DEMO: Trustworthy Cyberphysical Energy Systems: Time-Delay Attacks in a Real-Time Co-Simulation Environment

Juan Ospina, Ioannis Zografopoulos, XiaoRui Liu, Charalambos Konstantinou
{jjospina,izografopoulos,xliu9,ckonstantinou}@fsu.edu
Department of Electrical and Computer Engineering, FAMU-FSU College of Engineering
Center for Advanced Power Systems, Florida State University

ABSTRACT

In this work, we present the impact of time-delay attacks in cyber-physical energy systems. The evaluation is performed in a real-time co-simulation environment that captures the interdependency between the system's cyber and physical models.

CCS CONCEPTS

• **Security and privacy** → *Network security*; **Systems security**; • **Computer systems organization** → **Embedded and cyber-physical systems**.

KEYWORDS

Cyberphysical energy systems, co-simulation, time-delay attacks

ACM Reference Format:
Juan Ospina, Ioannis Zografopoulos, XiaoRui Liu, Charalambos Konstantinou. 2020. DEMO: Trustworthy Cyberphysical Energy Systems: Time-Delay Attacks in a Real-Time Co-Simulation Environment. In *2020 Joint Workshop on CPS&IoT Security and Privacy (CPSIOTSEC'20), November 9, 2020, Virtual Event, USA.* ACM, New York, NY, USA, 1 page. https://doi.org/10.1145/3411498.3422926

1 DEMO SETUP DESCRIPTION

The pursuit of more efficient and resilient electric power systems has ushered a shift towards more distributed architectures. Information and communication technologies, alongside grid-connected devices, can realize these goals albeit they increase the system's threat surface. Performing cybersecurity studies on actual power systems is infeasible due to high deployment costs and operational risks. Simulation testbeds of cyberphysical systems (CPSs) arise as ideal candidates for generating and evaluating holistically high-fidelity models of such complex CPS architectures.

The evaluation of attacks' impact on CPS testbeds may involve two or more simulation (co-simulation) environments that allow more comprehensive and accurate results. Co-simulation techniques are effective for evaluating the impact of different scenarios such as cyberattacks and control schemes [2]. In this demo, we evaluate the impact of time-delay attacks (TDAs), defined as a type of time-based attack that could destabilize system operations by delaying real-time control commands or data measurements. Despite TDAs being performed at the cyber (communication) system layer of the CPS, they can significantly affect the operation of the physical grid. Our setup involves a real-time co-simulation testbed demonstrating the impact of such TDAs in a microgrid system.

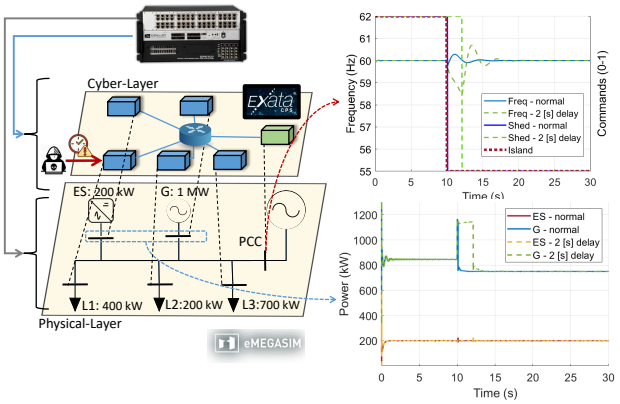

Figure 1: Co-simulation environment setup to evaluate time-delay attacks – TDAs (left). Impact of 2-*secs* TDA on shedding command vs. normal operation (right).

Figure 1 demonstrates the co-simulation setup used in this study to evaluate the impact of a 2-*secs* TDA. The microgrid is composed of one conventional generator (G), one energy storage (ES) system, a point-of-common-coupling (PCC) microgrid controller interfaced with the main grid, and three loads: L1 is a sheddable load, L2 is a critical load, and L3 is a regular load. Each of these nodes is mapped to cyber layer nodes that represents a master (PCC), or outstation (Others) device communicating via *DNP3* protocol. To evaluate the impact of the TDA, the physical layer of the microgrid is modeled using a real-time simulator (Opal-RT), and the cyber layer is modeled using the EXataCPS emulator. The graphs shown in Figure 1 depict a comparison between the normal operation of a load shedding mechanism vs. a 2-*secs* TDA implemented as an attack on the load-shed controller of the microgrid. In these scenarios, the microgrid performs an islanding operation at $t = 10$ *secs*, and due to insufficient generation, the microgrid controller sends a load shedding command to L1. As demonstrated in the graphs, in the TDA scenario, the load shedding command is delayed 2-*secs* causing the frequency of the microgrid to decrease below 59.5 *Hz* [1].

REFERENCES

[1] NERC. 2019. 2019 Frequency Response Annual Analysis. https://www.nerc.com/.
[2] C. Ogilvie, J. Ospina, C. Konstantinou, T. Vu, M. Stanovich, K. Schoder, and M. Steurer. 2020. Modeling Communication Networks in a Real-Time Simulation Environment for Evaluating Controls of Shipboard Power Systems. arXiv:2008.10441 [eess.SP]

CPSIOTSEC'20, November 9, 2020, Virtual Event, USA

ACM ISBN 978-1-4503-8087-4/20/11.
https://doi.org/10.1145/3411498.3422926