Location Anomalies Detection for Connected and Autonomous Vehicles

Xiaoyang Wang[1], Ioannis Mavromatis[1], Andrea Tassi[1], Raúl Santos-Rodríguez[1] and Robert J. Piechocki[1,2]

[1] University of Bristol, Bristol, UK
[2] The Alan Turing Institute, London, UK
{xiaoyang.wang, ioan.mavromatis, a.tassi, enrsr, r.j.piechocki}@bristol.ac.uk

23/09/2019 @ Honolulu, Hawaii

Content

Background

Data Generation

Methodology

Experiments

Conclusion

Content

Background

Data Generation

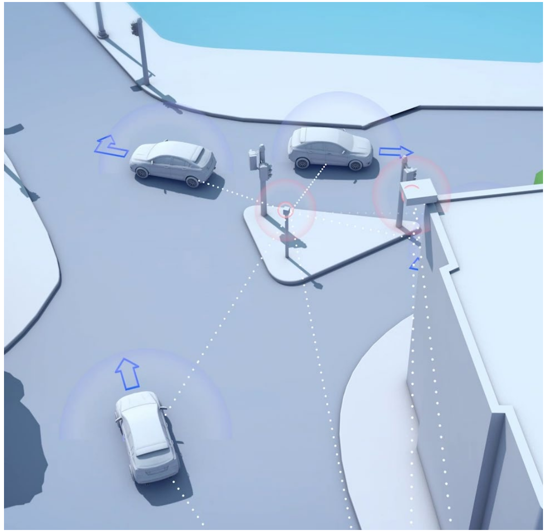
Methodology

Experiments

Conclusion

Background

- Connected and Autonomous Vehicles (CAVs), more generally Intelligent Transportation Systems (ITS) will form highly interconnected system
- CAVs collect and disseminate information
- Safety of vehicles relies on the knowledge from connected environment – no constant human intervention
- Early stage anomaly detection a key security feature
- Self-reported location (CAM/BSM) anomalies



Vehicles sharing locations and driving intentions[1]

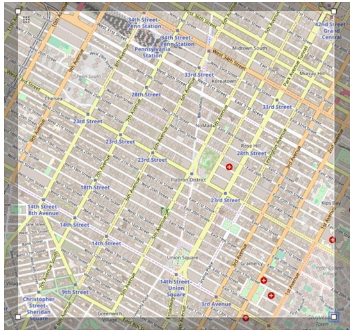
[1] http://www.flourishmobility.com/gallery

Previous Work

- SMARTER - Simulation Framework for City-Scale Experimentation[1,2]

Area-of-Interest

City Map



Simple Road

Traffic

Vehicles

Pedestrians

Indoor Users

Technologies

Wireless Technologies

MIMO

Antennas

Realism

Start/End Time

Tile Size

Tile Shape

Area Size

Simplification Tolerance

.
.
.

[1] https://github.com/ioannismavromatis/smarterSimulator

Content

Background

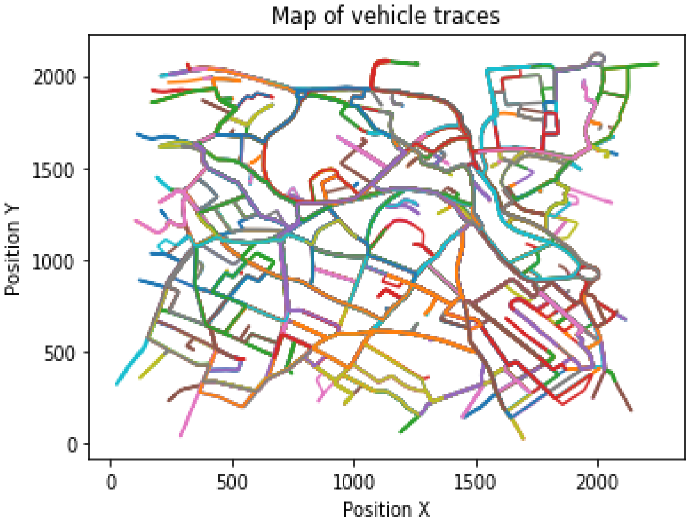
Data Generation

Methodology

Experiments

Conclusion

Simulation Scenario



- ~2km * 2km area in central Bristol, with ~150 vehicles driving for ~2,000s
- Each vehicle generate one beacon per second – an UPD packet of 140B
- Broadcasting to surrounding vehicles
- IEEE 802.11p transceiver, 5.9 GHz

