Risk Assessment, Prediction, and Deterrence of Soft Target Threats

Prof. Jun Zhuang, University at Buffalo

Advanced Development for Security Applications - Workshop 27

November 15, 2023

So What? Who Cares?

- Space: *Soft targets and crowded places (e.g., schools , transportation systems)*
- Problem: *How to best define, assess, predict, and minimize risks and threats*
- Solution: *Developing interpretable machine learning and network simulation models; game-theoretical modeling; resource allocation models; model validation using human subject experiments*
- Results: *Risks and threats can be modelled and mitigated in STCPs.*
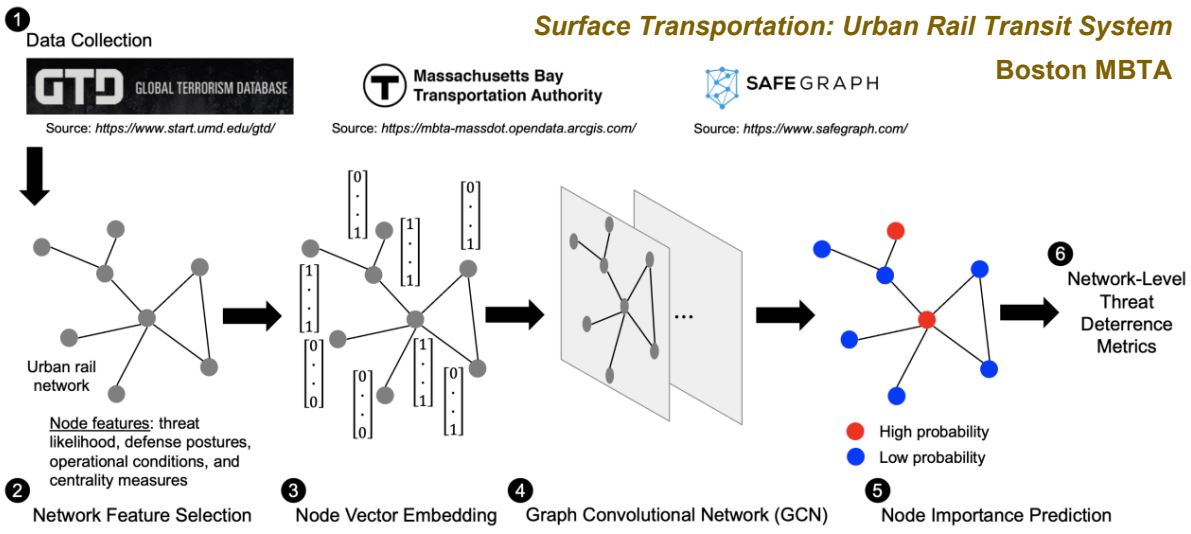- TRL: *3*

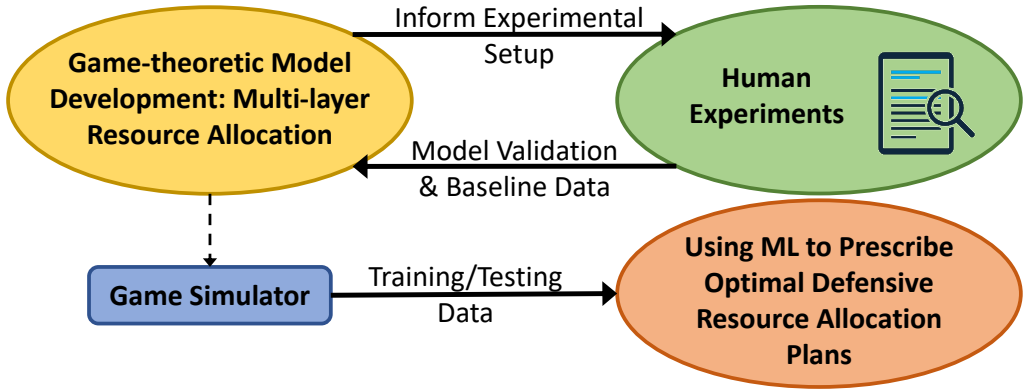# (RC): Threat Risk Assessment, Prediction and Deterrence

RC.1: Machine Intelligence for Effective Threat Deterrence and Risk Mitigation at Soft Targets and Crowded Places

