GPS SPOOFING ATTACK DETECTION ON INTERSECTION MOVEMENT ASSIST USING ONE CLASS CLASSIFICATION

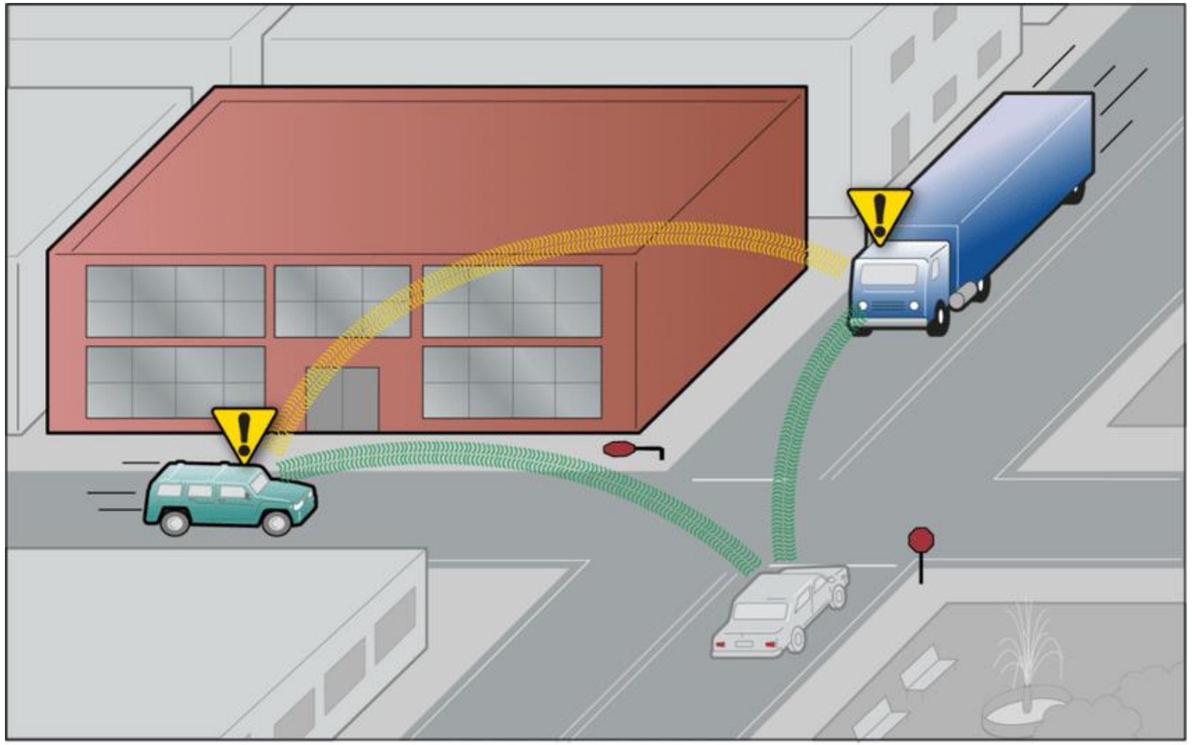
Jun Ying

Lyles School of Civil Engineering

Connected, Automated, and Resilient Transportation (CART) Lab

Introduction

