VANDERBILT UNIVERSITY

SIMULATION TESTBED FOR RAILWAY INFRASTRUCTURE SECURITY AND RESILIENCE EVALUATION

Himanshu Neema[1], Xenofon Koutsoukos[1], Bradley Potteiger[2], CheeYee Tang[3], Keith Stouffer[3]

1. *Institute for Software-Integrated Systems* ***[Vanderbilt University]***
2. *Applied Physics Laboratory* ***[John Hopkins University]***
3. *Networked Control Systems Group, Intelligent Systems Division, Engineering Laboratory* ***[National Institute of Standards & Technology (NIST)]***

Acknowledgement for Support:

NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA NSF NIST

HIMANSHU NEEMA, PhD
Research Assistant Professor
Vanderbilt University
himanshu.neema@vanderbilt.edu

HoTSoS 2020, September 22, 2020

MOTIVATION

There have been several safety-critical problems with trains in recent years

- Northwest Railway Attack
- Philadelphia Amtrack
- Washington State Amtrack
- South Carolina Amtrack CSX Freight Collision

Attackers can leverage interdependencies between physical and cyber domain to affect train behavior

Paul Bigland via Getty Images

CHALLENGES

Autonomous Control

- How can we optimize train travel times with distributed control?

Railway Signal/Switch Scenario

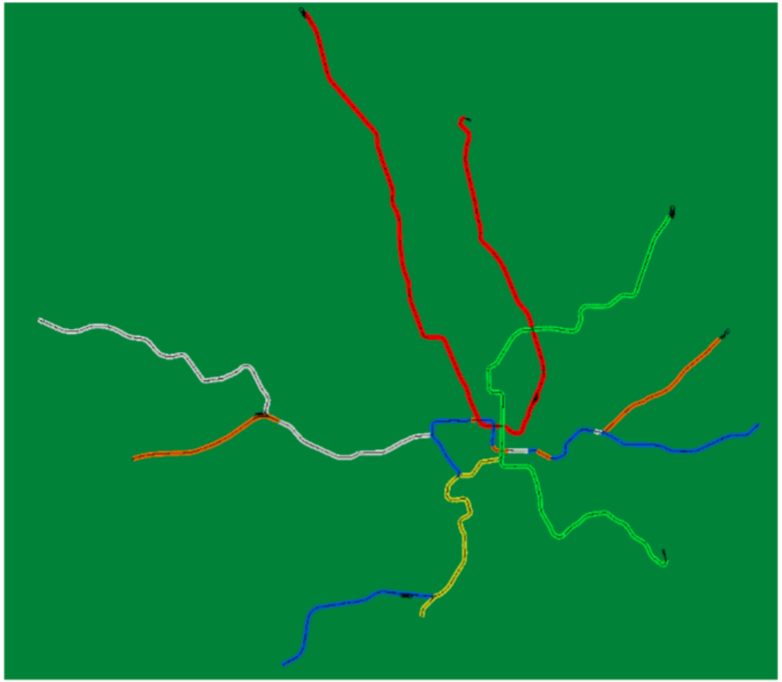
- How can we develop a control algorithm to optimize train travel through control of switches and rail signals in the network?

Security

- How can we make a train control algorithm resilient to physical/cyber attacks within the network?

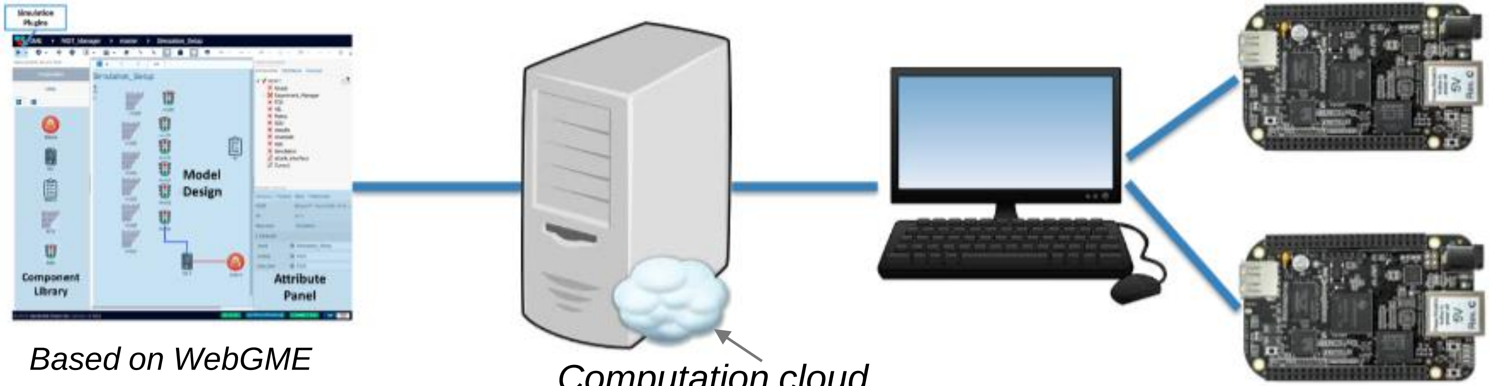
Goal

- **Provide a model-based framework with an integrated simulation and emulation testbed for analyzing the security and resilience of railway networks.**



