Demo Abstract: SURE: An Experimentation and Evaluation Testbed for CPS Security and Resilience

Himanshu Neema, Peter Volgyesi, Bradley Potteiger, William Emfinger, Xenofon Koutsoukos, Gabor Karsai, Yevgeniy Vorobeychik, Janos Sztipanovits
Institute for Software-Integrated Systems, Vanderbilt University
Nashville, TN, USA

***Abstract*— In-depth consideration and evaluation of security and resilience is necessary for developing the scientific foundations and technology of Cyber-Physical Systems (CPS). In this demonstration, we present SURE [1], a CPS experimentation and evaluation testbed for security and resilience focusing on transportation networks. The testbed includes (1) a heterogeneous modeling and simulation integration platform, (2) a Web-based tool for modeling CPS in adversarial environments, and (3) a framework for evaluating resilience using attacker-defender games. Users such as CPS designers and operators can interact with the testbed to evaluate monitoring and control schemes that include sensor placement and traffic signal configuration.**

Keywords*— *cyber-physical systems; security; resilience; simulation integration

I. SUMMARY

The fundamental feature of the SURE testbed is to support design and evaluation of networked CPS focusing on security and resilience in the presence of cyber attacks. The testbed integrates (1) a modeling and simulation integration platform called Command-and-Control Wind Tunnel (C2WT) [2] and a web-based collaborative (meta) modeling tool called WebGME [3]. Although the testbed can be customized for different applications and evaluation of various algorithms, this demonstration focuses on urban transportation networks and evaluation of resilient monitoring and control using attacker-defender games.

C2WT is a model-based integration framework for heterogeneous and distributed simulations and supports rapid design, synthesis, and evaluation of distributed simulations. In this testbed, C2WT provides an integration framework for the SUMO traffic simulation [6] and the OMNeT++ network simulator [7]. WebGME [3] is a novel, web- and cloud- based collaborative, scalable, and extensible (meta) modeling tool developed recently at our institute. It supports the design of Domain-Specific Modeling Languages as well as creation of corresponding domain models. It also provides a fine-grained version control of models. All design and evaluation tasks require only a web-browser.

SURE is used to evaluate resilient monitoring and control algorithms. Specific examples that have been already developed include: (1) Resilient observation selection where a Gaussian process regression model is used to determine sensor locations that are resilient to DoS attacks [4] and (2) resilient traffic signal configuration to minimize the congestion impact of tampering attacks [5]. Fig. 1 shows the web interface of the SURE testbed for evaluating observation selection strategies on the road network around the Vanderbilt University campus.

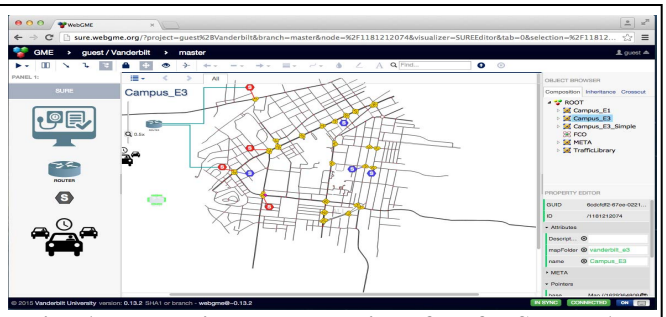

Fig. 1. Interactive web-based interface for SURE [1]

REFERENCES

[1] SURE: Science of SecUre and REsilient Cyber-Physical Systems. http://sure.isis.vanderbilt.edu

[2] G. Hemingway, H. Neema, H. Nine, J, Sztipanovits, and G. Karsai. "Rapid synthesis of high-level architecture-based heterogeneous simulation: A model-based integration approach", *Simulation*, Vol. 88 No. 2, pp. 217-232, Feb., 2012.

[3] WebGME: A Web- and Cloud-based Collaborative (Meta) Modeling Tool. http://www.webgme.org

[4] A.Laszka, Y. Vorobeychik, and X. Koutsoukos. "Resilient Observation Selection in Adversarial Setting", *CDC'15*, Osaka, Japan, Dec 15-18, 2015.

[5] A. Laszka, B. Potteiger, Y. Vorobeychik, S. Amin, and X. Koutsoukos. "Vulnerability of Transportation Networks to Traffic-Signal Tampering", *ICCPS 2016*, Vienna, Austria, April 12-14, 2016.

[6] D. Krajzewicz, J. Erdmann, M. Behrisch, and L. Bieker. "Recent Development and Applications of SUMO - Simulation of Urban Mobility", *International Journal on Advances in Systems and Measurements*, 5 (3&4):128-138, 2012.

[7] OMNeT++ - www.omnetpp.org

978-1-5090-1772-0/16/$31.00 ©2016 IEEE