Overview



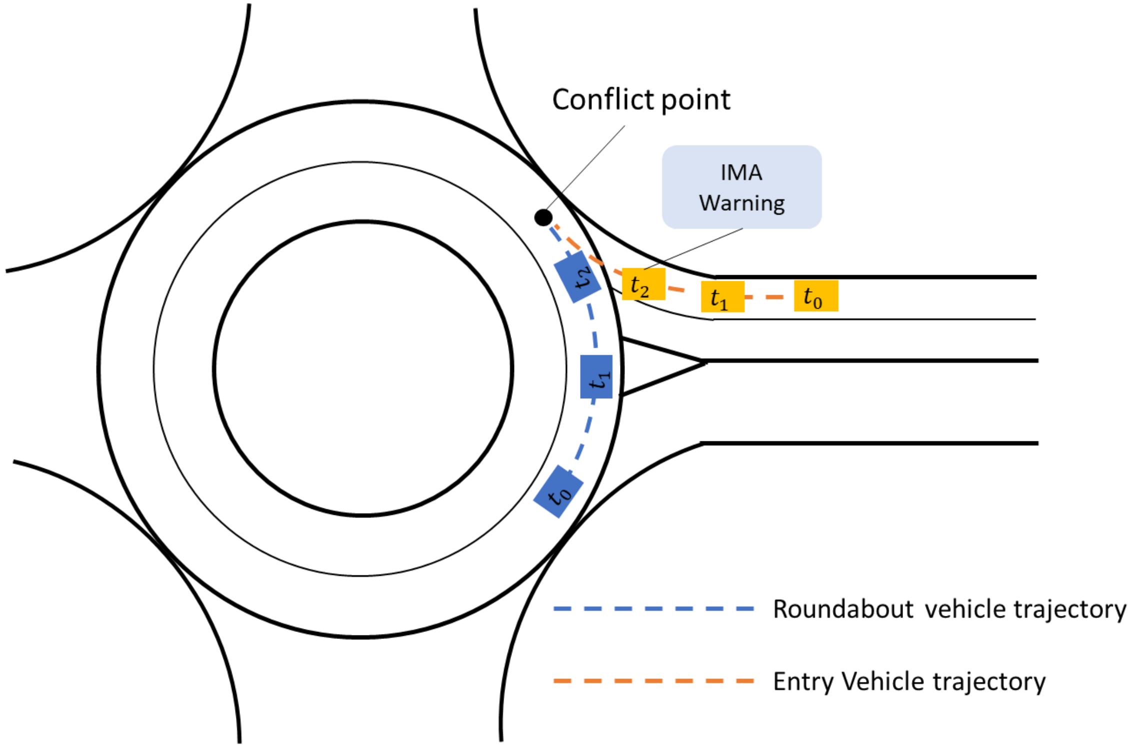
Source: GAO.

Emara, Karim. (2016). Safety-aware Location Privacy in Vehicular Ad-hoc Networks.

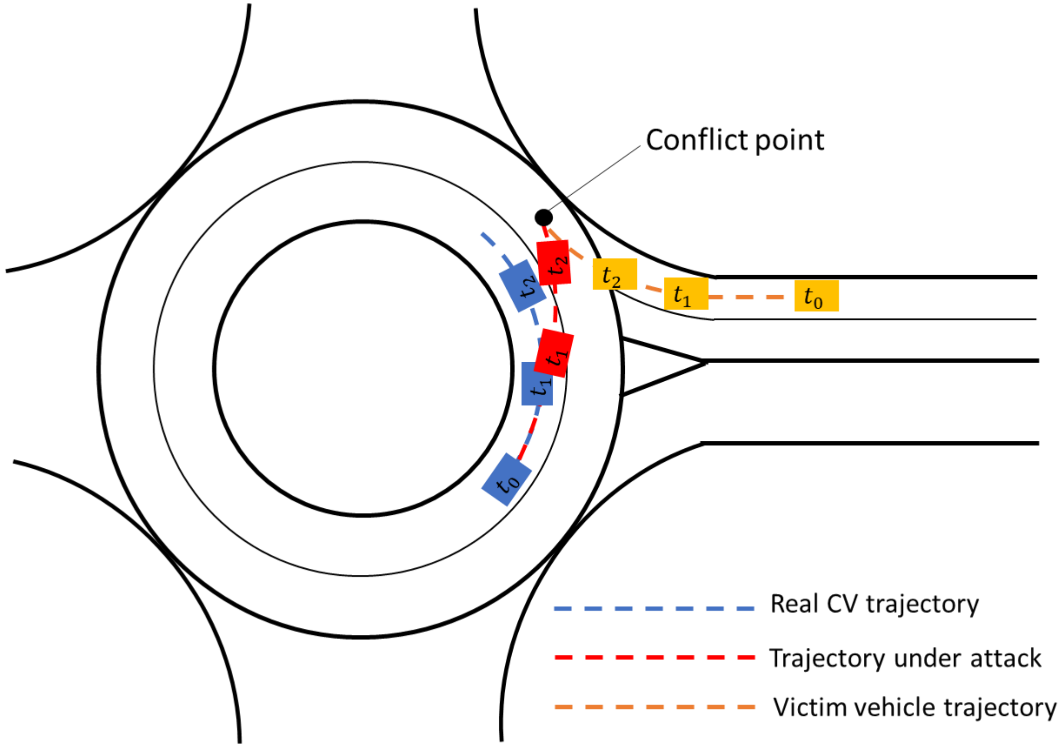
- GPS spoofing attack model
- Anomaly detection model

