Assessing Effects of Cyber-Attacks on Smart Grids through Power Grid and Communication Co-Simulation

1st Sascha Kaven
RTC CyberSec
Hamburg University of Applied Sciences
Hamburg, Germany
sascha.kaven@haw-hamburg.de

2nd Moritz Volkmann
RTC CyberSec
Hamburg University of Applied Sciences
Hamburg, Germany

3th Volker Skwarek
RTC CyberSec
Hamburg University of Applied Sciences
Hamburg, Germany

***Abstract*—The transition to renewable energy sources has led to the development of smart grids, which integrate advanced metering infrastructure and communication networks to enhance grid management. However, this evolution also introduces new cyber-attack surfaces. This paper presents a co-simulation tool designed to assess the impact of cyber-attacks on smart grids by simulating both power grid and communication components. Focusing on false data injection attacks, the tool evaluates the effects of manipulated measurement data on state estimation and grid stability. Initial results demonstrate the tool's capability to identify vulnerabilities and inform the development of robust security measures for future smart grid control systems.**

***Index Terms*—smart grid, cyber-attacks, power grid simulation, co-simulation.**

I. Introduction

To combat climate change, many efforts have been made to transition from fossil energy production to renewable energy sources. While large-scale energy plants, such as wind and photovoltaic (PV) systems, play a significant role, small-scale energy production has become increasingly accessible to end consumers through rooftop PV systems. This decentralization introduces new challenges for distribution grid operators (DGOs), who must balance energy production and consumption while maintaining grid stability. To achieve this, modern power grids are evolving into *smart grids*, incorporating metering infrastructure, communication networks, and control systems.

The German energy market, where our work is situated, is undergoing a regulated smart grid transformation driven by the Renewable Energy Sources Act. This mandates the deployment of advanced metering infrastructure (AMI) and smart meter gateways (SMGW) to enable real-time state estimation and grid control. While this transformation improves grid management, it also introduces new cyber-attack surfaces. As a critical infrastructure, the power grid falls under the Network and Information Security Directive NIS-2 [1] of the European Union, requiring robust security measures and continuous monitoring.

This work is part of the project SimCyberGrid, which is funded by the German Federal Ministry for Education and Research.

In modern smart grid architectures, network softwarization plays a crucial role. The increasing adoption of software-defined networking (SDN) and network function virtualization (NFV) enables flexible, scalable, and intelligent network control [2]. However, these technologies also introduce new security challenges, particularly regarding data and control plane resilience, network monitoring, and attack mitigation strategies. In this work, we explore the impact of cyber-attacks on smart grids, regarding network softwarization technologies as both an enabler and a target of attacks.

II. Research Gap

Existing research on smart grid security often focuses on traditional cybersecurity measures without considering the implications of software-defined networking and network virtualization ([3], [4]). While SDN and NFV offer enhanced flexibility and automation for smart grid communication, they also introduce vulnerabilities, such as controller-targeted attacks, topology poisoning, and denial-of-service attacks [5]. Additionally, programmable data planes allow fine-grained traffic control but can be exploited for malicious packet manipulation.

Thus, a major research gap exists in understanding how network softwarization affects the security and resilience of smart grid communications. In particular, the interplay between SDN-based control mechanisms, AMI data flows, and attack vectors such as false data injection attacks (FDIA) requires further investigation.

III. Our Contribution

To assess the impact of cyber-attacks on the smart grid, our goal is to create a co-simulation tool, which simulates both the power grid component and the communication component of the grid. This co-simulation tool will be used to simulate a plethora of cyber-attacks on the smart grid and study the effects they have on both the grid and the simulation to harden the attack surfaces for the smart grid control systems of the future by combatting the attacks automatically and educating DGO personnel on how to react to them. In this first iteration

of the simulation tool, we will focus on the AMI and state estimation and present the capabilities of the simulation tool to measure the impact of FDIA on the power grid.

IV. Co-Simulation Design

The functions that we simulate as part of the aforementioned smart grid control system are the aggregation of power flow calculation, congestion, and load calculation, aggregation of AMI measurement data, and state estimation, including bad data detection. The power grid simulation is conducted with the Python-based simulation framework PandaPower [6] with a low-voltage distribution grid model with load profiles from the SimBench [7] project. However, it offers the possibility to replace it with another compatible grid for testing different scenarios. To simulate the communication between the DGO's smart grid control system and the SMGW in the grid, a separate communication simulation is used. This simulation is conducted with the network simulation tool ns-3, which simulates the TCP/IP connections between the DGO and the SMGW.