Surface Transportation: Urban Rail Transit System

Boston MBTA

Objectives

Predict and assess threats to STCPs

Deter/mitigate threats to STCPs

RC. 2 Game-theoretic Framework for Multi-target, Multi-layer Defense against Strategic Attackers

RC.1: Machine Intelligence for Effective Threat Deterrence and Risk Mitigation at Soft Targets and Crowded Places
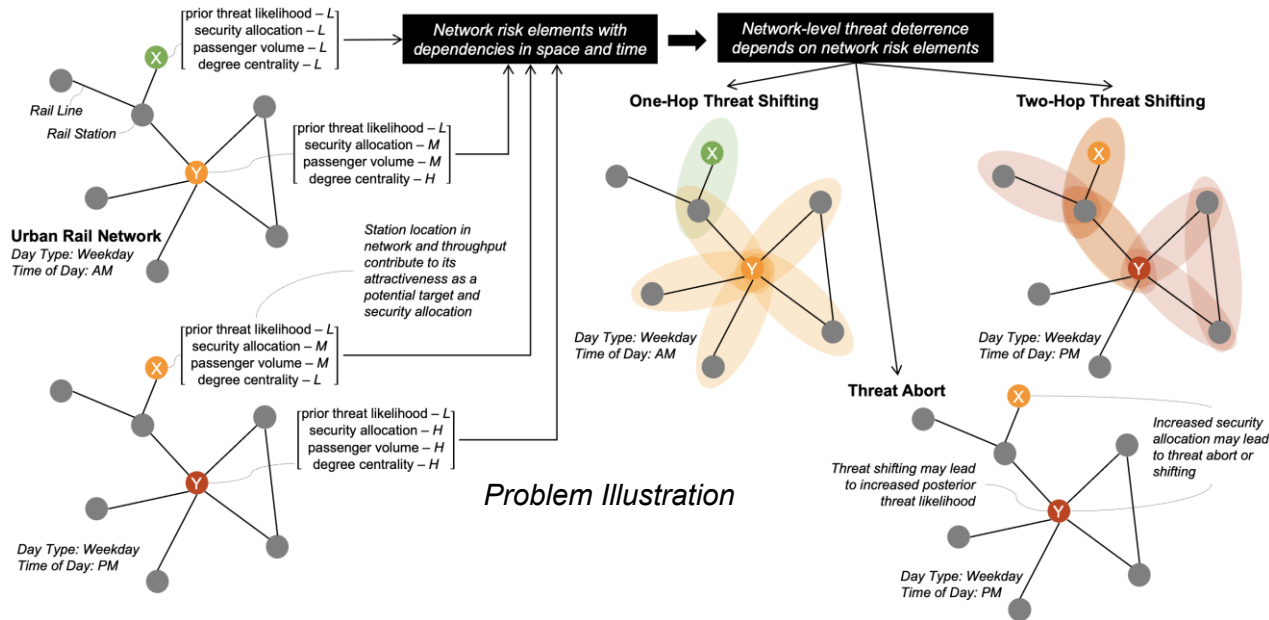
Problem

Define and quantify network-level threat deterrence with focus on urban rail networks

https://unsplash.com/

Problem Illustration

Network risk elements with dependencies in space and time → Network-level threat deterrence depends on network risk elements

- prior threat likelihood – L
- security allocation – L
- passenger volume – L
- degree centrality – L

Rail Line
Rail Station

- prior threat likelihood – L
- security allocation – M
- passenger volume – M
- degree centrality – H

Urban Rail Network
Day Type: Weekday
Time of Day: AM

Station location in network and throughput contribute to its attractiveness as a potential target and security allocation

- prior threat likelihood – L
- security allocation – M
- passenger volume – M
- degree centrality – L

Day Type: Weekday
Time of Day: PM

- prior threat likelihood – L
- security allocation – H
- passenger volume – H
- degree centrality – H

Day Type: Weekday
Time of Day: PM

One-Hop Threat Shifting
Day Type: Weekday
Time of Day: AM

Two-Hop Threat Shifting
Day Type: Weekday
Time of Day: PM

Threat Abort
Threat shifting may lead to increased posterior threat likelihood
Increased security allocation may lead to threat abort or shifting
Day Type: Weekday
Time of Day: PM