Content

Background

Data Generation

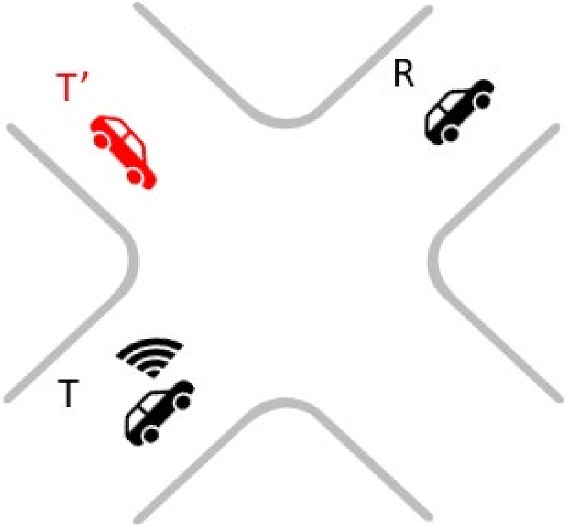
Methodology

Experiments

Conclusion

Problem Description

Self-reported CAV locations (contained in CAM/BSM)



T – Transmitter
R - Receiver

T' - Falsified location

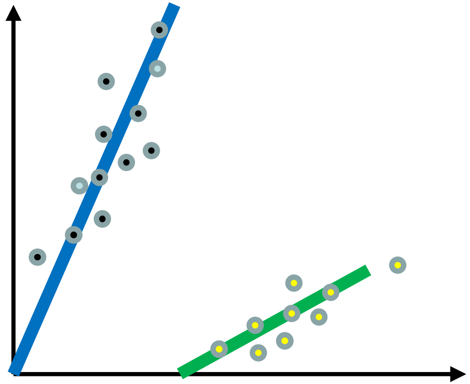
- A self-learning system for self-location anomaly detection
- Received Signal Strength Indicator (RSSI)
- State description:

$$X = [l_R, V_{\mathrm{RSSI}}, l_{T(T')}] \in R^{1\times 5}$$

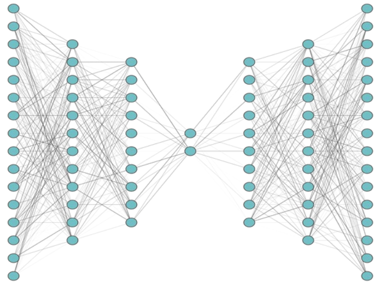
Methodology

Unsupervised learning

- Data/pattern mining
- No labels required
- Less human intervention



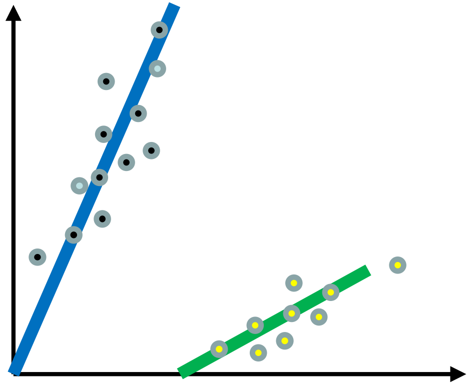
Autoencoder



Methodology

Unsupervised learning

- Data/pattern mining
- No labels required
- Less human intervention

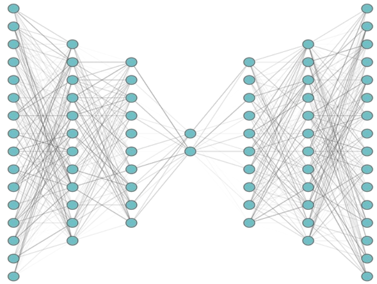


Autoencoder

Training

Novelty-free

$X \longrightarrow$

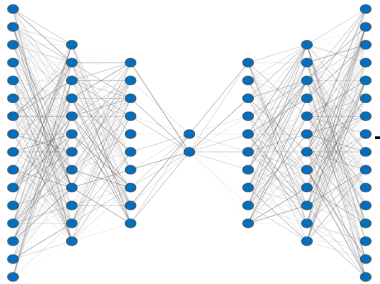


$\longrightarrow X'$

Goal: $\min |X' - X|$

Anomaly detection

$Y \longrightarrow$

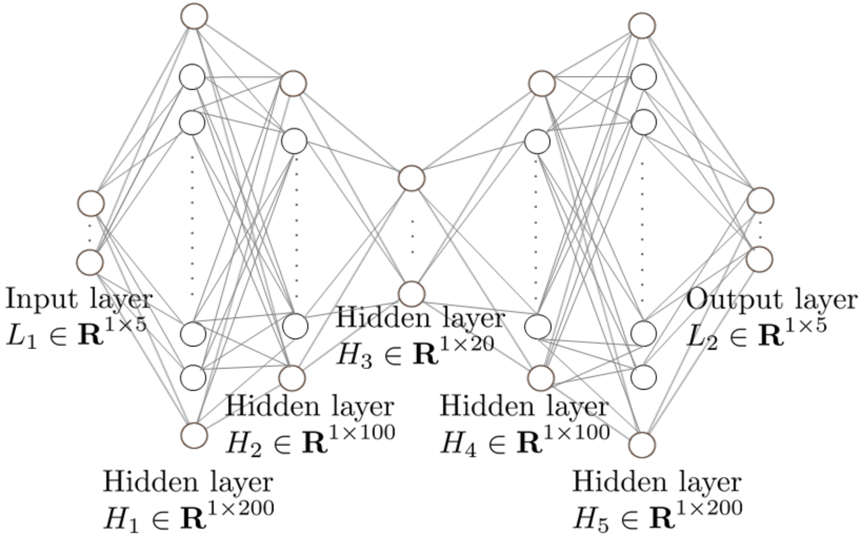


$\longrightarrow Y'$

Trained autoencoder

$\text{error} = |Y' - Y|$

Methodology



The seven-layer, fully-connected deep autoencoder structure designed in this work

Parameters	Value
Bottle neck size	20
Learning rate	0.00095
Number of layers	7
Training epochs	1000

Content

Background

Data Generation

Methodology

Experiments

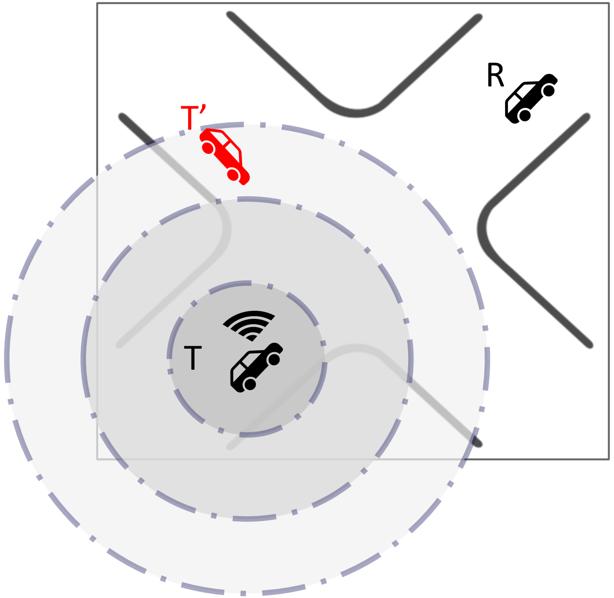
Conclusion

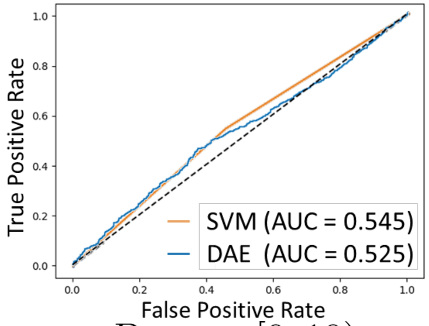
Experiments

- Anomaly data
  - Generating falsified TX locations T'
  - RX locations and RSSI remain untouched
- Evaluation Metrics – Receiver Operating Characteristic (ROC) curve
  - False Positive vs True Positive
  - Area Under Curve
- Baseline Method – One Class SVM
  - A classic unsupervised method for anomaly detection

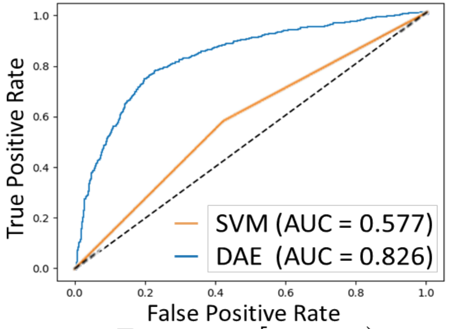
Experiments

- $D_{T,T'}$, the distance between real TX and the falsified TX (meters)

