Simulation Based Evaluation of Security and Resilience in Railway Infrastructure

Bradley Potteiger, Hamzah Abdel-Aziz, Himanshu Neema, Xenofon Koutsoukos
Vanderbilt University
Nashville, TN

ABSTRACT

Autonomous and connected vehicle technologies are rapidly emerging in the modern railway domain. Traditional standalone systems are now becoming more sophisticated, resulting in more distributed interfaces, and a larger attack surface. As such, there now exists a tightly coupled cyber-physical nature that makes a cyber-attack capable of not only exfiltrating sensitive data, but also manipulating safety-critical operations of the system. This manipulation can cause the train to experience unsafe conditions, potentially leading to derailments, explosions, and collisions. This makes it as important as ever to build in security and resilience at the earliest stages of design, making deployment infrastructure more safe, reliable, and predictable in a compromising environment. In this poster we demonstrate how to analyze the security and resilience of railway infrastructure by utilizing a domain specific simlation based framework. Our framework includes a simulation cluster with both transportation and network modeling capabilities, a graphical design studio to rapidly develop attack scenarios againt railway networks, and a results dashboard that includes real time visualization of various metrics. Additionally, we not only support software-in-the-loop, but have integrated a hardware-in-the-loop testbed to test realistic attacks that occur within the deployment environment. We illustrate the capabilities of our developed framework with a connected railway case study of the Washington D.C Metro rail network.

CCS CONCEPTS

• **Security and privacy**; • **Computer systems organization** → **Embedded and cyber-physical systems**;

KEYWORDS

Railway, Cyber-Physical Systems, Simulation Based Design, Resiliency, Hardware-in-the-Loop

ACM Reference Format:
Bradley Potteiger, Hamzah Abdel-Aziz, Himanshu Neema, Xenofon Koutsoukos. 2019. Simulation Based Evaluation of Security and Resilience in Railway Infrastructure. In *Hot Topics in the Science of Security Symposium (HotSoS), April 1–3, 2019, Nashville, TN, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3314058.3317731

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).
HotSoS, April 1–3, 2019, Nashville, TN, USA
© 2019 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-7147-6/19/04…$15.00
https://doi.org/10.1145/3314058.3317731

1 INTRODUCTION

Nowadays, autonomous and connected vehicles technologies are rapidly emerging in modern railway. Modern railway is a practical example of the traditional Cyber-Physical System (CPS) [4]. CPS enable the integration of computation and physical processes to facilitate safe and efficient operation of the railway. For instance, vehicle to infrastructure (V2I) interaction enables the development of complex algorithms to control railway infrastructures (e.g., rail switches and traffic signals). However, the integration of V2I connectivity with the computation and the physical processes of railway adds new avenues for adversaries to damage the system through cyber-attacks. Therefore, it is very important to determine how a cyber-attack will influence the operating railway system.

In this poster, we demonstrate a simulation-based platform that can be used to assess the security and resiliency of modern railway on V2I technology. The simulation platform provides the capability of integrating the network and computation components of CPS with the surrounding physical environment. Furthermore, the simulation platform provides metric-driven methodology to quantify the effect of different cyber-attacks. Hence, scientific analysis and methods can be used to develop and rank various defense mechanisms and identify critical vulnerabilities in the system.

2 DESIGN

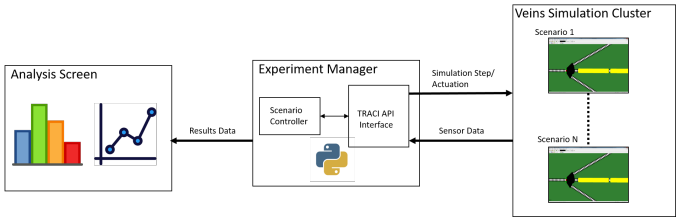


Figure 1: Testbed Architecture

Our simulation platform is comprised of three main components: the experiment manager, simulation cluster, and results dashboard. The basis behind our railway analysis revolves around the development of experiments, providing for a scientific approach to develop resilient approaches, test against realistic attacks, and utilize generated quantitative metrics for an analytical comparison. As such, the best approaches can be compared objectively to provide the most effective methods for securing the respective railway infrastructure.

2.1 Experiment Manager

The experiment manager (EM) provides the ability to rapidly develop, deploy, and execute railway attack scenarios. Additionally, the EM is responsible for fetching results from the respective simulations to relay to the results dashboard for visualization and analysis.

For development, we utilize a graphical web-based domain-specific modeling tool called WebGME [5] to provide the front-end for our user. WebGME allows not only a customizable graphical front-end, but also the integration of plugins to interpret model semantics, and execute the respective simulation programs. As such, it is possible to control all of the simulation specifics from the cloud, making experimentation possible from anywhere in the world.