Threat Model

IMA warning application



CV threat model



Threat Model

Trajectory generation model

$minimize_s\ \theta^T f(s,u)$ (1)

$s.t.$

$vehicle\ dynamic\ constraints$

Objective function:

Acceleration: $f_1 = \frac{1}{N}\sum_i a_i^2.$

Heading rate : $f_2 = \frac{1}{N-1}\sum_i(\dot{\psi_i})^2.$

Curvature: $f_3 = \frac{1}{N}\sum_i \sqrt{(x_i - x^c)^2 + (y_i - y^c)^2}.$

→ Generate close to realistic trajectory

Lateral terminal point: $f_4 = (x_N - x^{con})^2.$

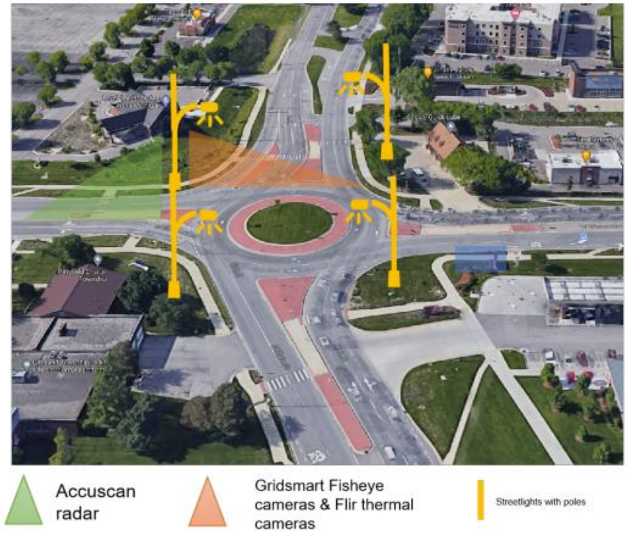
Longitudinal terminal point: $f_5 = (y_N - y^{con})^2$

