Leading vehicle on the target lane
  - Following vehicle on the target lane
- Feature vector $\mathbf{r}$ with dimension n
- $\mathrm{r}^{(\mathrm{t})} = \left[\mathrm{f}_1^{(\mathrm{t})}, \mathrm{f}_2^{(\mathrm{t})}, \ldots, \mathrm{f}_\mathrm{n}^{(\mathrm{t})}\right]$
  - Example: $\mathrm{f}_1^{(\mathrm{t})}$ is the position of the ego vehicle at time t, $\mathrm{f}_2^{(\mathrm{t})}$ is the velocity of the ego vehicle at time t and so on

Definitions: Trajectory Vector

- Feature vectors $\mathbf{r}$ can form a trajectory vector $\mathbf{R}$
- $\mathbf{w}$ is the length of a trajectory vector $\mathbf{R}$
- $\mathrm{R} = \left[\mathrm{r}^{(0)}, \mathrm{r}^{(1)}, \ldots, \mathrm{r}^{(w-1)}\right]$
- Example:
  - $\mathrm{r}^{(0)}$ = [100, 10, 1], $\mathrm{r}^{(1)}$ = [110, 11, 1], $\mathrm{r}^{(2)}$ = [121, 11, 1]
  - R = $[\mathrm{r}^{(0)}, \mathrm{r}^{(1)}, \mathrm{r}^{(2)}]$

Acceleration Bias Attack (1/2)

- Originally proposed in work [4], with some modifications
- In a trajectory vector $\mathbf{R}$, there is an acceleration vector $\boldsymbol{A}$
- $\mathrm{A} = \left[\mathrm{a}^{(0)}, \mathrm{a}^{(1)}, \dots, \mathrm{a}^{(\mathrm{w}-1)}\right]$
- Example:
  - $\mathrm{a}^{(0)}$ = [0,1,-1,0]
  - $\mathrm{a}^{(0)}$ is also a vector, containing the acceleration of the ego vehicle, the acceleration of the leading vehicle on the source lane and so on

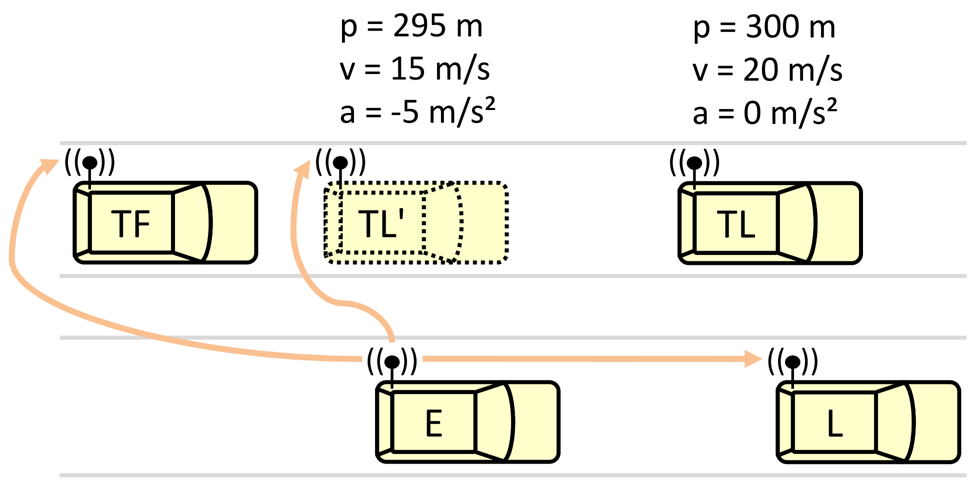
[4] "Deep-Learning-Based Anomaly Detection for Lane-Changing Decisions," IV'22

Acceleration Bias Attack (2/2)

- By adding an offset vector **o**, we can obtain attacked acceleration vector ***A'***
- Each vehicle has an unique seed ***s***
- $A' = \left[a^{(0)} + o^{(0)}, a^{(1)} + o^{(1)}, \dots, a^{(w-1)} + o^{(w-1)}\right]$
  - $o^{(t)} = [0, O(t, s_l), O(t, s_{tl}), O(t, s_{tf})]$
  - $O(t, s) = m \cdot \sin(0.02 \cdot ((s + t) \,\%\, 400))$
- Stealthy attack
  - With law of physics, recalculate the attacked trajectory vector R'