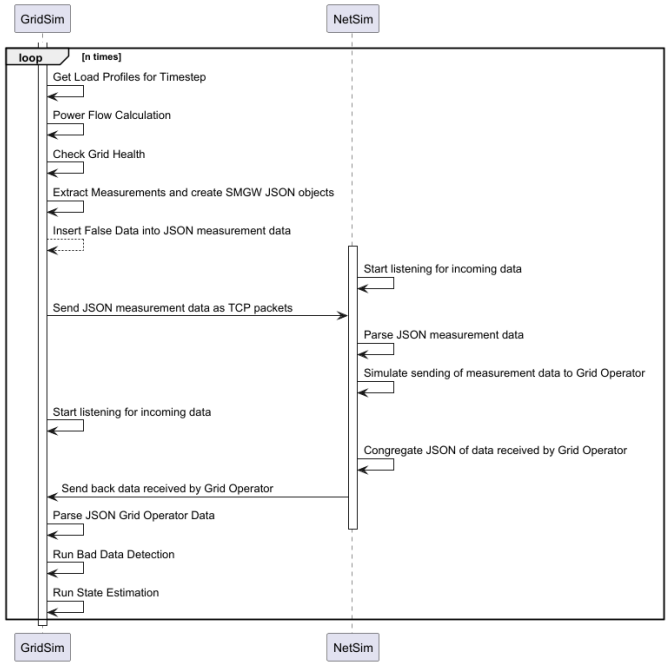

Fig. 1. Co-simulation sequence

To organize the co-simulation and ensure proper execution timing, a TCP socket-based communication framework is used. Each simulator establishes a TCP socket to listen for incoming packets and facilitate data transfer. The sequence diagram in Figure 1 shows the ordered actions of each simulator and its interface. The power grid simulator starts by loading data from the SimBench load profile for the current timestep, which serves as input for power flow calculation and generates measurement values. Depending on the settings, an FDIA may be performed. The measurement data, formatted as JSON files, are sent from the power grid's TCP socket to the communication simulator's TCP socket. Upon receiving the data, the simulation of the communication between the SMGWs and the grid operator is conducted. The power grid simulator then waits for incoming messages. Once the grid operator node aggregates the measurement data, they are forwarded to the communication simulator's TCP socket, which relays them to the power grid's TCP socket. The power grid simulation resumes with bad data detection and state estimation. This iterative process continues until all load profile data is processed, ensuring an orderly and comprehensive co-simulation. This approach highlights the systematic coordination and communication between simulators necessary for accurate co-simulation outcomes.

V. False Data Injection Attacks

In this first iteration of the simulation tool, we focus on FDIA as an attack vector for cyber-attacks. In an FDIA, the measurement data of one or several meters is manipulated to change the outcome of the state estimation as the attacker intends, such as suggesting a normal grid load, when in reality grid components are being overloaded. In a real-world scenario, the attacker has to obtain control over meters or the communication channels between the meters and the DGO, e.g. through a replay attack, to manipulate the measurement data. Since the cyber-security of AMI is a complete field of research on its own, we do not include this step in the simulation but rather assume that the attacker already controls some of the meters and can alter their measurement data freely. While the attacker theoretically could input any measurement data at the compromised meters, most state estimations used by grid operators include a *bad data detection*. This process was originally designed to remove measurement errors from the dataset, usually by some form of distribution test such as 2-norm or χ^2 tests, but serves an additional purpose as an unintended protection against FDIA by removing measurement data that does not match the distribution of the dataset. This forces the attacker to manipulate the measurement data only in certain boundaries, so as not to trigger bad data detection.

In the scope of this work, we tested the ability to simulate the effects of FDIA by injecting randomly generated false measurements at 6 of the 43 available metering points. To avoid triggering bad data detection, the boundaries for each measurement voltage (U), voltage angle (φ), active power (P), and reactive power (Q) were lowered in a boundary-value analysis to approach the ideal range for FDIA for this specific grid model. The FDIA simulation was then simulated via the process described in the previous section in 96 timesteps representing 15-minute intervals.

