Cyber security in connected autonomous vehicles

As part of an Innovate UK funded project, the STFC Hartree® Centre worked with Chilton Computing, Huduma and Oxfordshire County Council as part of a consortium focusing on cyber security in connected autonomous vehicles.

Challenge

Advances in automotive technology have paved the way for organisations to explore connected vehicles, usually with their own internet connection that allows cars to exchange data with other devices such as navigation and entertainment systems. Connected and autonomous vehicles (CAVs) bring a range of possible challenges such as communication with other vehicles and external infrastructure. This potentially makes CAVs susceptible to cyber attacks making it crucial to incorporate cyber security considerations in to their future development.

Approach

Hartree Centre’s data science team used statistical methods to analyse publicly available data on various types of cyber attack, extracting the probability of occurrence. To address questions surrounding the use of cyber security in CAVs, the team used a game theoretic simulation methodology to describe a decision-making process for CAV designers as to whether they should invest. This incorporated results of the data analysis performed in the cyber attack dataset alongside practical considerations such as the impact of a potential cyber attack on the company to help guide decision making.

Benefits

This work was able to address a challenging issue by quantifying the security level of a CAV system. The team were able to develop a model for data-driven decision making in a CAV framework during a short, three month project. The proposed methodology to model decision making can easily be extended to facilitate additional factors that automotive companies might wish to take into account going forward. An example of this is the cost of a cyber security solution, both in terms of actual cost or whether solutions are compatible with existing software. Additionally, if CAV related cyber security data are made available, the results from analysis of these data can be used to further enhance the proposed game theoretic model for decision making.

“Working with Hartree Centre has enabled our company to take a fresh look at our computational approach for cyber risk assessment for the CAVs.”

Erica Yang
Chilton Computing

www.hartree.stfc.ac.uk
Demonstrates that analysis of cyber security data sets can be used as inputs to the decision-making processes.
Methodology can be generalised to accommodate input data resulting from cybersecurity threats directly related to CAVs.

- Statistical methods used to analyse public server log data.
- A game-theoretic approach was used to describe the interactions between attackers and defenders in the CAVs setting.

### Who we are
- 60+ computational scientists and technologists
- World-leading supercomputing and AI infrastructure
- Bespoke small teams built around your project
- Tailored business development support
- Access to our network of industry, academic and technology partners

### What we do
- Boost productivity and enhance innovation for industry
- Big data analytics and artificial intelligence (AI)
- High performance computing and quantum simulation
- Training and skills development
- Insights into emerging technologies

### Our impact on UK industry and society
The Hartree Centre was created by UK Government to transform industry by accelerating the adoption of high performance computing (HPC), big data analytics and artificial intelligence (AI) technologies. We play a key role in realising UK Government’s Industrial Strategy by stimulating applied digital research and innovation, creating value for the organisations we work with and generating economic and societal impact for the UK.

The Science and Technology Facilities Council (STFC) Hartree Centre is part of UK Research and Innovation.

www.hartree.stfc.ac.uk