Acceleration Bias Attack Example

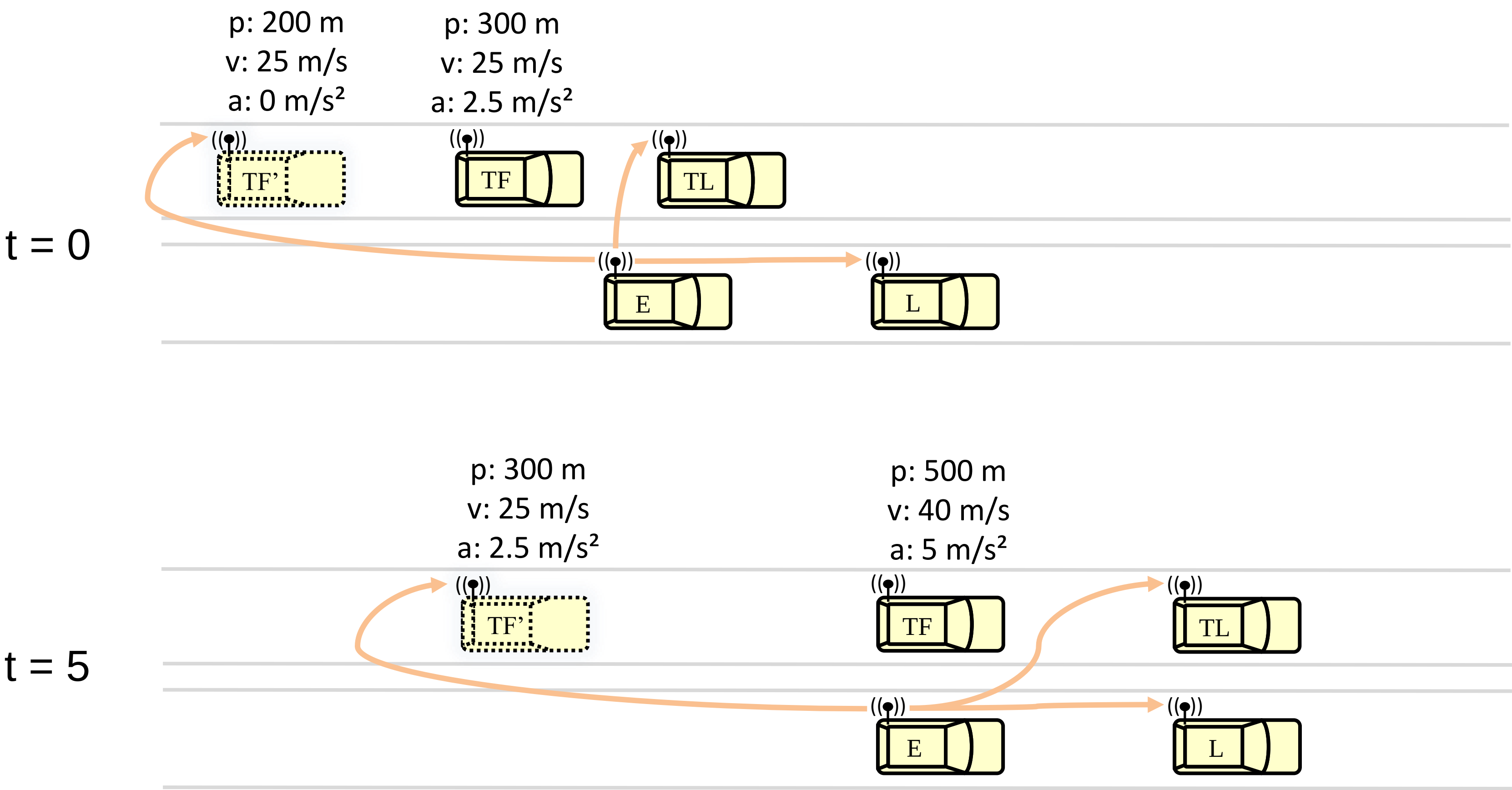
- ❑ Anomalous information about TL may indicate TL as TL'



Mistiming Trajectory Attack

- Anomalous vehicles transmit outdated data about themselves
- $r^{(t)} = \left[f_1^{(t)}, f_2^{(t)}, \dots, f_n^{(t)}\right]$
- $r'^{(t)} = \left[f_1^{(t)}, f_2^{(t)}, f_3^{(t)}, f_4'^{(t)}, f_5'^{(t)}, \dots, f_{n-2}'^{(t)}, f_{n-1}'^{(t)}, f_n'^{(t)}\right]$
- $f'^{(t)} = \begin{cases} f^{(t-\Delta t)}, & \text{if the vehicle is anomalous} \\ f^{(t)}, & \text{if the vehicle is normal} \end{cases}$

