Simulation Testbed for Railway Infrastructure Security and Resilience Evaluation

Submitted by himanshu on Thu, 03/12/2020 - 10:13am. Contributors:
Himanshu NeemaXenofon KoutsoukosBradley PotteigerCheeYee Tang

The last decade has seen an influx of digital connectivity, operation automation, and remote sensing and control mechanisms in the railway domain. The management of the railway operations through the use of distributed sensors and controllers and with programmable and remotely controllable railway signals and switches has led to gains in system efficiency as well as operational flexibility. However, the network connectivity has opened up the railway cyber communication networks to cyber-attacks. These are a class of cyber-physical systems (CPS) with interconnected physical, computational, and communication components. The cyber-attacks on these systems could potentially cascade through these interconnection and result into significant damage. These systems are safety-critical owing to their large-scale monetary and, more importantly, human life safety concerns.

Therefore, it is better to incorporate security and resilience requirements right from the design time. In this paper, we describe a domain-specific framework for simulations in the railway domain. The framework allows analyzing the resilience of railway operations in the presence of cyber-attacks. In particular, our simulation framework allows modeling the railway network as well as the railway transportation. It provides an online graphical modeling environment that allows multiple users to collaborate, through a web-based interface, over the same model for the railway infrastructure as well as network attacks. The framework also allows the user to configure and run experiments through the web-interface and also to visualize the key operational metrics from the railway domain as the experiment is running. The framework also supports executing large simulations in the cloud. In addition, it supports hardware-in-the-loop (HIL) simulation for incorporating physical effects and network attacks that can only be realized realistically in the hardware. A detailed case study is provided to demonstrate the framework's capabilities.

Himanshu Neema is a Research Assistant Professor of Computer Science at Vanderbilt University. He holds a M.S. and Ph.D. in Computer Science from Vanderbilt University. Dr. Neema researches in the general area of model-based design and modeling and simulation of Cyber-Physical Systems and their integrated simulation with hardware- and humans- in the loop. His research interests include: Model-Based Design, Cyber-Physical Systems, Distributed Simulations & Analysis of System-of-Systems, Heterogeneous Simulation Integration, Cybersecurity, Risk Analysis, Network Simulation, Scenario-Based Experimentation, Cloud Computing, Big Data, Resilient Systems, Design Automation, Design Space Exploration, Artificial Intelligence, Machine Learning, Adversarial Machine Learning, Constraint Programming, Planning & Scheduling, Resource Allocation, Constraint Solving, Operations Research, Service-Oriented Architectures, Blockchains, Smart-Grids, Transactive Energy, Smart Cities. Dr. Neema has 22 years of experience in research and development of software applications covering above areas and has co-authored more than 50 publications. He is the creator of the model-based simulation integration and rapid experimentation framework called Cyber-Physical Systems Wind Tunnel (CPSWT), which has been recently successfully transitioned to the US National Institute of Standards and Technology (NIST).

Himanshu Neema | Xenofon Koutsoukos | Bradley Potteiger | CheeYee Tang

License: Creative Commons 2.5

Other available formats:

Simulation Testbed for Railway Infrastructure Security and Resilience Evaluation

Switch to normal viewerSwitch to experimental viewer

Presentation Paper Session 1