Pacific Northwest
NATIONAL LABORATORY

PNNL-37022

Modeling Communication Infrastructures of Cyber Physical Systems

November 2024

Joshua Bigler
Oceane Bel
Ivan Callejas
Gregory Thomas
Garret Seppala

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from
the Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062
www.osti.gov
ph: (865) 576-8401
fox: (865) 576-5728
email: reports@osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov

PNNL-37022

Modeling Communication Infrastructures of Cyber Physical Systems

November 2024

Joshua Bigler
Oceane Bel
Ivan Callejas
Gregory Thomas
Garret Seppala

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Abstract

This effort explores modeling cyber infrastructure, including communication devices like switches, routers, sensors, and controllers, and physical media attributes like propagation of radio signals, in coordination with power distribution system model layouts. To do this, the project studies real-world configurations to define axioms of how different communication media is deployed with control equipment. These axioms will be used to develop tools to generate realistic cyber infrastructure models from starting power system models. This effort leverages and builds on the co-simulation platform developed by the other RD2C projects. The axioms and tools will be validated and demonstrated with the NS3 simulation tool as part of a co-simulation to show the behavior/impacts of cyber infrastructure on control operations.

Acknowledgments

This research was supported by the Resilience through Data-Driven intelligently-Designed Control (RD2C), under the Laboratory Directed Research and Development (LDRD) Program at Pacific Northwest National Laboratory (PNNL). PNNL is a multi-program national laboratory operated for the U.S. Department of Energy (DOE) by Battelle Memorial Institute under Contract No. DE-AC05-76RL01830.

Contents

Figures

1.0 Introduction

Power grids are increasingly relying on communication networks to perform many crucial functions, such as monitoring and control, data transmission, remote operations, and others. These systems use a wide variety of communications technologies, topologies, and protocols to perform these tasks. When studying the effects of adverse situations on power grid systems, it is important to consider the communications layer for these power grid systems as any failures, delays, or compromises of this layer can negatively impact the operations of the power grid.

However, existing power grid network models face limitations when attempting to simulate communications in a power grid system. They may oversimplify the network's topology, thus failing to represent the complexity of the communication components. They may also fail to represent the stochastic nature of power load demands and energy sources (such as renewables) [2]. The ability to simulate critical events like large-scale cyber attacks may be limited or the models may lack real-time data integration. Network models should adequately the highly-reliable nature of power grids and also meet the workload demands while working within power, throughput, and other constraints.

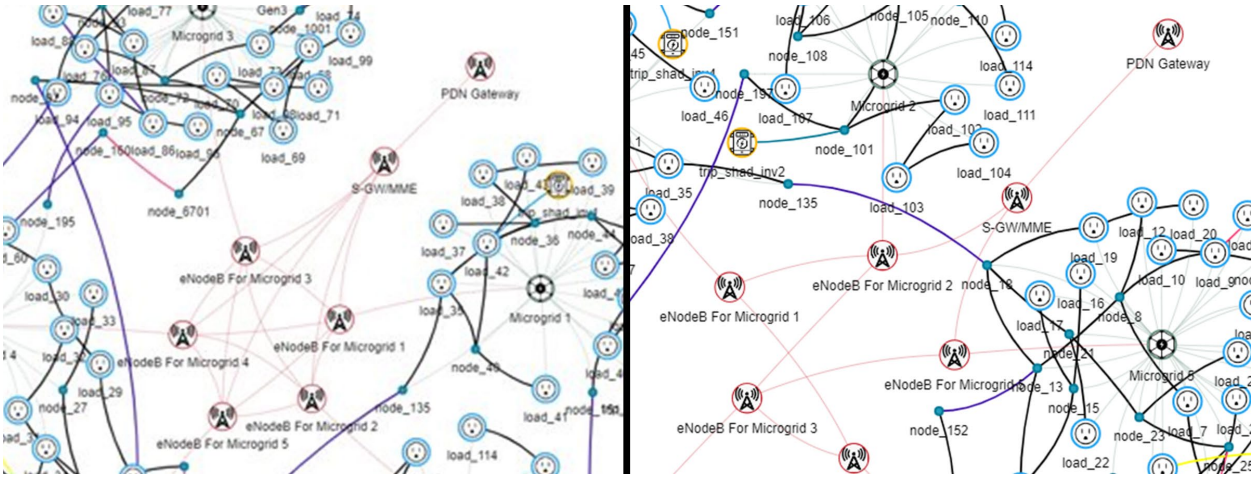

Figure 1. Two LTE communications topologies

1.1 Background

The RD2C effort has developed the ability to simulate power grid systems using a variety of tools. Network Simulator 3 (NS3) is used to simulate the communications layer between power grid components in most of the tooling. For example, Network Attack Testbed In Power Grid (NATIG) uses NS3 in conjunction with GridLAB-D for a containerized co-simulation platform. It can simulate cyber security scenarios against a power grid system. NATIG contains different cyber security situations, as well as a library of both power grid and communications models to select from and simulate. NATIG provides valuable metrics in determining the impact on a power grid communication system, such as packet loss, jitter, and delay of packets.