Figure 2 shows the impact of the FDIA attack by measuring the deviation from the original state estimation data. For this, a metric similar to the coefficient of variation was used, where the difference between the manipulated and original state variables is divided by the sum of their absolute values. Thus, the values for the metric range between -1 (large negative difference) and 1 (large positive difference). Each of the four subfigures represents one measurement type, where the colored line shows the mean deviation per node over all time steps

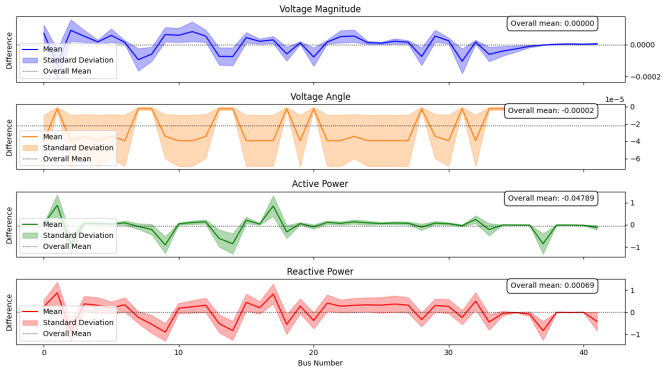

Fig. 2. Simulation Results

from the original state estimation data and the colored area around it represents the standard deviation. This gives an overview of which nodes were particularly affected by the FDIA and how large the deviations were on average. In the simulation tool, this is combined with other metrics, such as a congestion calculation tool, to accurately predict the impact of an FDIA on the power grid.

VI. Outlook

While the simulation tool described in this paper offers interesting insights into the effect of FDIA on the low-voltage distribution grid, this paper serves rather as an outlook and there are many additions to be made and a plethora of further research questions to be addressed in future research.

While writing this paper, the developed tool is still in an early stage. However, it offers a solid foundation for future works, including the addition of functionalities of SDN and NFV, as well as the improvement of the communication simulation through the inclusion of e.g. encryption and simulation of wireless communication. Furthermore, the integration of control sequences derived from congestion management processes will play a big role in the smart grid control system of the future and should be rigorously analyzed regarding cyber-security. Additionally, FDIA are only one possible attack vector on the smart grid and the simulation tool will be adapted and used to test the impact of different attack vectors, including SDN attacks.

References

[1] European Parliament. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance), December 2022.

[2] Xinshu Dong, Hui Lin, Rui Tan, Ravishankar K. Iyer, and Zbigniew Kalbarczyk. Software-Defined Networking for Smart Grid Resilience: Opportunities and Challenges. In *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*, CPSS '15, pages 61–68, New York, NY, USA, April 2015. Association for Computing Machinery.

[3] Jianguo Ding, Attia Qammar, Zhimin Zhang, Ahmad Karim, and Huansheng Ning. Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions. *Energies*, 2022.

[4] Shahid Tufail, Imtiaz Parvez, Shanzeh Batool, and Arif Sarwart. A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid. *Energies*, 14, 2021.

[5] Mubashir Husain Rehmani, Alan Davy, Brendan Jennings, and Chadi Assi. Software Defined Networks-Based Smart Grid Communication: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials*, 21(3):2637–2670, 2019. Conference Name: IEEE Communications Surveys & Tutorials.

[6] Leon Thurner, Alexander Scheidler, Florian Schäfer, Jan-Hendrik Menke, Julian Dollichon, Friederike Meier, Steffen Meinecke, and Martin Braun. Pandapower—An Open-Source Python Tool for Convenient Modeling, Analysis, and Optimization of Electric Power Systems. *IEEE Transactions on Power Systems*, 33(6):6510–6521, November 2018. Conference Name: IEEE Transactions on Power Systems.

[7] Steffen Meinecke, Annika Klettke, Dzanan Sarajlic, Jörg Dickert, Matthias Hable, Franziska Fischer, NetzeBW GmbH, Martin Braun, Albert Moser, and Christian Rehtanz. GENERAL PLANNING AND OPERATIONAL PRINCIPLES IN GERMAN DISTRIBUTION SYSTEMS USED FOR SIMBENCH. 2019.