The impact of Machine Learning Security on the resilience of Connected Autonomous Vehicle Architectures

Background and motivation

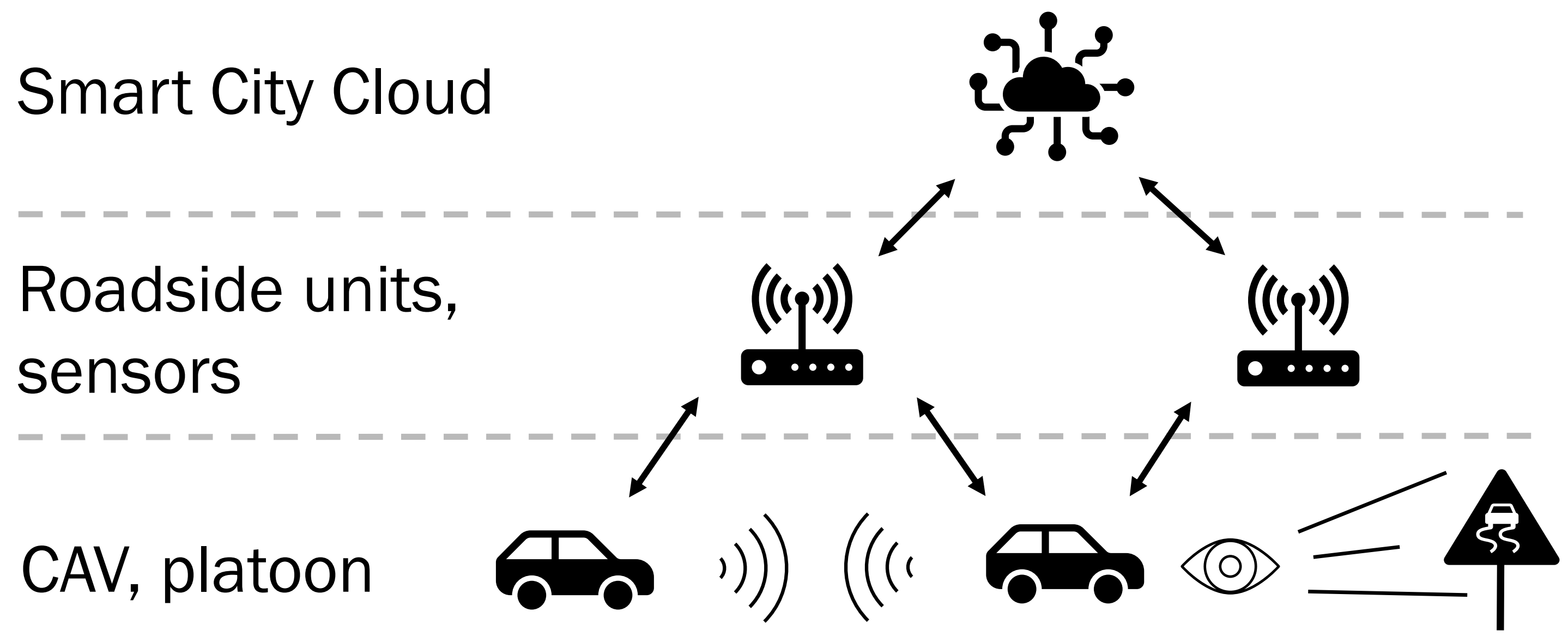
The future integration of Connected Autonomous Vehicles (CAV) into Smart Cities will benefit mobility, efficiency and safety. At the heart of both Smart Cities and CAV is the use of various machine learning models for analytics and control.

However, machine learning introduces security risks and in a highly connected environment that could impact the operation of CAV. Architects may want to ask what are the risks of introducing machine learning at different places in a CAV architecture. Attacks on CAV can impact the safety of passengers, pedestrians and the mobility systems of a city. CAV presents a complex dynamic and connected system of machine learning models. In this system, we need to consider the cascading impacts of attacks on the different machine learning systems and assess the resilience of CAV systems.

Therefore, how resilient is machine learning and how does it affect the complex systems of CAV?

Objectives

1. Evaluate the applications of machine learning models and their security issues in CAV
2. How can resilience of machine learning security be measured to inform threat models?
3. How can machine learning resilience measures be used to model the resilience of a CAV architecture?
4. How can the strengths and weaknesses of a CAV security model architecture be assessed?
5. What are the impacts of attacks on machine learning in a CAV security model architecture?



Smart City Cloud

Roadside units, sensors

CAV, platoon

Challenges

- Different dimensions of machine learning to consider in security assessments,
  - Data preprocessing
  - Feature selection
  - Algorithms and models
- Comparable resilience measures between different model types
- Impact of security and performance tradeoffs
  - Requirement for real-time decision-making
  - Transparency and accountability

Methodology

Phase 1: Desk based research

- Analysis of literature to inform and formalise resilience measures
- Analysis of CAV architectures

Phase 2: Experimentation and model building

- Experimentation of techniques such as graph theory, game theory or traffic simulators where dynamics of the system is determined by the resilience measures
- Investigate adversarial behavior modelling

Phase 3: Evaluation of models

- Utilise the finalized experimentation methods or strategies to investigate the impact of machine learning resilience

Outcomes

- Resilience measure(s) for machine learning models
- Technique for modelling the resilience of CAV architectures

Winston Ellis

winston.ellis@bristol.ac.uk

Supervisors: Dr Sana Belguith, Professor Theo Tryfonas

University of BRISTOL

Bristol Cyber Security Group