Progress

- Defined a GCN-based network threat deterrence analysis methodology
- Developed software code implementing a GCN node classification algorithm
- 2023 SRA invited presentation; 2022 IEEE-HST Best Paper Award
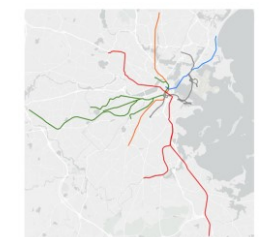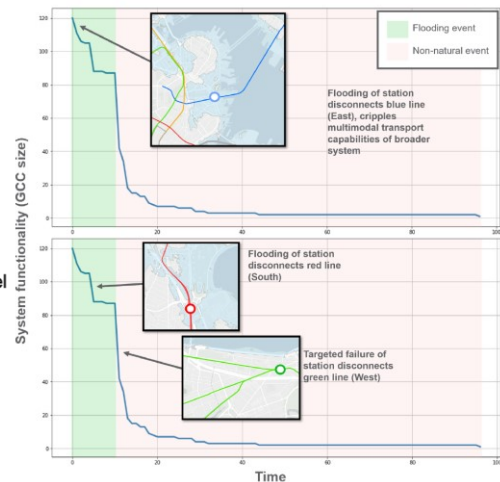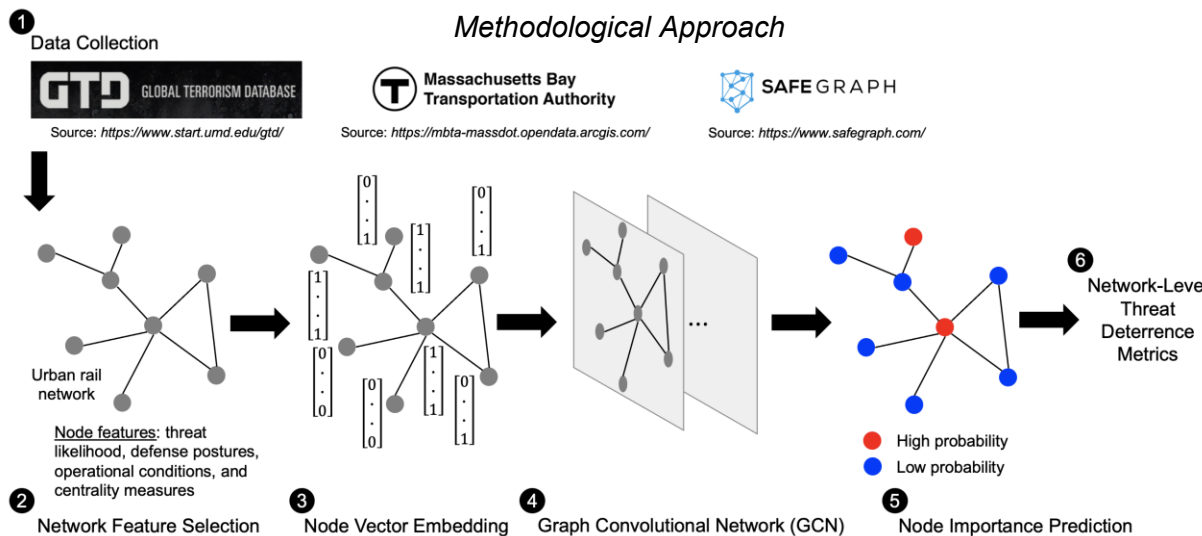- Engagements and connections: MBTA, DHS CISA, ICE, SafeGraph

Solution

Graph Convolutional Network (GCN) approach for network-level threat deterrence analysis with proof-of-concept application to MBTA rail network

Methodological Approach

1 Data Collection

GTD GLOBAL TERRORISM DATABASE
Source: https://www.start.umd.edu/gtd/

Massachusetts Bay Transportation Authority
Source: https://mbta-massdot.opendata.arcgis.com/

SAFEGRAPH
Source: https://www.safegraph.com/

2 Network Feature Selection
Urban rail network
Node features: threat likelihood, defense postures, operational conditions, and centrality measures