Washington, DC Metro Railway Network

MODELING & SIMULATION FRAMEWORK



Simulation Design

Web Server

Simulation Workstation

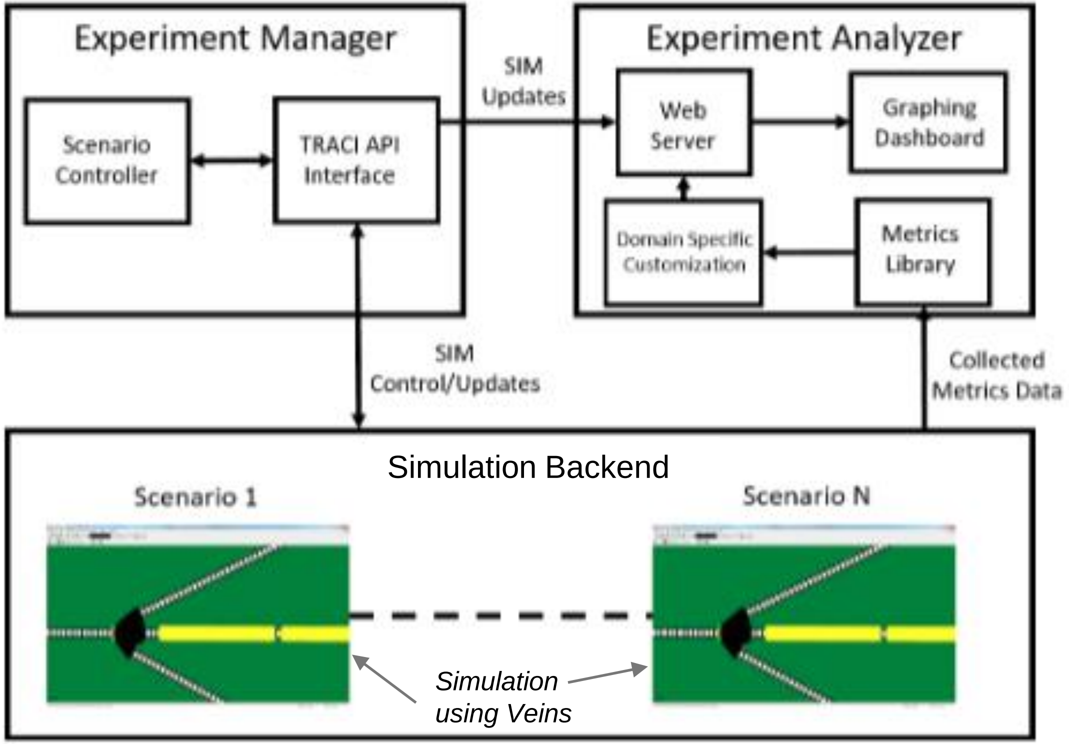
Based on WebGME

Computation cloud

Programmable boards for HIL simulation

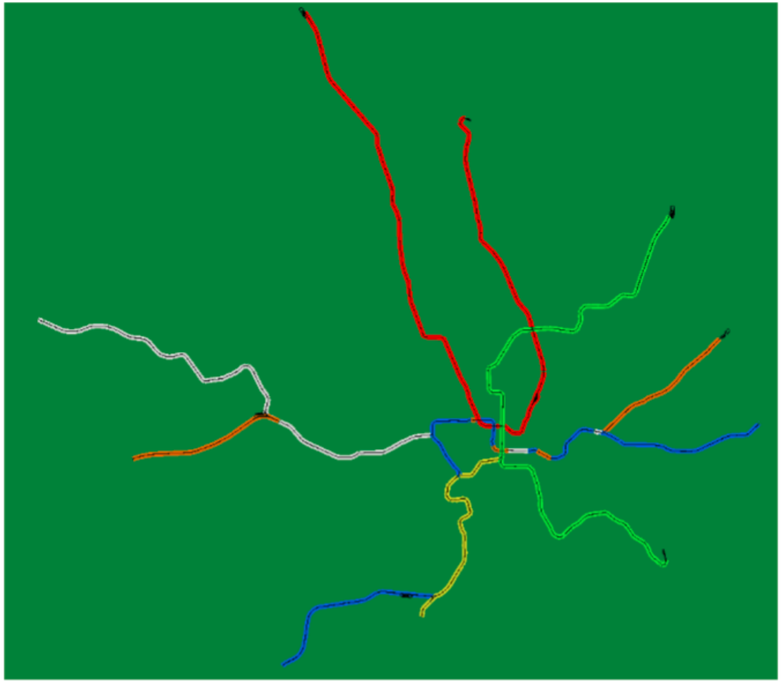
- Support for parallel experiment execution
- HIL support for replacing railway modules with customized controllers
- Results are fetched in real-time