Mistiming Trajectory Attack Example

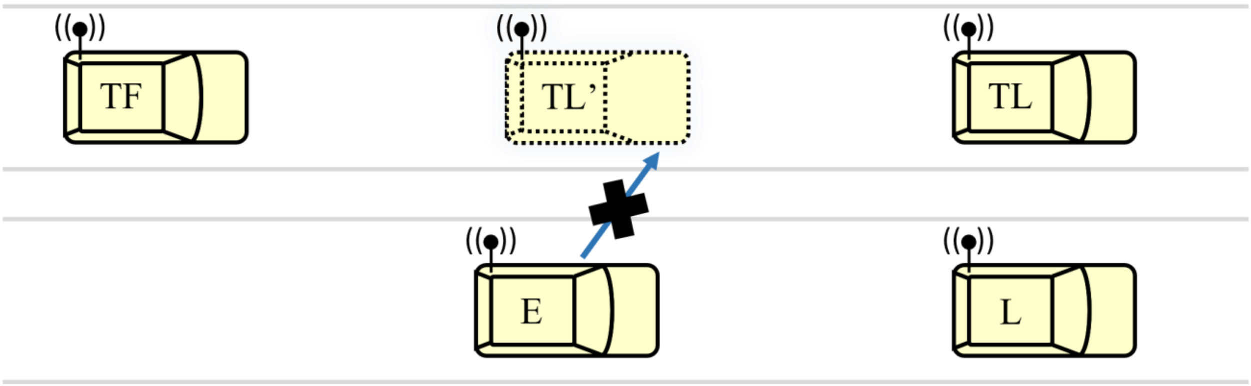


Data Selection: Overview

- We select the lane-changing scenarios that have greater importance
  - The leading vehicle on the target lane blocks the lane-changing route
  - The following vehicle on the target lane blocks the lane-changing route
  - Colliding with the leading vehicle on the target lane during a lane-changing maneuver
  - Colliding with the following vehicle on the target lane during a lane-changing maneuver
- We do not select scenarios that the leading vehicle is anomalous vehicle