3 Node Vector Embedding

4 Graph Convolutional Network (GCN)

5 Node Importance Prediction
- High probability
- Low probability

6 Network-Level Threat Deterrence Metrics

Compound failure simulation

Flooding event
Non-natural event

Flooding of station disconnects blue line (East), cripples multimodal transport capabilities of broader system

Flooding of station disconnects red line (South)

Targeted failure of station disconnects green line (West)

System functionality (GCC size)

Time

MBTA rail network

IEEE-Homeland Security Technologies (HST) 2022 Best Paper Award
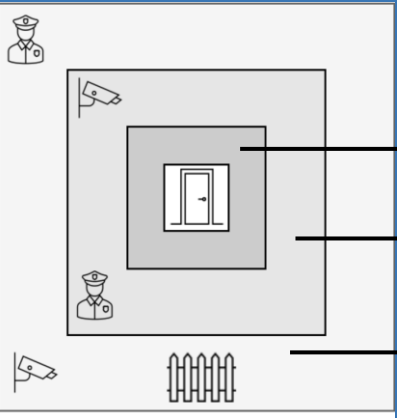
RC.2 Modeling Defensive Resource Allocation in Multi-layered Systems under Probabilistic and Strategic Risks

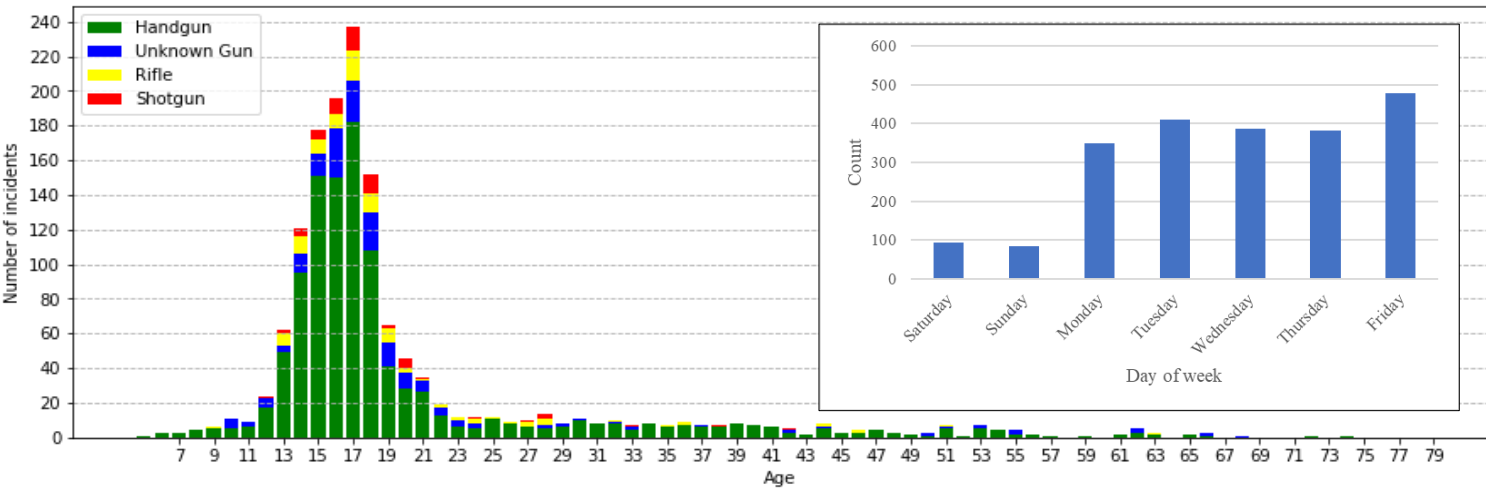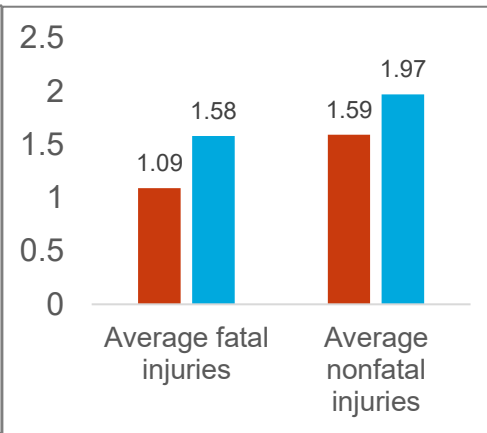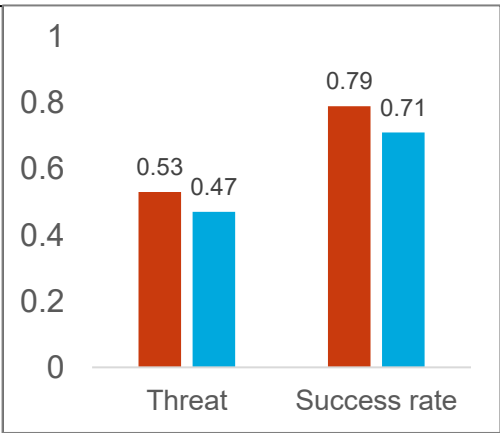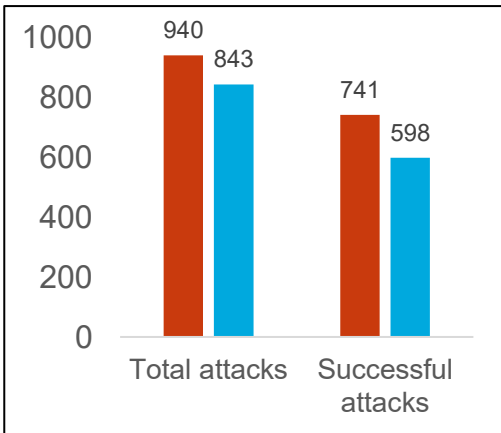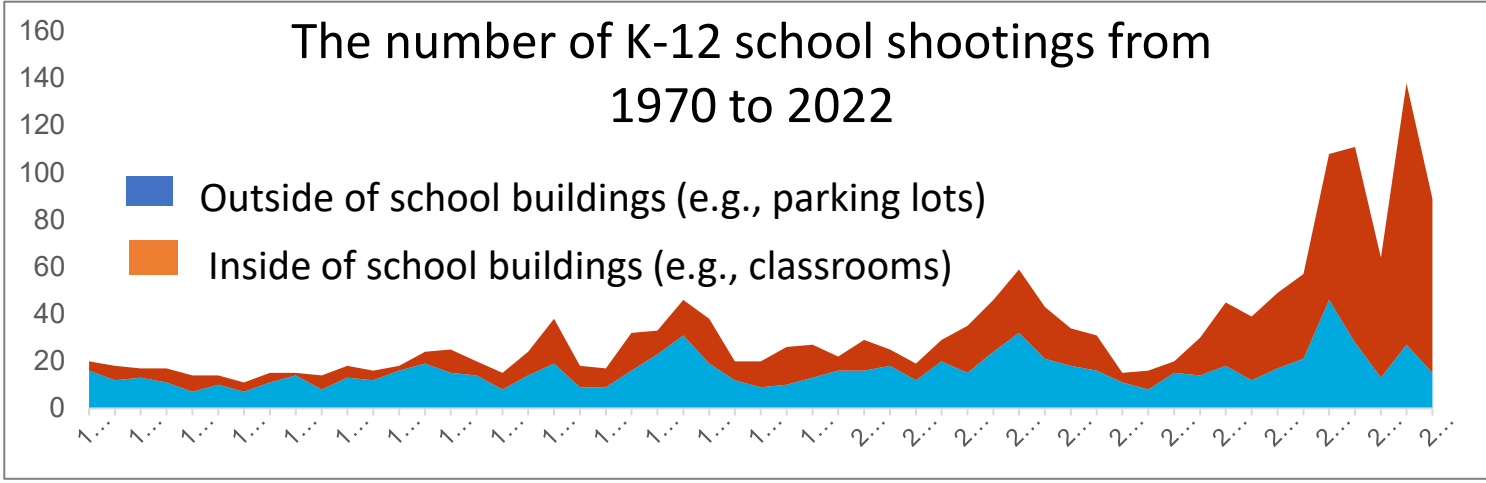Layered systems (each layer provides extra defence to prevent single points of failure)

A hybrid-game theoretical model is developed

Two types of violence: random vs. targeted

We use K-12 School Shooting Database (Riedman (2023) to illustrate the models

The number of K-12 school shootings from 1970 to 2022

- Outside of school buildings (e.g., parking lots)
- Inside of school buildings (e.g., classrooms)

