Cyber-Physical Simulation Testbed for MadIoT Attack Detection and Mitigation

Gong Chen
gchen31@hawk.iit.edu
Illinois Institute of Technology
Chicago, IL, USA

Yanfeng Qu
yqu9@hawk.iit.edu
Illinois Institute of Technology
Chicago, IL, USA

Dong Jin
dongjin@uark.edu
University of Arkansas
Fayetteville, AR, USA

ACM Reference Format:
Gong Chen, Yanfeng Qu, and Dong Jin. 2022. Cyber-Physical Simulation Testbed for MadIoT Attack Detection and Mitigation. In *SIGSIM Conference on Principles of Advanced Discrete Simulation (SIGSIM-PADS '22), June 8–10, 2022, Atlanta, GA, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3518997.3534995

The smart grid offers great promise to transform today's power system by increasingly interconnecting information technology (IT) and operational technology (OT), but on the other hand, making IT vulnerabilities a significant OT risk. For example, the recent Manipulation of Demand via IoT (MadIoT) attack [2] is a new class of attacks originated from the cyber-world, i.e., Internet of things (IoT) devices, and affect the electrical load of the physical power system. In particular, adversaries leverage a botnet controlling a large number of high-wattage IoT appliances (e.g., air conditioners) to launch a coordinated attack by manipulating the power demand (e.g., switching on/off appliances). Such attacks can trigger severe power disturbance or even cascade failures leading to blackouts. Therefore, a comprehensive study is urgently needed to analyze the attack behavior and propose feasible mitigation solutions.

One key challenge in studying the MadIoT attack is the lack of appropriate testing environments. A testbed is needed to avoid interference and security breaches to the real system. However, a MadIoT attack is conducted across multiple domains, including power systems, communication networks, and IoT devices. The scale of each system makes it infeasible to build a physical testbed. To address this, simulation testbeds can offer the desired flexibility and scalability for testing MadIoT attack behaviors and evaluating proposed solutions before their integration into the real system. However, due to the cross-domain nature of the MadIoT attack, the existing simulation testbeds [1] are not capable of modeling and simulating such a scenario.

Testbed Overview. We propose a cyber-physical testbed to support the simulation and modeling of scenarios containing power systems, communication networks, and IoT devices. The testbed also enables direct code execution through container-based emulation to support high-fidelity experiments. To construct a MadIoT attack scenario in the testbed, we model the power system in a simulator while running real software in the containers to model IoT devices, generate attack traffic, and execute various proposed detection/mitigation schemes. To achieve such a unique testing environment, we seamlessly integrate a power distribution system simulator, OpenDSS, and a container-based network emulator, Mininet, as depicted in Figure 1a. The network emulator consists of the IoT device layer, the communication network layer, and the control layer that operates the network through attack/detection/mitigation models. The control layer is highly customizable. For instance, we can launch the MadIoT attacks with various strategies and perform the detection with various machine-learning models. The power grid, on the other hand, is simulated using OpenDSS, in which we model the electricity consumer and the power distribution system. The consumer module aggregates the status and load of each IoT device and offers updated information to the power distribution system. A key challenge is synchronizing the two systems as the emulator advances in wall-clock, and the simulator advances in the virtual clock. To address this challenge, we leverage our prior work [1, 3] and extensively modify the Linux kernel to enable virtual time in the emulated containers and develop an effective algorithm to synchronize the two systems based on virtual time.

Experimental Results. We designed and implemented multiple detection models and mitigation mechanisms against the attack and evaluated their performance using the simulation testbed. The models of the power system and the communication network were constructed based on IIT's campus microgrid . Figure 1b demonstrates the change of power demand with and without the mitigation scheme after a simulated MadIoT attack. The mitigation consists of two steps: (1) anomaly detection using network domain information (e.g., packet size, port number) and power domain information (e.g., the variance of power demand) and (2) malicious host blocking based on the detection result and IoT device status adjustment (e.g., switching off the appliances that the attacker turned on). We observed that our detection and mitigation mechanism significantly reduced the effeteness of the MadIoT attack and recovered up to 88.57% of the undesired power consumption generated by the attacker. We also performed many other experiments to compare different detection models and mitigation mechanisms. For instance, the detection models considering the cross-domain data had an overall accuracy of 99.87%, which out-performed the models only considering network domain data with an accuracy of 91.82%.

In this work, we develop a cyber-physical simulation testbed to study the recent MadIoT attack. The modular and layered design approach allows us to extend the testbed to conduct other cyber-attacks and security applications for modern power grids, such as network-wide configuration verification and context-aware intrusion detection.

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).
SIGSIM-PADS '22, June 8–10, 2022, Atlanta, GA, USA
© 2022 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-9261-7/22/06.
https://doi.org/10.1145/3518997.3534995

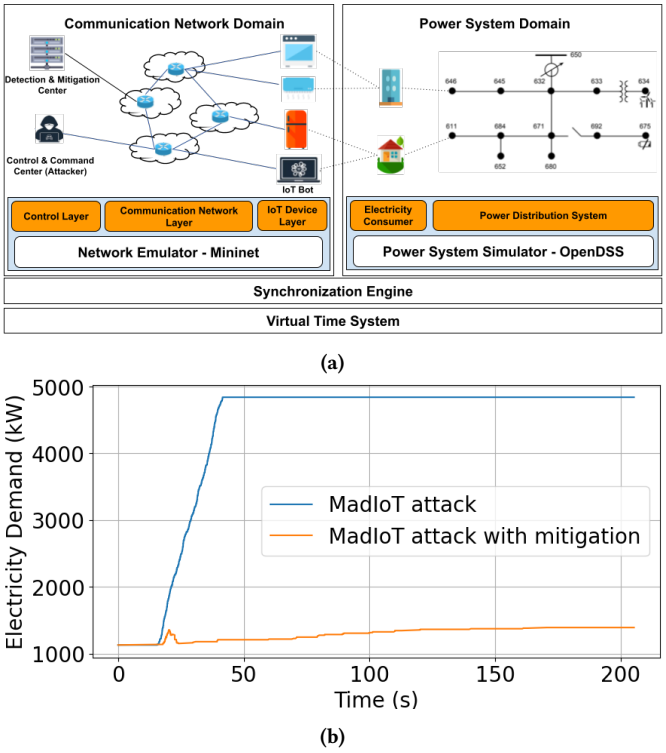

Figure 1: (a) Simulation Testbed Architecture (b) Impact of Attack Mitigation Scheme on Power Demand

REFERENCES

[1] Christopher Hannon, Jiaqi Yan, and Dong Jin. 2016. DSSnet: A Smart Grid Modeling Platform Combining Electrical Power Distribution System Simulation and Software Defined Networking Emulation. In *Proceedings of the 4th ACM SIGSIM Conference on Principles of Advanced Discrete Simulation.*

[2] Saleh Soltan, Prateek Mittal, and H. Vincent Poor. 2020. BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid. *IEEE Transaction on NSE* 7 (2020), 1310–1326. https://doi.org/10.1109/TNSE.2019.2922131

[3] Jiaqi Yan and Dong Jin. 2015. A Virtual Time System for Linux-Container-Based Emulation of Software-Defined Networks. In *Proceedings of the 3rd ACM SIGSIM Conference on Principles of Advanced Discrete Simulation.*