2.0 Advancements

This section describes the technical advancements made to the RD2C suite of tooling and capabilities under this effort. These include developing high-fidelity models to existing simulation capabilities, integrating new functionality and capabilities to the simulators, and providing communication components for Hardware-In-The-Loop simulations.

2.1 Communications Models in NATIG

NATIG comes bundled with a selection of both 123-node and 9000-node GridLAB-D models, as well as a library of communications models tailored to the two power grid models. Improving the communications components is a point of emphasis in this effort.

The NATIG tool now has communications models for the following technologies and topologies:

- 5G
- 4G LTE
- 3G
  - Star, ring, and mesh topology shapes

This library gives more options for analysts and researchers to explore how different communications configurations are affected by cyber security events. More work is to be done here, as there are more technologies and topologies that can be added, such as LoRaWAN.

2.2 NATIG integration with GLIMPSE

Grid Layout Interface for Model Preview and System Exploration (GLIMPSE) is a grid visualization tool developed and maintained by RD2C efforts, which aids in visualizing GridLAB-D models and seeing the components connected to each other. Later versions of GLIMPSE incorporated the ability to visualize overlay components, including associating grid components to microgrids, as well as adding communications components to the microgrids. This gives users the ability to visualize both the grid models as well as the communications model associated with the grid component.

GLIMPSE and NATIG have been separate components – GLIMPSE would only display static models, while NATIG would run simulations off them. This effort introduced an integration between them – simulations in NATIG now can update a GLIMPSE visualization based on events occurring in the simulation. Grid and communication components are highlighted when there is activity occurring there. A component can be highlighted red when it reaches established thresholds – for example, high activity can turn a communications component red. This gives analysts a live visual feed to show the impacts of cyber events on power grid and communications model.

The integration is in the early phase – the thresholds as well as the highlighting colors are hard-coded into the integration. Future work will involve the ability to give options on how NATIG interacts with the GLIMPSE visualization, such as giving the ability to select color palates, set thresholds for different NATIG metrics, and better indicate the direction in which packets are traversing in the communication components.