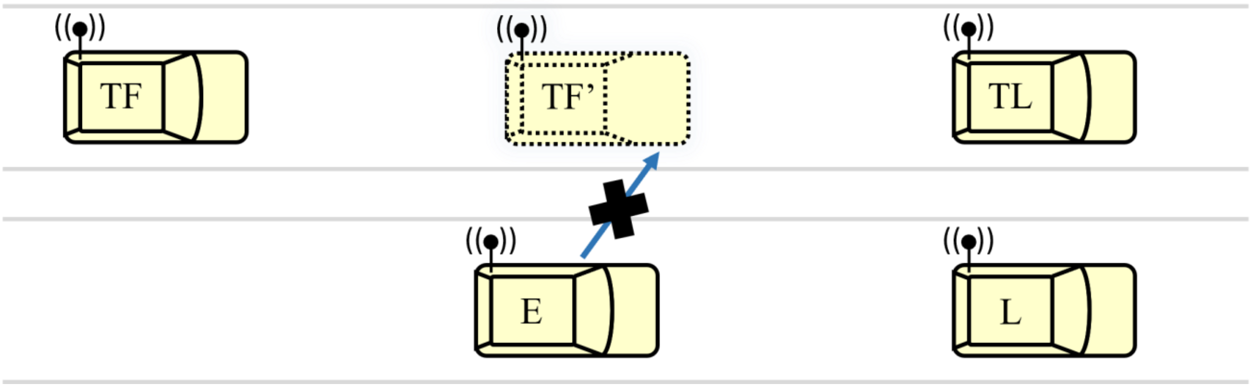
Data Selection: Case 1

- The leading vehicle on the target lane blocks the lane-changing route



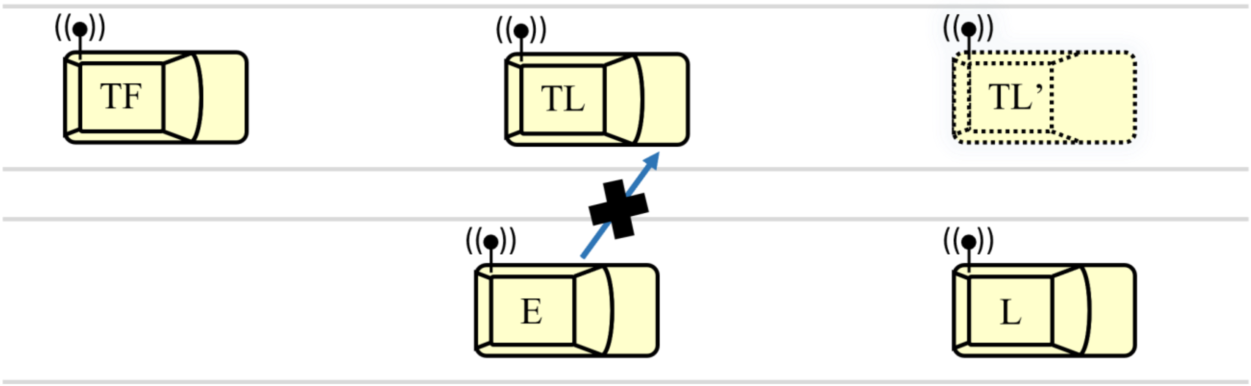
Data Selection: Case 2

- The following vehicle on the target lane blocks the lane-changing route



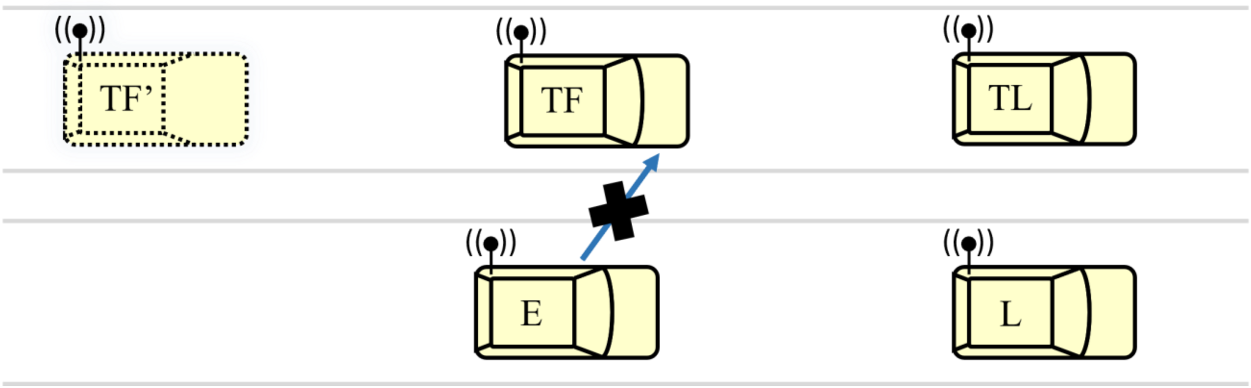
Data Selection: Case 3

- Colliding with the leading vehicle on the target lane during the lane-changing maneuver



Data Selection: Case 4

- Colliding with the following vehicle on the target lane during the lane-changing maneuver