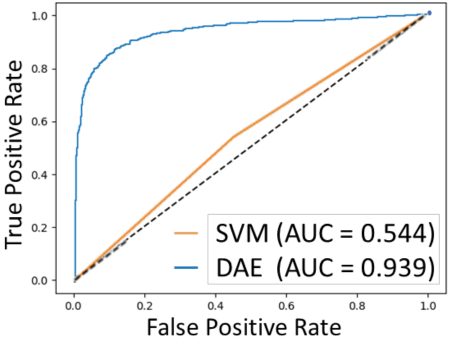




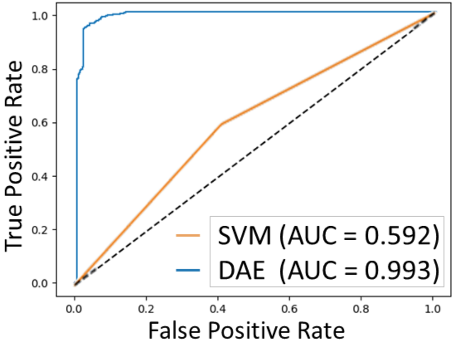
$D_{T,T'} \in [0, 10)$



$D_{T,T'} \in [30, 40)$

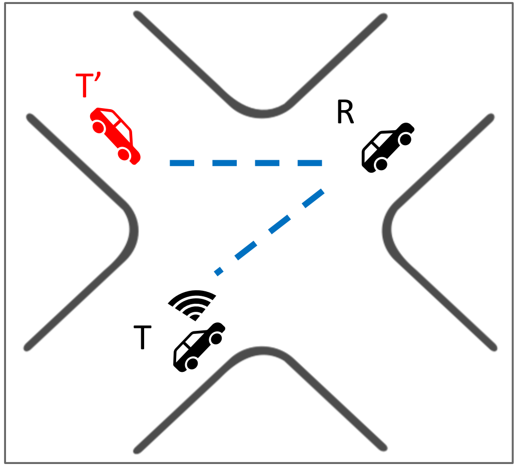


$D_{T,T'} \in [50, 100)$

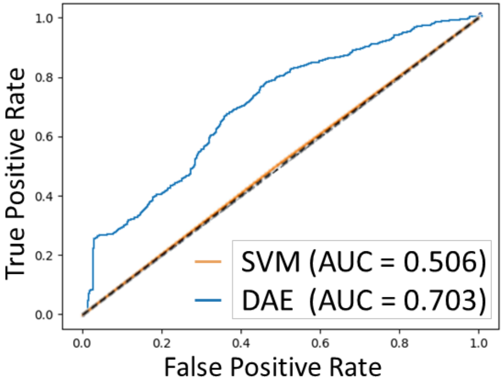


$D_{T,T'} \in [100, 500)$

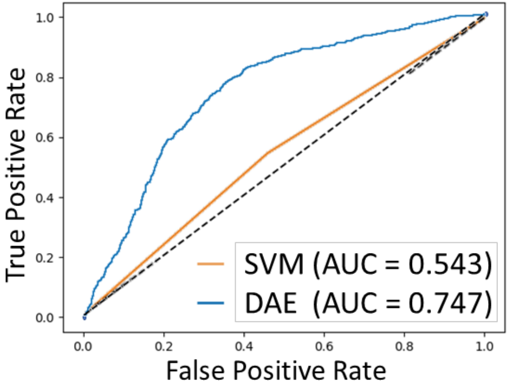
Experiments



- When $|D_{T',R} - D_{T,R}| < \epsilon$



$D_{T,T'} > 30\text{m}$
while $|D_{T',R} - D_{T,R}| < 1\text{m}$



$D_{T,T'} > 30\text{m}$
while $|D_{T',R} - D_{T,R}| \in [10, 20]\text{m}$

Content

Background

Data Generation

Methodology

Experiments

Conclusion

Conclusion and Future Work

- Autoencoder-based approach

  Self-learning approach for self-reported location anomaly detection

- The limitation of using only locations and RSSI

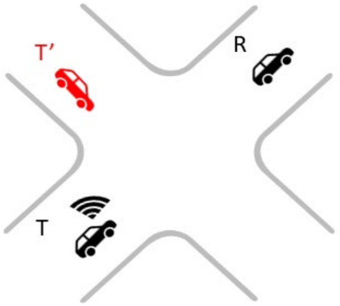
- Early state anomaly detection could help improve the security of CAVs

- Further improve the performance on more “smarter” anomalies

This work is partially funded by the Next-Generation Converged Digital Infrastructure (NG-CDI) Project, supported by British Telecommunications Group and Engineering and Physical Sciences Research Council (EPSRC), Grant ref. EP/R004935/1. It was also supported in part by the Innovate UK Grant No. 102582 (Flourish Project).

Thanks!

Q&A



{xiaoyang.wang, ioan.mavromatis, a.tassi, enrsr, r.j.piechocki}@bristol.ac.uk