CORE SYSTEM ARCHITECTURE



- Support for parallel experiment execution
- HIL support for replacing railway modules with customized controllers
- Results are fetched in real-time

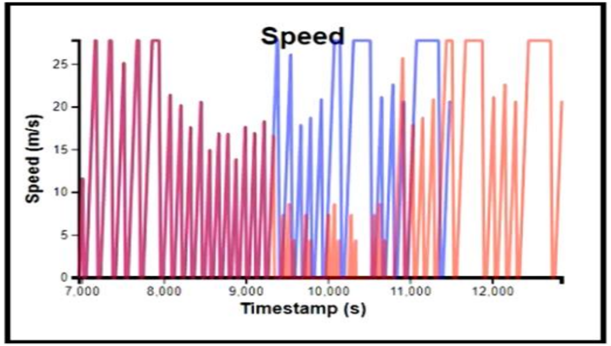
CASE STUDY

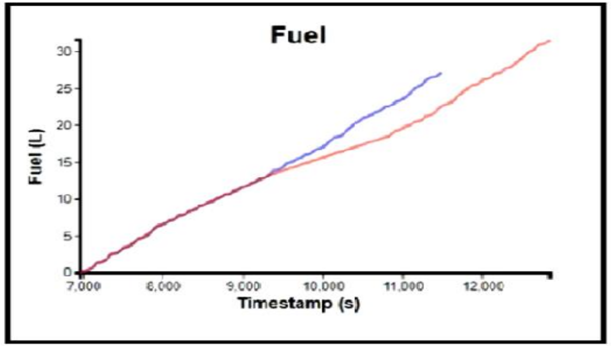


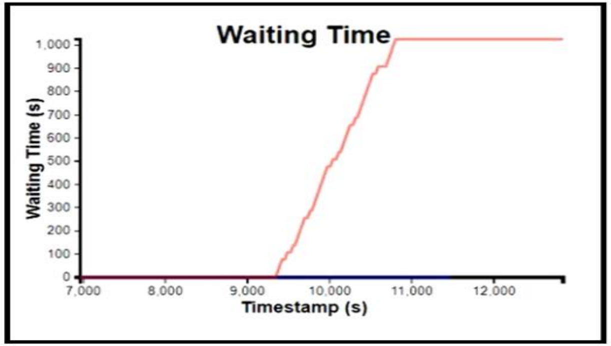
Washington, DC Metro Railway Network

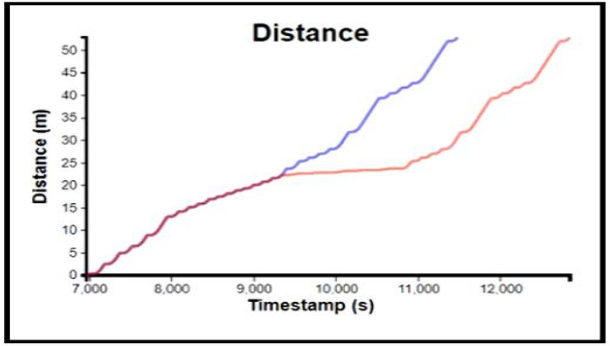
- Realistic railway network
- Rail signals and switches
- Shared tracks
- V2V and V2X communications
- V2X comm. from approaching trains enable controlling switch actuations
- Cyber-attacks from attack-library
- HIL simulation
- DDoS attack in the hardware
- Analysis of “operational metrics”