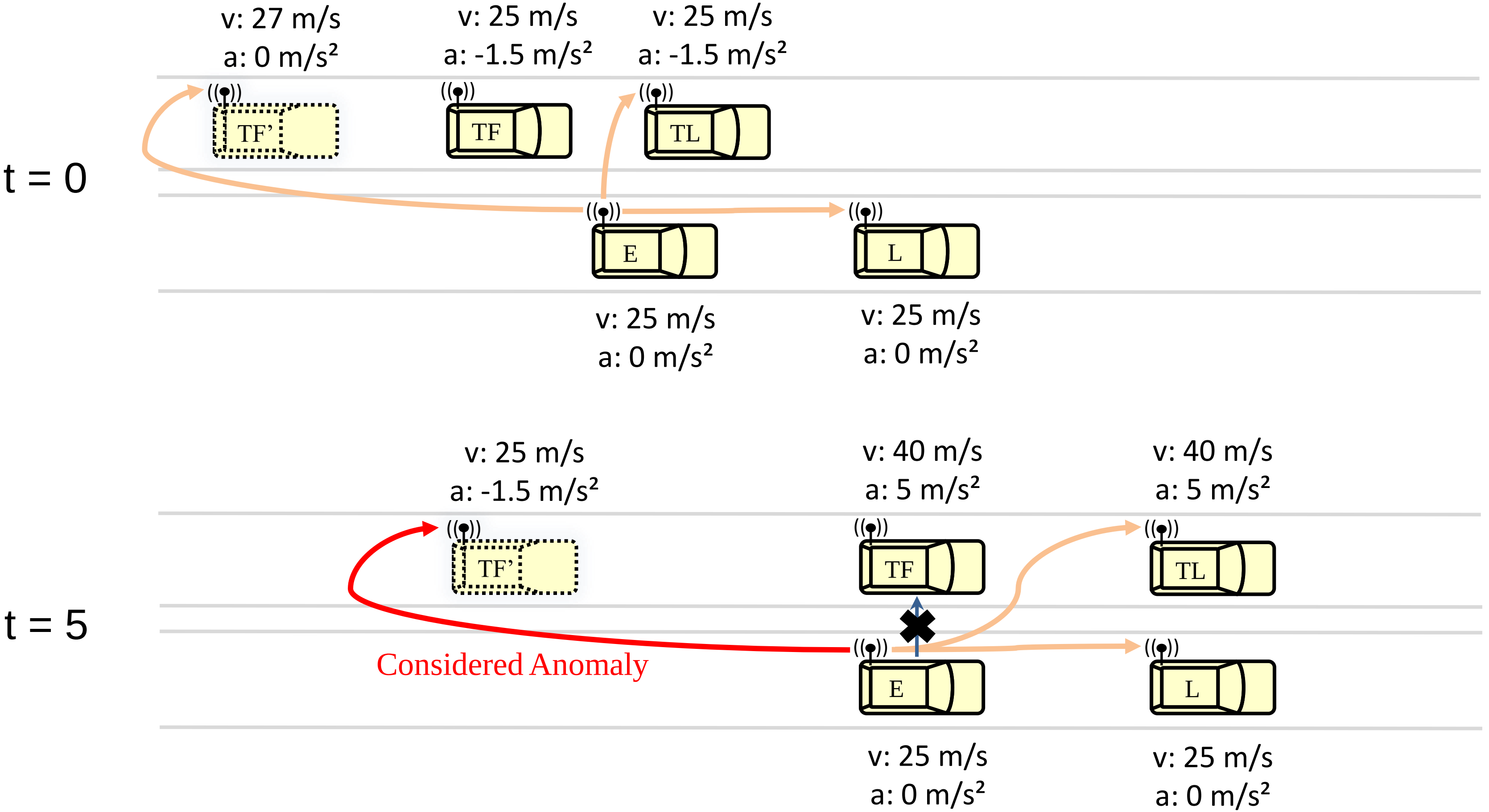
Detection Goal (1/2)

- $\mathrm{F(R)} = \begin{cases} 1, & \text{there is anomaly in R} \\ 0, & \text{there is no anomaly in R} \end{cases}$
  - $\mathrm{TP} = \{\mathrm{R'} \mid \mathrm{F(R')} = 1\}$
  - $\mathrm{FN} = \{\mathrm{R'} \mid \mathrm{F(R')} = 0\}$
  - $\mathrm{FP} = \{\mathrm{R} \mid \mathrm{F(R)} = 1\}$
  - $\mathrm{TN} = \{\mathrm{R} \mid \mathrm{F(R)} = 0\}$

Detection Goal (2/2)

- Both anomalous data and normal data have similar positional patterns
  - Detection models need to detect whether a vehicle performs the normal driving behavior
- Detection models detect whether the driving behavior of the vehicle is normal
  - Detect acceleration and velocity offsets
  - Detect whether information from the past aligns with the normal driving behavior at the current point in time

Detection Goal Example



Traffic Environments

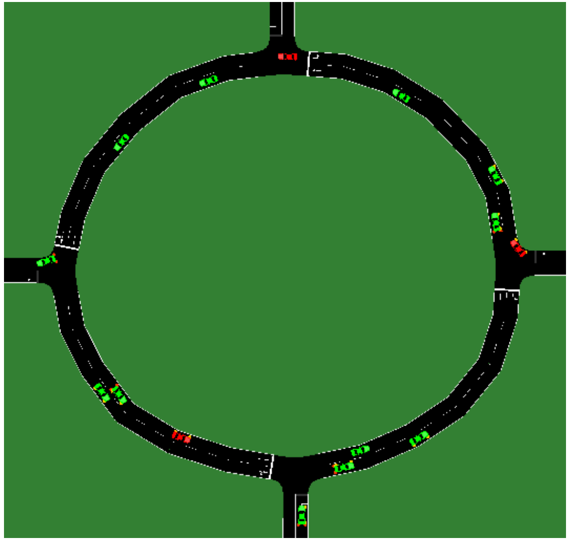
- Three traffic environments
  - Highway, roundabout and opposite overtaking
  - Provide a broader range of scenarios analysis
- Different driving behavior in traffic environments

Highway

- Heavy traffic flow
  - Frequent lane changing by vehicle in order to maintain a smooth flow of traffic
- High level of safety
  - Vehicles traveling at high speed on a highway can have life-threatening accidents with a single operational mistake