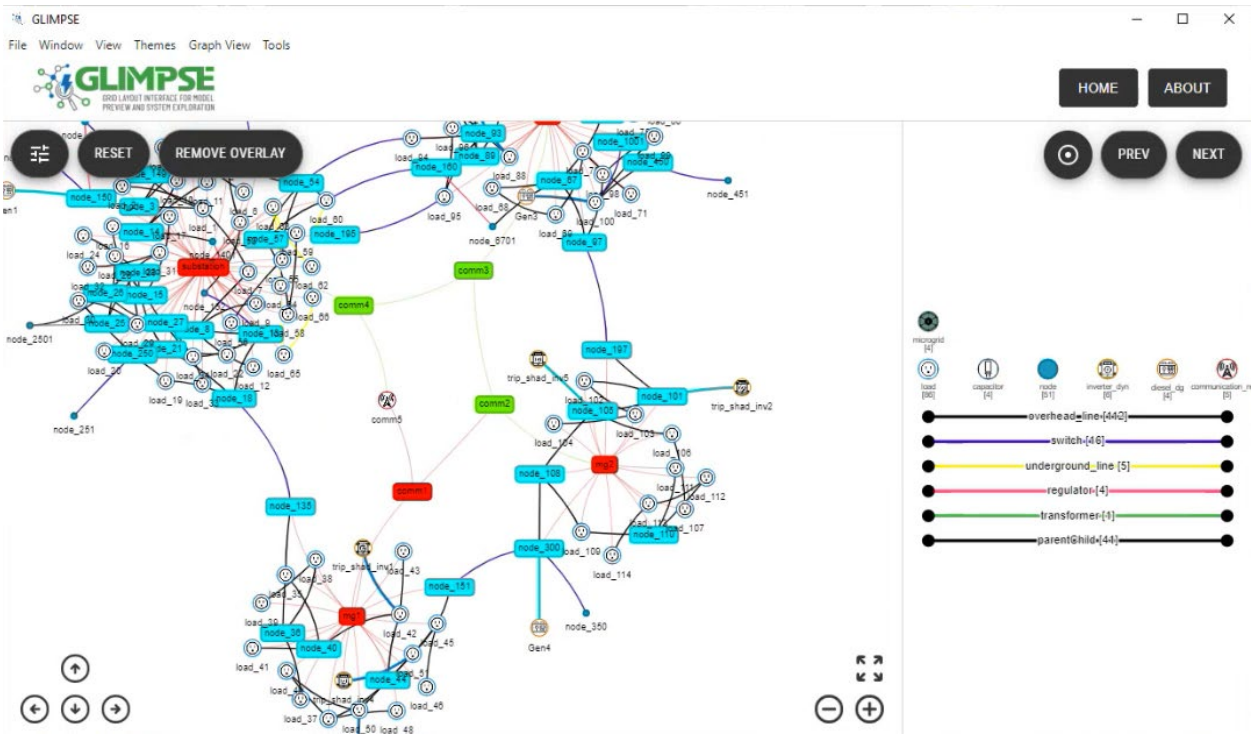

Figure 2. Demonstration of NATIG's integration with GLIMPSE

2.3 Integration with HIL

In addition to the containerized co-simulation tool, there are efforts to create a hardware-in-the-loop (HIL) simulation platform. The benefit with hardware-in-the-loop in this context is it can involve actual devices sending actual network packets. The goal is to leverage NS3's TapBridge module to use actual network packets generated outside of NS3, run it through a communications model, and eventually the packet reaches its destination outside of the NS3 model. Hosts outside this NS3 model acts as agents simulating different power grid components attempting to communicate with each other.

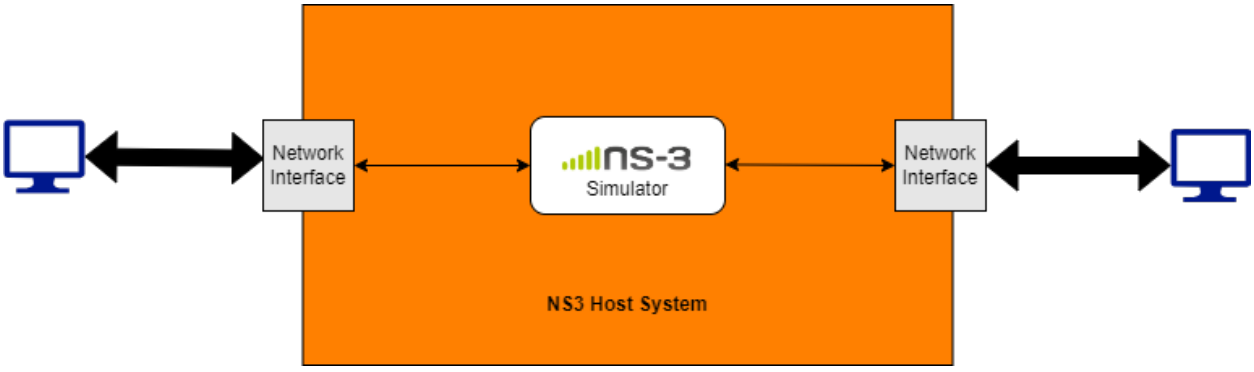

Figure 3. NS3 HIL diagram

The idea is to be able to "plug and play" different communications models into the HIL environment and measure their impacts the agents. Early experiments on this effort involved standing up a dedicated virtual machine that runs NS3 with the tap bridge, and having two other

virtual machines on two different ends of this NS3 host in different networks, each of them configured to use the NS3 host as their gateway. A simplistic “passthrough” model was used to show that packets from one host make its way to the other. Future work will involve incorporating more complex communications models, such as larger number of networks and using topologies such as mesh and ring topologies.

3.0 Conclusion

In this report, we provide a summary of the work done to incorporate high-fidelity communications models with the RD2C suite of simulation capabilities. This work aims to provide higher confidence in the ability to understand the impact of adverse events on power grid systems that can face many challenges and threats in the cybersecurity landscape. The work done will provide a platform to improve the ability to further improve RD2C's modeling capabilities, both with co-simulation platforms and hardware-in-the-loop platforms.

4.0 References

1. K. Shafiee , J. B. Lee, V. C. Leung, and G. Chow, “Modeling and simulation of vehicular networks,” in Proceedings of the first ACM international symposium on Design and analysis of intelligent vehicular networks and applications, pp. 77–86, 201
2. S. Kumar Samanta and C. K. Chanda, “Stability analysis in a smart grid network due to dynamic demand load respond,” in 2017 International Conference on Computer, Electrical & Communication Engineering (ICCECE), pp. 1–5, IEEE.

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354

1-888-375-PNNL (7665)

www.pnnl.gov