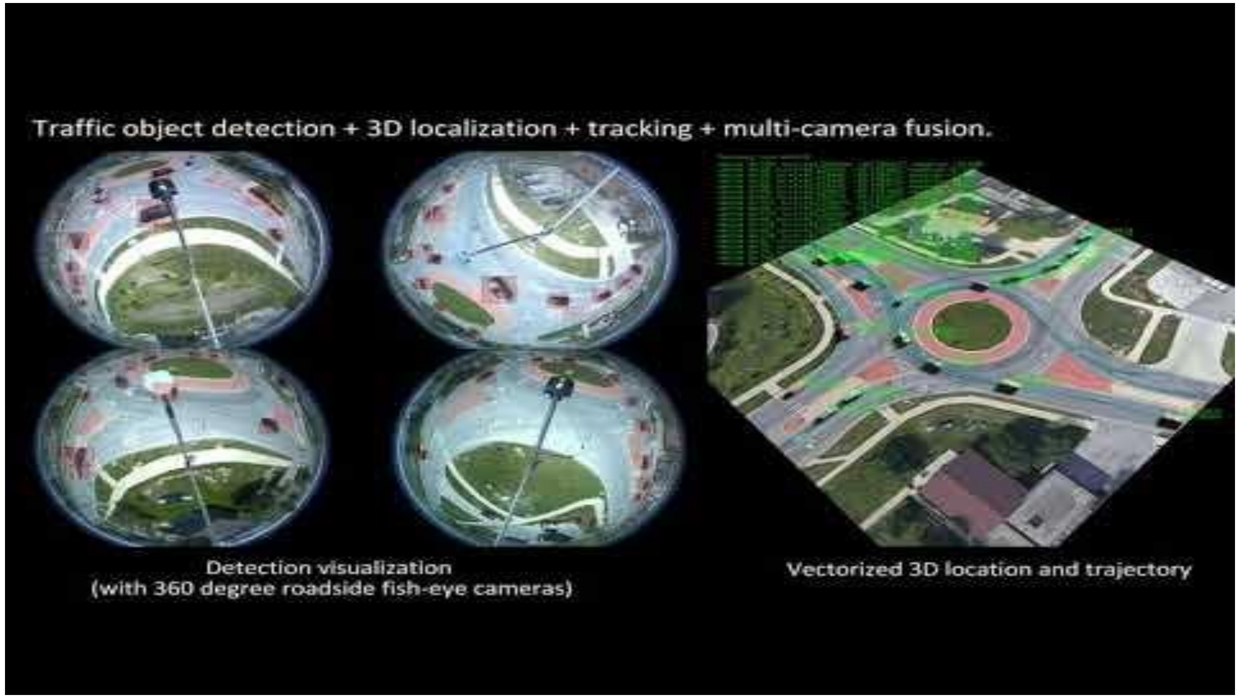
→ Trigger victim vehicle’s IMA warning

Data Set Description

Trajectory data collected from the State & Ellsworth roundabout at Ann Arbor, Michigan

- Time step 0.4s
- Vehicle location
- Speed
- Heading
- Acceleration
- Neighboring vehicle information