EXPERIMENT RESULTS





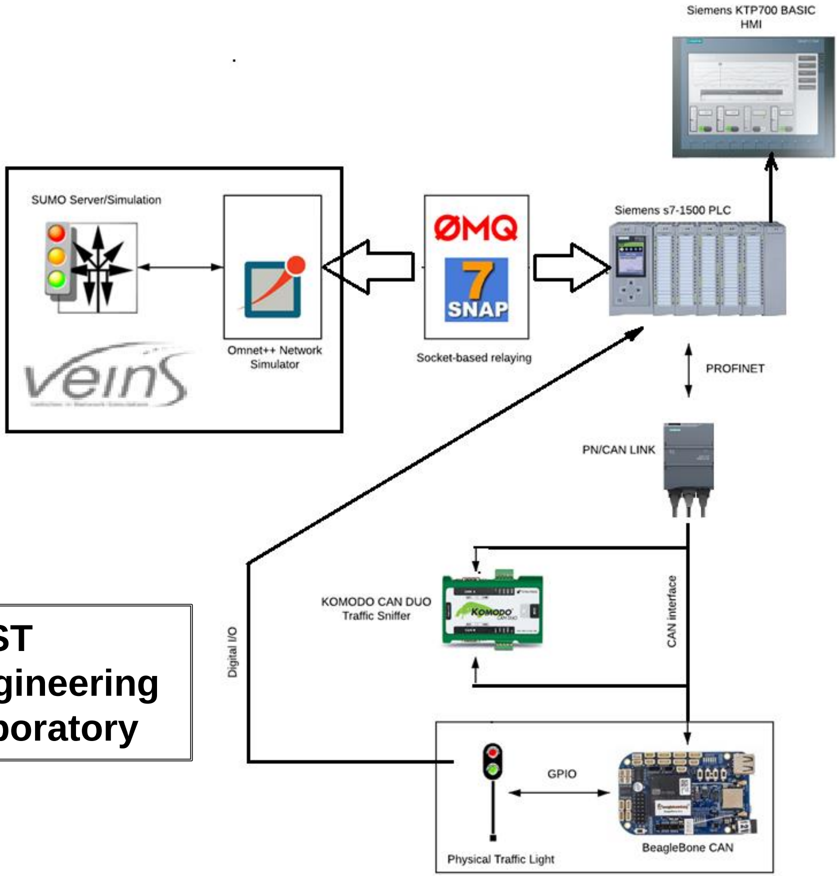




- *Results for train worst impacted by cyber-attacks*
- *Blue color: Baseline (No attacks)*
- *Red color: With attacks*

- Reston, VA to Greenbelt, MD
- Baseline path: Silver (East) -> Blue (North; inner city) -> Green (NE)
- Integrity Attack: Blue (South; southern perimeter)
- DDoS Attack: Delay before transfer to Green line
- Results for worst impacted train are shown
- Attack duration: 9300-11000 seconds

NIST LABORATORY:
HIL EXPERIMENTATION PLATFORM*



* NIST Engineering Laboratory

- NIST HIL Testbed’s 3 major components:
  - Train operation simulation
  - Network comm. simulation
  - Physical hardware
- Siemens S7 PLC:
  - Controls traffic signal at railroad track intersection
  - Has HMI interface and PN/CAN Link
- Communication protocols:
  - PROFINET: B/n PLC and PN/CAN Link
  - CAN: B/n PN/CAN and field devices (BBB)
- Real commercial hardware
- SNAP7 and ZMQ for comm. b/n simulator and hardware

CONCLUSION & FUTURE WORK

- Railway transportation is becoming *highly interconnected* with increasing sensors, embedded devices for computation and control, and wireless networking for communication.
- This has *increased attack surface* for this highly safety-critical infrastructure vulnerable to attacks and thereby to major damage and even loss of human life.
- This research work demonstrates a *model-based framework* for rapidly designing railway scenarios with cyber-attacks and an *integrated cloud environment* for *execution, monitoring, and real-time analysis of experiments* using web-based browser plugins.
- The simulation backend also supports hardware-in-the loop simulations via integrated and programmable embedded devices.
- The major components of the framework, including the cyber-attack libraries have been developed as modular, reusable, and configurable for use in different scenarios for rapid and customized experimentation.
- We demonstrated the framework using a realistic case-study from Washington DC railway network.
- Importantly, **this testbed has been successfully transitioned to NIST's Engineering Laboratory** and is actively being further developed and refined there for real-world use-cases.

- In future, we plan to apply the testbed to other transportation applications such as self-driving vehicles.
- Also, we plan to extend model libraries with more reusable cyber-attacks and security solutions.

THANK YOU!

ANY QUESTIONS?

- Himanshu.Neema@Vanderbilt.Edu
- Xenofon.Koutsoukos@Vanderbilt.Edu
- Brad.Potteiger@Jhuapl.Edu
- Cheeyee.Tang@Nist.Gov
- Keith.Stouffer@Nist.Gov

Acknowledgement for Support: