Synchronized Power Simulation and Programmable Network Emulation Testbed for SCADA System Security Evaluation

Zheng Hu
zhenghu@uark.edu
University of Arkansas
Fayetteville, AR, USA

Luke Waind
ldwaind@uark.edu
University of Arkansas
Fayetteville, AR, USA

Yanfeng Qu
yqu@uark.edu
University of Arkansas
Fayetteville, AR, USA

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

ABSTRACT

We present a cyber-physical testbed that synchronizes power simulation with programmable network emulation, specifically designed for evaluating the security of SCADA systems within smart grids. This testbed demonstrates the utilization of information from both communication networks and power systems to accurately detect attacks on DNP3-based SCADA systems, showcasing its effectiveness in addressing cyber-physical security challenges.

CCS CONCEPTS

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

ACM Reference Format:
Zheng Hu, Luke Waind, Yanfeng Qu, and Dong Jin. 2024. Synchronized Power Simulation and Programmable Network Emulation Testbed for SCADA System Security Evaluation. In *38th ACM SIGSIM Conference on Principles of Advanced Discrete Simulation (SIGSIM PADS '24), June 24–26, 2024, Atlanta, GA, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3615979.3662153

1 INTRODUCTION

Supervisory Control and Data Acquisition (SCADA) systems serve as the backbone of our electrical grid's monitoring and control mechanisms. The integrity and reliability of SCADA systems are paramount, not only for the efficient operation of power distribution networks but also for the prevention of potential cascading failures that could lead to widespread service disruption and jeopardize public safety. Thus, these systems are increasingly targeted by sophisticated cyber-physical attacks. Traditional security measures, relying on either the cyber or physical domain, fall short in detecting and mitigating attacks that exploit the interconnected nature of SCADA systems.

Recognizing this need, our approach introduces a synchronized power simulation and programmable network emulation testbed, specifically engineered for the comprehensive security evaluation of SCADA systems. This testbed is pivotal for two key reasons: firstly, it mitigates the risk of interference and potential security breaches to the operational system by providing a controlled, simulated environment for the exploration of cyber-physical threats. Secondly, it incorporates mechanisms for utilizing information of both the communication network traffic and the power system measurements, thereby enhancing the accuracy of attack detection. By simulating realistic scenarios that span both the cyber and physical aspects of SCADA systems, this testbed not only illuminates the intricate dynamics of potential attacks but also aids in the development and validation of more effective detection and mitigation strategies. Through this integrated simulation and emulation approach, we aim to fortify the security posture of SCADA systems against the evolving landscape of cyber-physical threats, ensuring the resilience and reliability of our smart grid infrastructure.

2 TESTBED DESIGN

In this study, we present a cyber-physical testbed designed for evaluating the security of SCADA systems within smart grids. Figure 1 provides an overview of the testbed's architectural design.

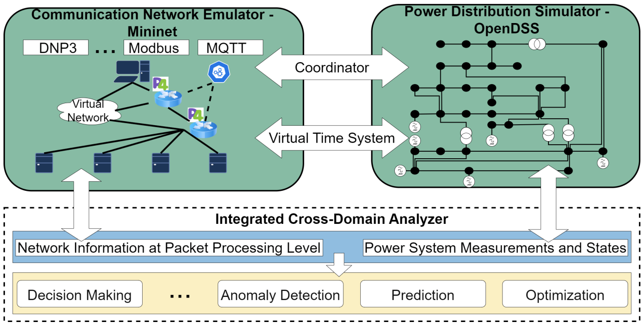
Communication Network Emulator - Mininet
DNP3
...
Modbus
MQTT
Virtual Network
Coordinator
Virtual Time System
Power Distribution Simulator - OpenDSS
Integrated Cross-Domain Analyzer
Network Information at Packet Processing Level
Power System Measurements and States
Decision Making
...
Anomaly Detection
Prediction
Optimization

Figure 1: Testbed Overview

Virtual Time System builds upon the foundational work of our prior work [4] [2] with a substantial modification of the timekeeping routing in the Linux kernel. The new kernel not only imbues emulated containers with virtual time capabilities but also underpins the development of an advanced synchronization method. Our implementation assigns an individual virtual clock to each container, liberating the applications running inside the containers from the global time dictated by the Linux OS. It also allows containers to independently adjust their clocks, slowing down, speeding up, or pausing, in order to maintain synchronization with the power simulation.

Coordinator functions as a central controller overseeing both power system simulation and network emulation, comprising both the network and power coordinators. The power coordinator interacts with the OpenDSS [3] power simulator for circuit setup, request mediation, and time progression. The network coordinator sets up network emulation in Mininet [5], including topology, hosts,

SIGSIM PADS '24, June 24–26, 2024, Atlanta, GA, USA

ACM ISBN 979-8-4007-0363-8/24/06
https://doi.org/10.1145/3615979.3662153

controllers, and P4 switches [1], and handles the timing synchronization between simulation and emulation. It adjusts the speed or pauses processes to align virtual times, listening for synchronization events to manage the network's pace, ensuring temporal accuracy in experiments while maintaining high-fidelity execution within the emulated network through kernel modifications.

Cross-Domain Analyzer operates on the P4 switches, serving as a central hub for collecting and analyzing data across both communication network and power system domains. It utilizes specialized parsers for industrial network protocols to efficiently extract information from packet headers and payloads. Leveraging network details such as topology, timing, and traffic, the analyzer offers thorough monitoring, scrutinizing packet payloads containing power measurement data from OpenDSS simulations to provide extensive insights into the power systems. Additionally, it computes aggregated statistics, such as power flow sums or latency standard deviations, further enhancing its analytical capabilities.

3 CASE STUDY

We utilize the Substation Circuit Breaker Takeover (SCBT) Attack [6] within DNP3-based SCADA systems as a case study. This demonstrates the distinct advantages of our testbed in analyzing and assessing the role of cross-domain information for accurately detecting attacks.

The SCBT attack targets control over substations, causing significant disruptions by disconnecting critical components from the grid. The importance of substations for grid stability means their compromise could lead to widespread blackouts, as evidenced by a 2014 assessment suggesting that compromising just nine critical substations in the U.S. could trigger nationwide outages [8]. Actual SCBT attacks in 2015 and 2016 in Ukraine highlighted this risk, causing substantial power outages [9]. However, this attack presents significant detection challenges when relying solely on network domain information due to its subtle and sophisticated nature. Attackers exploit the specific protocols and operational commands used within SCADA systems, such as those based on DNP3, to issue commands that appear valid to the system. Since these commands, such as open or close circuit breaker instructions, are inherently part of the normal operational repertoire, distinguishing malicious intent from legitimate control actions becomes very difficult without deeper understanding of the operational context and physical behaviors of the power grid.

Figure 2 shows the detection accuracy of SCBT Attacks using our testbed. The vertical bars represent the detection accuracy under two scenarios: using network domain data only and leveraging cross-domain data. The x-axis indicates the number of compromised substations ranging from 1 to 4 on the IEEE 30 bus distribution system during a simulated SCBT attack. The y-axis measures the accuracy of the attack detection, scaled from 80% to 100%. The error bars indicate variability in detection accuracy across 35 simulation runs, reflecting the robustness of the testbed to different attack configurations. The results displayed in blue (network data only) suggest that reliance on a single domain for detection is less effective, with the accuracy level fluctuating notably as more substations are compromised, ranging from 90.97% to 91.75%. In contrast, the utilization of cross-domain information (illustrated in striped bars) significantly improves the detection accuracy, attributed to the rapid changes in power information that occur when multiple substations are compromised. The cross-domain approach achieves higher accuracy ranging from 96.99% to 99.56%, consistently outperforming the method using network data only by a significant margin of 6 to 8 percentage points. The red line connecting the top of the striped bars highlights the consistent accuracy achieved, emphasizing the effectiveness of the cross-domain approach in enhancing SCBT attack detection.

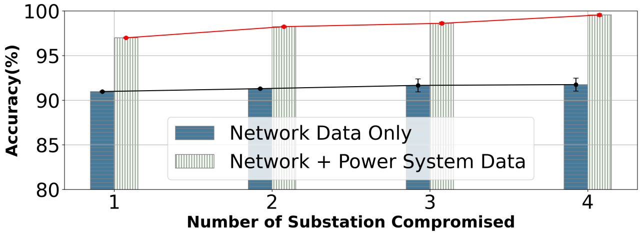

Figure 2: Comparison of SCBT Attack Detection Model Accuracy with and without Cross-domain Information

4 FUTURE WORK

Integration of Hardware P4 Switches: Migrating from software-based P4 switches in Mininet to hardware P4 switches is a crucial next step. This transition will better align the testbed's performance with smart grid operational realities, improving network behavior replication and enabling more realistic assessments of cyber-physical threat responses.

Adoption of Real-Time Power Simulation OPAL-RT: Upgrading our testbed to include OPAL-RT [7] for real-time power simulation marks a pivotal advancement. This shift to a hardware-in-the-loop framework enhances the testbed's realism, allowing for immediate simulation of power grid dynamics and interactions under threat scenarios.

ACKNOWLEDGMENTS

The authors are grateful for the support of the National Science Foundation under Grant CNS-2247721, and EEC-2113903.

REFERENCES

[1] Pat Bosshart et al. 2014. P4: Programming protocol-independent packet processors. *ACM SIGCOMM Computer Communication Review* (2014).
[2] Gong Chen, Zheng Hu, Yanfeng Qu, and Dong Jin. 2023. VT-IO: A Virtual Time System Enabling High-fidelity Container-based Network Emulation for I/O Intensive Applications. *ACM TOMACS* (2023).
[3] Electric Power Research Institute. 2016. OpenDss. https://sourceforge.net/projects/electricdss/
[4] 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 *2016 ACM SIGSIM-PADS*.
[5] Bob Lantz, Brandon Heller, and Nick McKeown. 2010. A network in a laptop: rapid prototyping for software-defined networks. In *2010 ACM SIGCOMM Hotnets*.
[6] Robert Lee, Michael Assante, and Tim Conway. 2016. Analysis of the cyber attack on the Ukrainian power grid. *E-ISAC* (2016).
[7] OPAL-RT Technologies Inc. 2023. OPAL-RT: Real-Time Simulation and Testing Solutions for Power Systems, Power Electronics, and Motor Drives.
[8] Rebecca Smith. 2014. US risks national blackout from small-scale attack. *Wall Street Journal* (2014).
[9] David E Whitehead, Kevin Owens, Dennis Gammel, and Jess Smith. 2017. Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. In *2017 70th Annual conference for protective relay engineers (CPRE)*. IEEE.