- Building interior
- Building perimeter
- School grounds

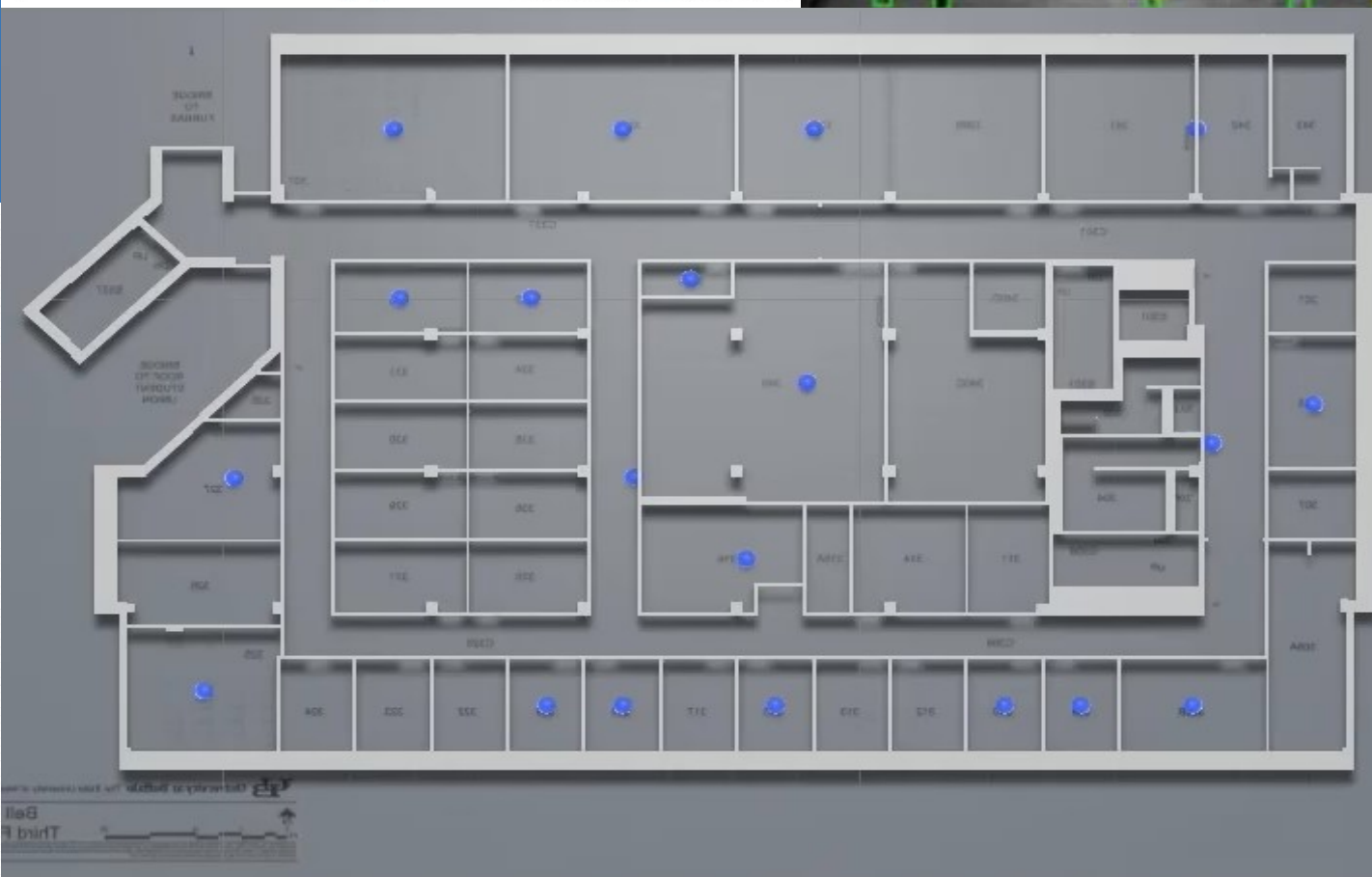A Preliminary Multi-layer, Multi-pathway Diagram for K-12 School Security
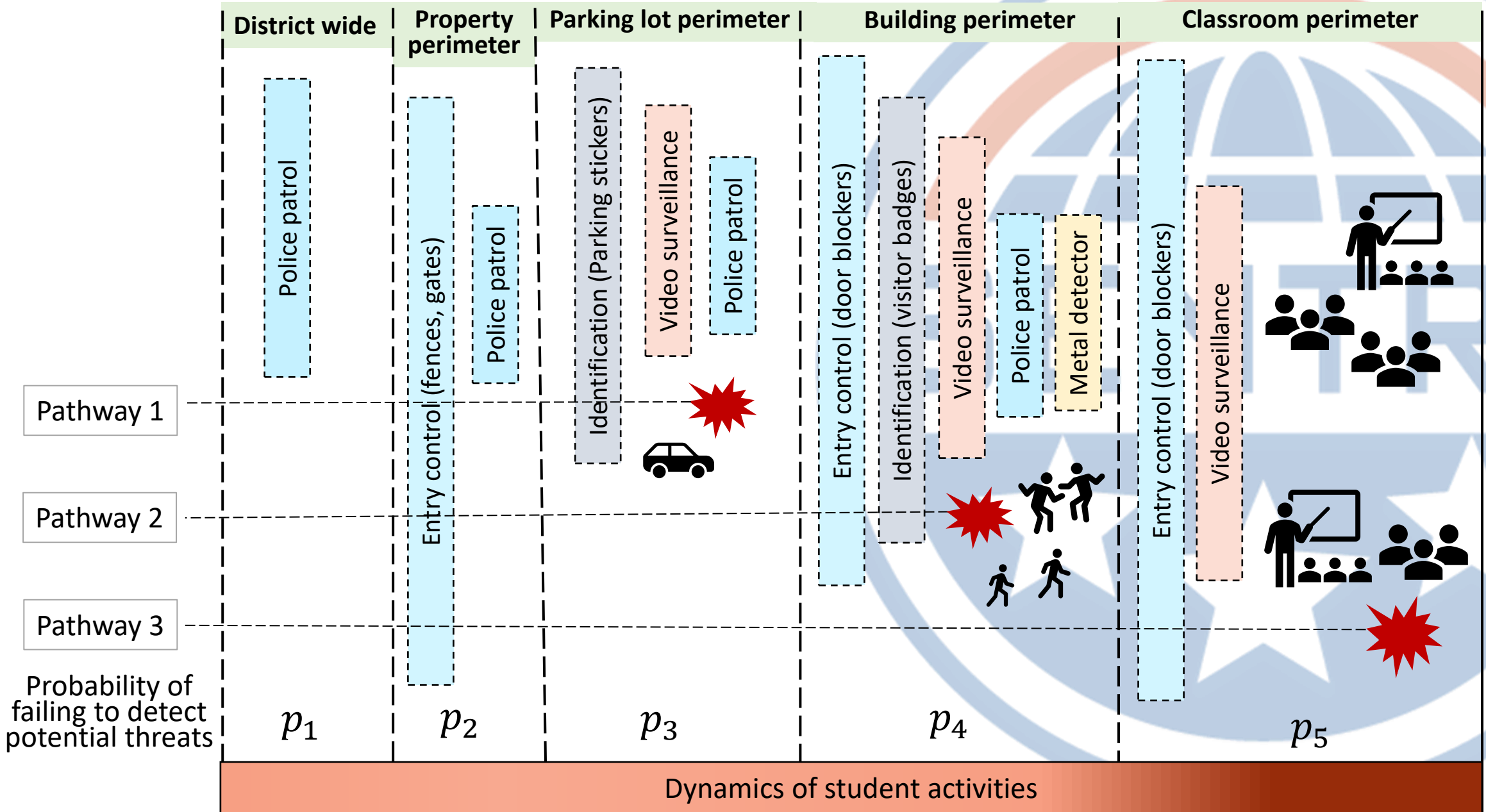
Optimal Location of Sensors/Cameras in Venues

Working with floor plan layout and utilizing 3D modeling software to model what different types of cameras can see

Optimal location of sensors to cover the critical pathway to reduce risks

Comments/Questions?

Prof. Jun Zhuang

SENTRY RC Lead
Morton C. Frank Professor

University at Buffalo

jzhuang@buffalo.edu