Combining Power Simulation and Programmable Network Emulation for Smart Grid Security Application Evaluation

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

Zheng Hu, Yanfeng Qu, Dong Jin
{zhenghu,yqu,dongjin}@uark.edu
University of Arkansas
Fayetteville, AR, USA

ABSTRACT

We present a unique virtual testbed that combines a data-plane programmable network emulator and a power distribution system simulator to evaluate smart grid security and resilience applications. The testbed employs a virtual time system for effective simulation synchronization and fidelity enhancement. We showcase the advantages of the simulation testbed through an anomaly detection case study.

CCS CONCEPTS

• Networks → Network simulations; **• Security and privacy → Network security**; **• Computing methodologies → Modeling and simulation**.

ACM Reference Format:
Gong Chen and Zheng Hu, Yanfeng Qu, Dong Jin. 2023. Combining Power Simulation and Programmable Network Emulation for Smart Grid Security Application Evaluation. In *ACM SIGSIM Conference on Principles of Advanced Discrete Simulation (SIGSIM-PADS '23), June 21–23, 2023, Orlando, FL, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3573900.3593633

1 INTRODUCTION

Cyber-physical systems such as the power grid face a broad spectrum of security risks today. A prime example is the 2015 Ukraine power blackout, where cyber-criminals penetrated the nation's power distribution network, leading to a widespread outage that impacted around 230,000 individuals [7]. Such incidents emphasized the pressing requirement for resilience and security measures to protect vital national infrastructures.

To address this challenge, researchers leverage the recent advances in programmable networks such as P4 [3] to construct a new network architecture that provides strong assurance of the correctness of the management and operations of the communication networks. P4 is a data-plane programming language that defines how packets are processed and forwarded in the network. P4 is a complementary technology to software-defined networking (SDN) and can be used to implement a wide range of network functions, including in-network processing, load balancing, intrusion detection, and more. P4 offers several benefits: it provides increased flexibility by enabling customized and optimized network functions for new and existing protocols; it enhances network performance by offloading workload to the programmable data plane, allowing for faster and more efficient network operation; and it also enables the implementation of in-network functions, improving network efficiency by reducing data transfer and processing times.

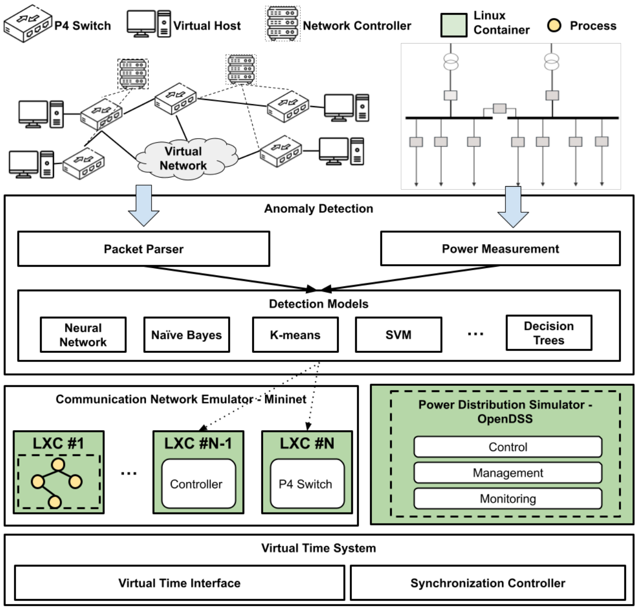

Figure 1: Overview of simulation testbed

Consequently, there is a compelling need to establish P4-compatible smart grid testbeds that would enable the creation of customized network functions that meet the unique security needs of smart grids. In this work, we propose a virtual testbed designed for assessing smart grid security applications, which integrates P4-enabled Mininet [1], a communication network emulator, and OpenDSS [2], a power distribution system simulator. Figure 1 illustrates the three-layer design overview of the simulation testbed.

Virtual time system layer is a Linux container-based framework that improves the temporal fidelity of the virtual testbed constructed upon it. This system allows each virtual node or container in the testbed to have an independent virtual clock that progresses only when the node is executing. Freed from the system clock, nodes can perceive their own virtual time as operating independently and concurrently on separate physical machines, thereby enhancing the testbed's temporal fidelity. The virtual time system comprises two main modules: a virtual time interface that intercepts and manages

SIGSIM-PADS '23, June 21–23, 2023, Orlando, FL, USA

ACM ISBN 979-8-4007-0030-9/23/06.
https://doi.org/10.1145/3573900.3593633

time-related functions like gettimeofday, and a synchronization controller that offers a barrier-based conservative mechanism ensuring each node's clock advances at a consistent pace [4].

Cross-domain simulator layer consists of a communication network emulator, Mininet, and a power distribution system simulator, OpenDSS. Both Mininet and OpenDSS operate inside Linux containers. The underlying virtual time system handles their execution and synchronization. Notably, P4 is integrated with Mininet, providing network programmability for both the control plane (controllers) and the data plane (P4 switches), allowing the virtual testbed to parse and analyze packets in real time.

Application layer can thus utilize information from both communication networks (e.g., packet lengths and port numbers) and power grids (e.g., voltage and frequency) to develop innovative cross-domain security applications. For example, an anomaly detection application, as shown in Figure 1, can combine signatures from both domains and use pre-trained machine-learning models, such as neural networks and decision trees, for classification. Depending on specific requirements, the detection model can be deployed on either network controllers or P4 switches. Network controllers can run more complex models with high accuracy and possess a global view of the network topology to build more accurate detection models, while models deployed on P4 switches can parse and detect packets in real-time but are limited by computational resources, allowing them to run only relatively simple models. However, the latter approach may add less network load as suspicious packets do not need to be mirrored and transported to the controller.

2 CASE STUDY

We use the Manipulation of Demand via IoT (MadIoT) attack [6] to showcase the unique advantages of our testbed in analyzing and evaluating smart grid security applications. MadIoT attacks represent a new category of cyber-physical threats that stem from the cyber world, specifically Internet of Things (IoT) devices, and impact the electrical load in physical power systems. Adversaries employ a botnet to control a large number of high-wattage IoT devices (e.g., air conditioners) and orchestrate a coordinated attack by manipulating power demand (e.g., turning appliances on/off). These attacks can cause significant power disturbances or even cascade failures that result in blackouts [6].

Detecting and mitigating MadIoT attacks present a considerable challenge as information from either the power or network domain alone is insufficient to pinpoint the attack source. For example, solely using power domain data, one could identify an anomaly (e.g., a sharp increase in power demand) by monitoring the grid's status, but the root cause would remain unknown. Conversely, relying only on network domain data, detecting the attack becomes difficult due to the MadIoT attack's distinctiveness. Unlike many distributed attacks (e.g., Mirai [5]) that utilize thousands of IoT bots to launch a DDoS attack on a single target victim, the victims of MadIoT attacks can encompass all IoT devices within a sub-area, rendering traditional DDoS detection models ineffective.

Our virtual testbed provides a unique approach for users to develop detection models by utilizing both network and power domain information. The resulting detection models accurately identify the attack source, enabling the implementation of mitigation measures, such as blocking the IPs of IoT bots. Comparative detection results of four machine learning models are presented in Table 1, demonstrating that models using cross-domain information outperform those relying solely on network-domain data. Logistic Regression exhibits the most significant gap, where the cross-domain model achieves 95.28% accuracy compared to 59.0% for the network-domain model. The other three cross-domain models maintain an average lead of 7% over their network-domain counterparts.

Table 1: Accuracy of detection models using network-domain data and cross-domain data

	Network-domain	Cross-domain
Neural Network	91.43%	98.0%
Decision Tree	91.82%	99.87%
Logistic Regression	59.0%	95.28%
Random Forest	91.99%	99.87%

3 FUTURE WORK

Our testbed has a notable feature where models can be deployed on either controllers or P4 programmable switches. We plan to implement a bi-level detection model that conducts real-time detection at the line rate on the P4 switch and forwards uncertain cases to the controller for further comprehensive analysis.

The software P4 switches integrated with Mininet, such as the BMv2 virtual switches, exhibit a significant performance gap in terms of throughput and processing delay compared to bare hardware P4 switches. Therefore, we plan to incorporate P4 hardware into the loop to significantly enhance the testbed's fidelity.

ACKNOWLEDGMENTS

The authors are grateful for the support of the National Science Foundation (NSF) under Grant CNS-2247721 and the NSF Center for Infrastructure Trustworthiness in Energy Systems (CITES) under Grant EEC-2113903.

REFERENCES

[1] 2021. Mininet: an Instant Virtual Network on your Laptop (or other PC). http://mininet.org/
[2] 2021. OpenDSS: an electric power distribution system simulator. https://www.epri.com/pages/sa/opendss
[3] Pat Bosshart, Dan Daly, Glen Gibb, Martin Izzard, Nick McKeown, Jennifer Rexford, Cole Schlesinger, Dan Talayco, Amin Vahdat, George Varghese, et al. 2014. P4: Programming protocol-independent packet processors. *ACM SIGCOMM Computer Communication Review* 44, 3 (2014), 87–95.
[4] Gong Chen, Zheng Hu, and Dong Jin. 2022. Integrating I/O Time to Virtual Time System for High Fidelity Container-Based Network Emulation. In *Proceedings of the 2022 ACM SIGSIM Conference on Principles of Advanced Discrete Simulation (SIGSIM-PADS '22)*. 37–48.
[5] Brian Krebs. 2016. New Mirai worm knocks 900k Germans offline. https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/
[6] Saleh Soltan, Prateek Mittal, and H. Vincent Poor. 2018. BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid. In *Proceedings of 27th USENIX Security Symposium (USENIX Security 18)*. 15–32.
[7] David E. Whitehead, Kevin Owens, Dennis Gammel, and Jess Smith. 2017. Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. In *Proceedings of 2017 70th Annual Conference for Protective Relay Engineers (CPRE)*. 1–8.