2.2 Simulation Cluster

The simulation cluster (SC) is the backbone of our platform, providing the ability to translate the developed railway model into real-world results. The SC utilizes the Veins open source simulator [2] which combines network simulation with OMNeT++ [8] and transportation simulation with Sumo [3] to support a modern connected vehicle simulation environment. The SC supports multiple parallel simulations, and includes components representing railway switches, railway signals, and data acquisition modules.

2.2.1 Metrics Library. A generalized metrics library is developed to support the acquisition of various domain-specific metrics within the simulation [7]. Due to the modular approach of developments, either an existing set of metrics can be utilized, or new customized metrics can be developed. Some example metrics include train speed, fuel consumption, waiting time, and travel distance.

2.2.2 Attack Library. A component-specific attack library is developed for integrating attacks into software components within the simulation. This attack library was built by customizing the base module for V2X communications in Veins. It can be configured to incorporate DOS, integrity, or delay attacks on railway nodes. This allows for experiment with different combinations of cyber-attacks within a software-in-the-loop environment.

2.2.3 Harware in the Loop Testbed. In addition to software-in-the-loop testing, a hardware-in-the-loop testbed is integrated to allow for the testing of railway infrastructure controllers on embedded hardware consistent with the deployment environment. During experiment scenario design, a component can be specified to be implemented within the software or hardware environment. Additionally, a hardware-specific cyber-attack library is implemented to perform attacks in an embedded environment that might be harder to implement within the simulation environment. Some example attacks include DDOS, delays caused by attacks that create severe network congestion, and integrity attacks that utilize hardware vulnerabilities.

2.3 Results Dashboard

The results dashboard utilizes the Grafana open source library [1] to provide real-time visualization capabilities within the platform. This dashboard front-end is integrated with the InfluxDB database backend [6] to fetch and store experiment results from the simulation cluster during run-time. One of the biggest benefits of these visualization mechanisms is the ability to plot muliple simulation scenarios within the scope of one graph to objectively compare the impact of various attacks and defense strategies.

3 DEMONSTRATION

For demonstration purposes, we utilizes two experiment scenarios based on the Washington D.C. Metro Rail Network to illustrate the capabilities of our simulation platform. The first scenario focuses on the software-in-the-loop capabilities of our platform by utilizing the component-based attack library to implement an integrity attack on a rail switch within the network. This attack results in the railway switch receiving invalid information resulting in transferring the trains to the wrong track segment. The second scenario focuses on demonstrating our hardware-in-the-loop capabilities of our platform by performing a DDOS attack on a critical railway switch within the network. With the significant increase in messages received by the railway switch controller, the actuation is not able to change track segments in time. Thus, the respective incoming trains are routed down the wrong path, resulting in an inability to reach their destinations.

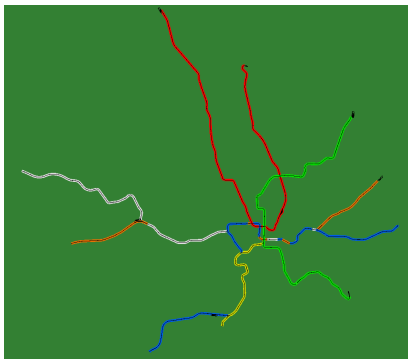


Figure 2: Washington D.C. Metro Rail Network

4 ACKNOWLEDGEMENTS

This work is supported in part by the National Security Agency (H98230-18-D-0010), the National Science Foundation (CNS-1739328), and by NIST (70NANB17H266). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of NSA, NSF, or NIST.

REFERENCES

[1] Grafana - the open platform for analytics and monitoring. https://grafana.com/. (Accessed on 02/22/2019).
[2] Veins. https://veins.car2x.org/. (Accessed on 02/04/2019).
[3] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz. Sumo–simulation of urban mobility. In *The Third International Conference on Advances in System Simulation (SIMUL 2011), Barcelona, Spain*, volume 42, 2011.
[4] B. Chen, C. Schmittner, Z. Ma, W. G. Temple, X. Dong, D. L. Jones, and W. H. Sanders. Security analysis of urban railway systems: the need for a cyber-physical perspective. In *International Conference on Computer Safety, Reliability, and Security*, pages 277–290. Springer, 2014.
[5] M. Maróti, R. Kereskényi, T. Kecskés, P. Völgyesi, and A. Lédeczi. Online collaborative environment for designing complex computational systems. *Procedia Computer Science*, 29:2432–2441, 2014.
[6] S. N. Z. Naqvi, S. Yfantidou, and E. Zimányi. Time series databases and influxdb. *Studienarbeit, Université Libre de Bruxelles*, 2017.
[7] H. Neema, B. Potteiger, X. Koutsoukos, C. Tang, and K. Stouffer. Metrics-driven evaluation of cybersecurity for critical railway infrastructure. In *2018 Resilience Week (RWS)*, pages 155–161. IEEE, 2018.
[8] A. Varga and R. Hornig. An overview of the omnet++ simulation environment. In *Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops*, page 60. ICST (Institute for Computer Sciences, Social-Informatics and âĂę, 2008.