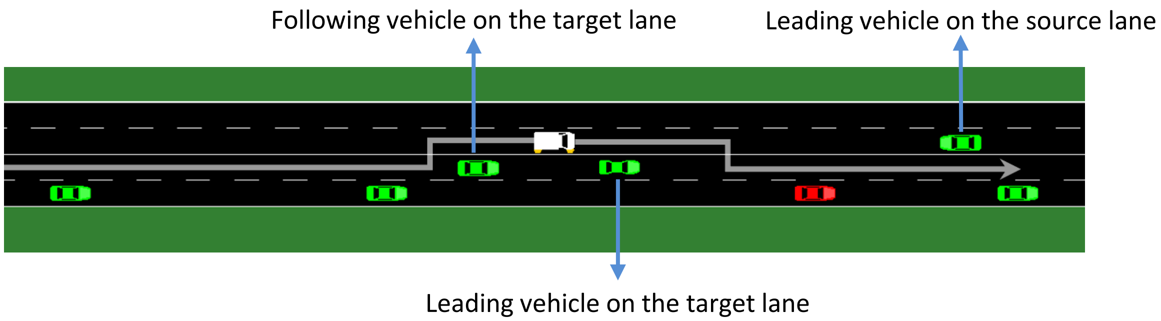
Roundabout

- Frequent lane changing
  - Vehicles drive on the inner lane during general circulation and change to the outer lane for leaving
- Exit-related driving behavior
  - Vehicles have frequent accelerations and decelerations when they near exits



Opposite Overtaking

- ❑ **Dangerous situation**
  - ➢ Put both the oncoming vehicles (leading vehicle) and the overtaking vehicle itself in significant danger
- ❑ **Inconsistent driving behavior**
  - ➢ Vehicles perform unusual driving behavior when they encounter the emergency events

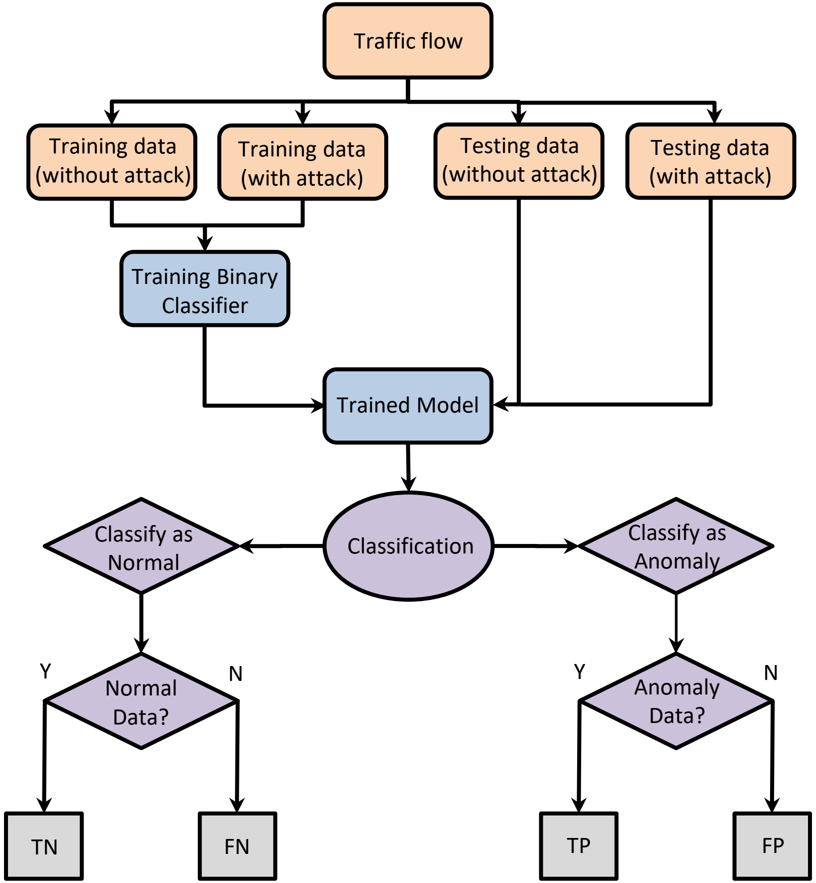


Outline

- ❑ Introduction
- ❑ Problem Formulation
- ❑ **Proposed Approaches**
- ❑ Experimental Results
- ❑ Conclusion

