STRICT - Cyber Security Solutions for Smart Traffic Control Systems

PI: Long Tran-Thanh, University of Southampton, UK
Contact: l.tran-thanh@soton.ac.uk

Co-I: Nicholas R. Jennings, Imperial College London, UK

Singaporean Collaborators:

Co-PI: Bo An, SCE, NTU
Co-I: Mo Li, SCE, NTU

03rd July, 2018
Background: Smart Traffic Control Systems

- **Traffic congestions in large cities**
  - High noise
  - Air pollution
  - Waste of traffic time

- **Smart traffic control systems**
  - Green Link Determining (GLIDE) System, Singapore
  - Allocates green time for motorists and pedestrians based on demand
  - Provides "green wave" link between adjacent junctions
Cyber Security Threats

- **Cyber Attacks**
  - E.g., hack the sensors and send fake data to the controller, remotely hack into the controller and take control.
  - Example from Hollywood movies
  - Real-world example
    - Israeli students attacked Waze APP with fake traffic jam in 2014

- **Challenges for preventing attacks in traffic control systems**
  - Human-agent heterogeneity
  - Robustness to strategic attackers
  - Adaptiveness
  - Decision making with limited resources
State of the Art, Objective and Key Idea

● Cyber security issues have been ignored
  ➢ Congestion control minimisation
  ➢ Passenger safety

● Research Objective

Model the traffic control systems and major attack scenarios, develop first generation approaches, and systems that can quickly detect the malicious behavior and effectively deploy security resources that will protect the system against a wide range of sophisticated strategic adversaries, build simulator and test bed to demonstrate the feasible and efficient of our approach

● Key idea

Game Theory

+ 

Machine Learning
Project Objectives

1. Identify major attack scenarios
   - 2a. Suspicious behavior detection mechanisms
   - 2b. Adaptive online defense mechanisms
   - 3. Game theoretic resource allocation algorithm
   - 4a. A smart traffic control systems simulator
   - 4b. Test bed implementation & validation

- Malicious behaviours detection algorithm
- Attacker action prediction algorithm
- Real testbed

25/05/2017
Attack Scenarios

● Device level
  ➢ Traffic data manipulation
  ➢ Traffic light manipulation

● Local control module level
  ➢ Coordinated data/traffic light manipulation in parts of the system

● System level
  ➢ Attack against resource management
Device Level Attacks

- **Traffic data manipulation**
  - Standard defense mechanism: outlier detection
  - Vulnerability analysis: data poisoning against outlier detection algorithms – published at GameSec’16
  - New defence mechanism (ML + game theory based) – to submit to IoTJ
  - Software based simulator

- **Traffic light manipulation**
  - Underlying mechanism: clustering
  - Vulnerability analysis: data poisoning against smart traffic light control systems – demo
Local System level Attacks

- **Pursuit Evasion Game**
  - Setting: escaper (e.g., robber) aims to leave the area a.s.a.p. – catchers (e.g., police forces) want to find the guy
  - Formulated as a Stackelberg game + proposed optimal solutions – published at IJCAI’17

- **Traffic routing manipulation**
  - Setting: self-interested traffic participant submits incorrect destination to traffic navigation system in order to gain benefit
  - Trustful navigation mechanisms – to submit to AAAI’18
System Level Attacks

- **Resource allocation dilemma**
  - Dollar Auction with spiteful players: in which both the defender and attacker has limited resources, and can decide how much they should use for the defense/attack
  - Goal: both maximise own utility + maximise opponent’s loss (not a zero-sum game)
  - Thorough analysis for players with deterministic strategies – published at AAAI’17