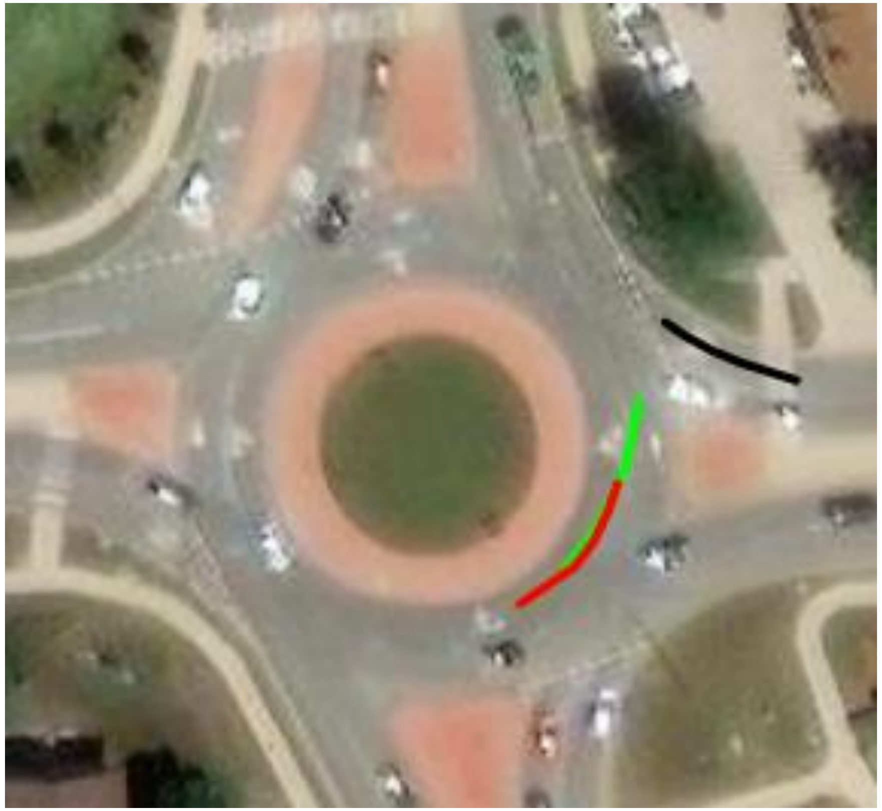

Traffic object detection + 3D localization + tracking + multi-camera fusion.
Detection visualization (with 360 degree roadside fish-eye cameras)
Vectorized 3D location and trajectory

Video Source: Michigan Traffic Lab

Zhang R, Zou Z, Shen S, Liu HX. Design, implementation, and evaluation of a roadside cooperative perception system. Transportation research record. 2022 Nov;2676(11):273-84.

CV Threat Model Experiments

Numerical Experiments

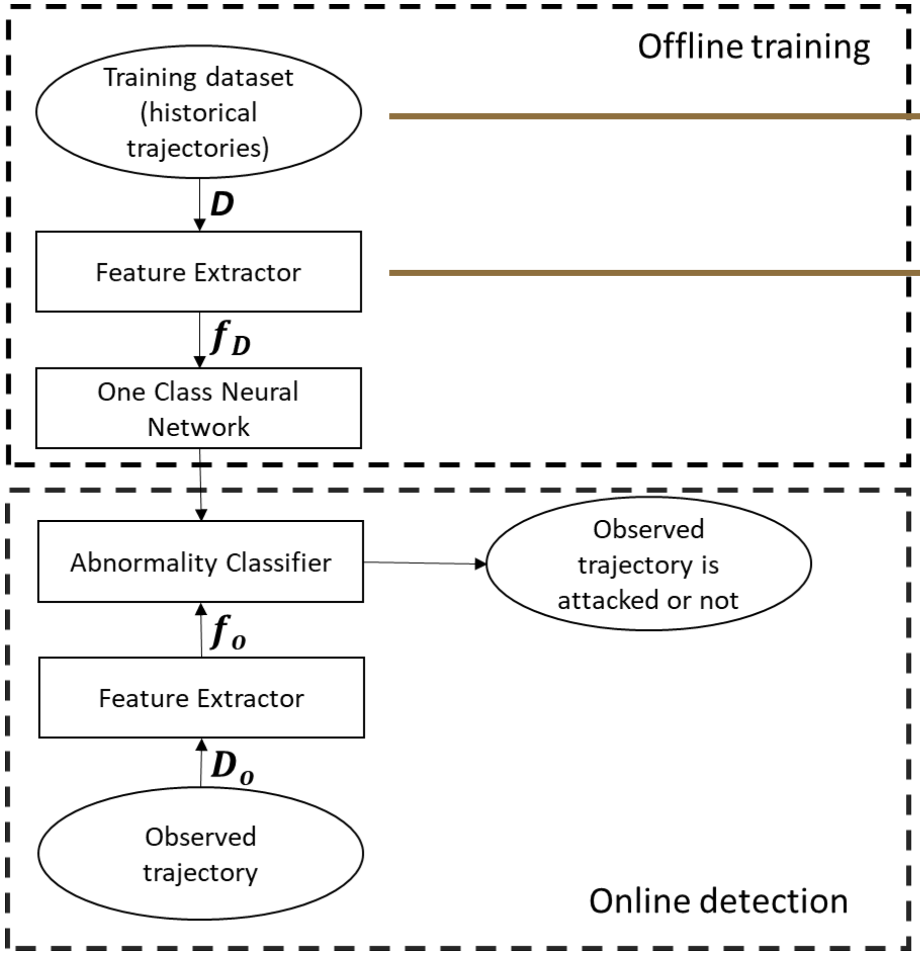


- 927 vehicle pairs
- Attack success rate:77.970%.
- Average attack success time: 1.71s.