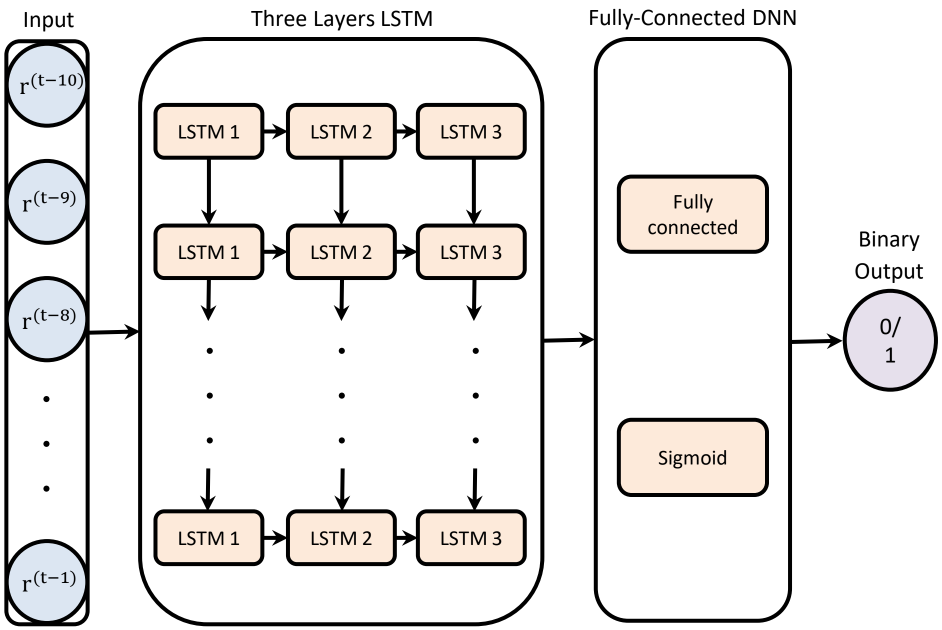
Classifier Approach

- ❑ Binary classification
- ❑ Propose two deep-learning-based models
  - ➢ Long Short-Term Memory based RNN
  - ➢ Deep Neural Network
- ❑ Two machine-learning-based models / Rule-based model
  - ➢ Mainly for the comparison of deep-learning-based models



Long Short-Term Memory (LSTM)

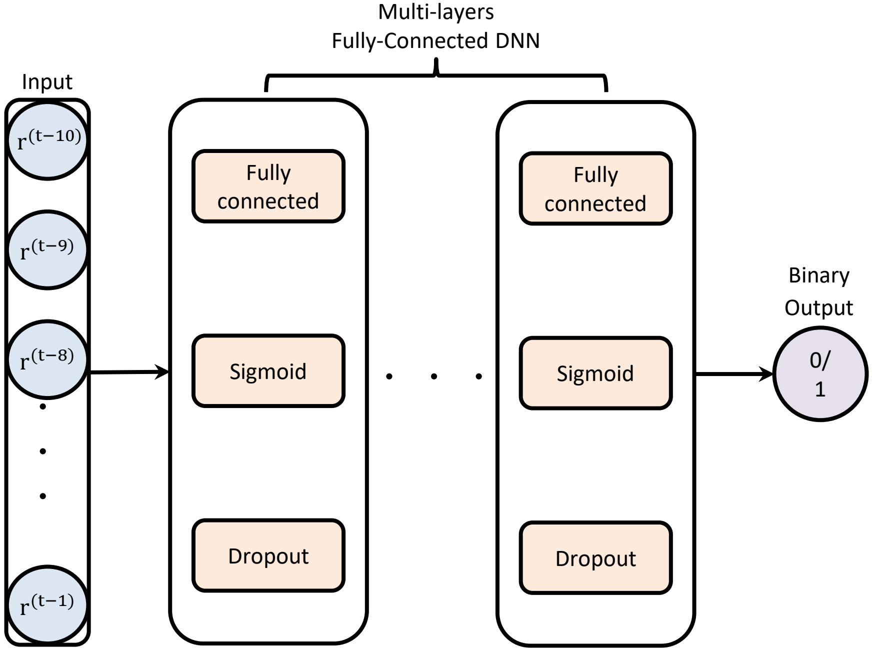
- LSTM is well-suited for processing time-series data
  - LSTM layer contains memory units that can capture and retain the long-term dependencies
- The long-term dependencies
  - How the behavior of a vehicle is affected by the surrounding vehicles



Deep Neural Network (DNN)

❑ DNN is able to detect the abnormal driving behavior

- DNN can detect the abnormal driving behavior by significant differences in speed, position, or acceleration compared to surrounding vehicles