🟥 Real vehicle trajectory
🟩 BSM trajectory under attack
⬛ Victim vehicle trajectory

Detection Methodology

Detection Framework

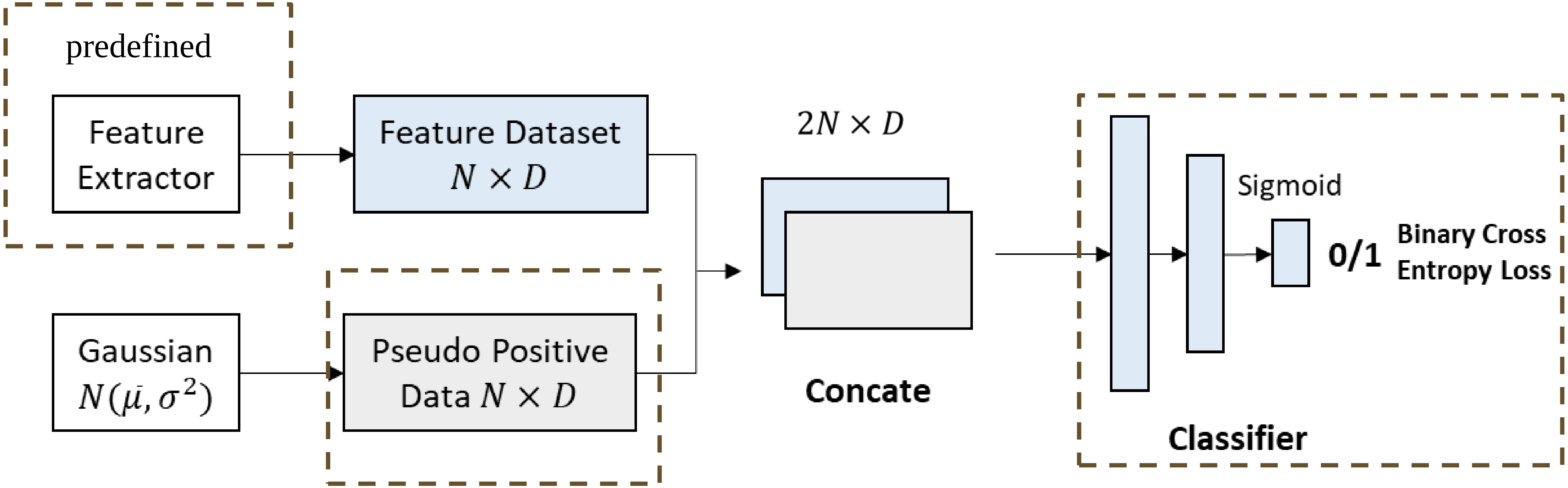


Historical normal trajectory

Map trajectory to feature vector

Detection Methodology

One class classification


predefined
Feature Extractor
Feature Dataset $N \times D$
Gaussian $N(\bar{\mu}, \sigma^2)$
Pseudo Positive Data $N \times D$
$2N \times D$
Concate
Sigmoid
0/1
Binary Cross Entropy Loss
Classifier

Detection framework evaluation

Offline detection

False positive rate: 8/1539 (0.52%)
False Negative rate: 2/490 (0.2%)

Online detection

False Positive Rate	False Negative Rate	Mean attack succeed time (s)	Mean detection time (s)	Mean time to attack succeed(s)
14/1539 (0.91%)	0/314 (0%)	2.096	1.600	0.497

Collaborators

Yiheng Feng
Purdue University
feng333@purdue.edu

Qi Alfred Chen
University of California at Irvine
alfchen@uci.edu

Z. Morley Mao
University of Michigan
zmao@umich.edu

Acknowledgement

Thank you!

Questions?

Contact: Jun Ying (ying29@purdue.edu), Yiheng Feng (feng333@purdue.edu)