Outline

- ❑ Introduction
- ❑ Problem Formulation
- ❑ Proposed Approaches
- ❑ **Experimental Results**
- ❑ Conclusion

Setting

- All the experiment are running on the desktop with Intel Core i7-9700 CPU, and NVIDIA-2080Ti GPU
- Use SUMO **(S**imulation of **U**rban **MO**bility**)** to generate training and testing data
- Three traffic environments are used in the simulation

SUMO

- SUMO is a simulation platform
  - 5000 training data and 1000 testing data in highway and roundabout
  - 1500 training data and 300 testing data in opposite overtaking
  - 1:1 ratio between normal data and anomaly data
- Directly deploy the attacks into simulation
  - Generate data to better reflect the real-world scenarios

Comparative Models

- Support Vector Machine (SVM)
  - Effectively handle high dimensional data and nonlinear problems
- Random Forest (RF)
  - High robustness and flexibility
- Rule-based model (RBS)
  - Physics rules
  - No sudden brake or acceleration

Results: Acceleration Bias Attack

- Deep-learning-based models outperform other models
  - LSTM better than DNN due to its model characteristics that can handle time series data
  - Rule-based model cannot detect the anomaly since our attacks are stealthy
- Longer data length leads to better result

Environment / Data Length	LSTM	DNN	SVM	RF	RBS
Highway / 5	0.92	0.86	0.74	0.79	0.03
Highway / 10	0.95	0.92	0.72	0.80	0.04
Roundabout / 5	0.90	0.87	0.78	0.76	0.03
Roundabout / 10	0.94	0.92	0.77	0.77	0.05
Overtaking / 5	0.84	0.78	0.63	0.64	<0.01
Overtaking / 10	0.85	0.81	0.63	0.61	<0.01

Results: Acceleration Bias Attack

- **Highway**
  - The normal driving behavior on the highway is much stricter
  - Easier to detect the added attack offset on acceleration and velocity
- **Roundabout**
  - Vehicles have frequent acceleration and deceleration near exits
  - Harder to detect the added attack offset on acceleration and velocity
- **Opposite overtaking**
  - Vehicles accelerate and decelerate to provide sufficient spaces for the opposite overtaking vehicles

Results: Mistiming Trajectory Attack

- ❑ Deep-learning-based models outperform other models
- ❑ Longer time step intervals lead to better results
  - ➢ The larger differences in driving behavior

Environment / Time step intervals	LSTM	DNN	SVM	RF	RBS
Highway / 10	0.72	0.66	0.60	0.51	<0.01
Highway / 20	0.81	0.72	0.63	0.56	<0.01
Roundabout / 10	0.86	0.83	0.65	0.64	<0.01
Roundabout / 20	0.89	0.84	0.71	0.67	<0.01
Overtaking / 10	0.70	0.61	0.61	0.59	<0.01
Overtaking / 20	0.75	0.65	0.64	0.60	<0.01

Results: Mistiming Trajectory Attack

- Highway
  - Some of the data are not ideal
- Roundabout
  - Driving behavior is more likely to be affected by surrounding vehicles
- Opposite overtaking
  - The inconsistency of driving behavior makes it difficult to classify

Runtimes

- The testing time of detection models are not longer than 0.21 milliseconds per data
  - Suitable for real-time systems

Model	LSTM	DNN	SVM	RF
Training Time (minutes)	14	15	2	3

Model	LSTM	DNN	SVM	RF
Testing Time per Data (milliseconds)	0.21	0.07	0.03	0.05

Outline

- ❑ Introduction
- ❑ Problem Formulation
- ❑ Proposed Approaches
- ❑ Experimental Results
- ❑ **<u>Conclusion</u>**

Conclusion

- Propose stealthy attacks
  - Cannot be detected by a rule-based model
- Propose deep-learning-based models for anomaly detection
  - The models achieve decent detection performances against the anomaly
- Have a general anomaly detection workflow
  - The workflow can be used in different lane-changing environments
  - Analyzing the driving behavior in three different traffic environments
- Deploy the attacks directly into SUMO during the simulation
  - Generate data to better reflect the real-world scenarios
  - Establish the standards and specifications for the operations in SUMO

Future Work

- Explore more efficient detection approaches
  - Convolutional Neural Networks model (CNN)
  - Generative Adversarial Networks model (GAN)
- Explore powerful attack models
  - Collaborative Attacks
- Take actions after detecting the anomaly
  - Make vehicles stay away from anomalous vehicles

Q&A

Thank You!