Remotely Accessible Cyber-Physical System Testbed for Power Grid's Security and Reliability

Mazharul Islam
Electrical and Computer Engineering
North South University
Dhaka, Bangladesh
mazharul.islam1@northsouth.edu

Tahmid Ashraf Khan
Electrical and Computer Engineering
North South University
Dhaka, Bangladesh
tahmid.khan1@northsouth.edu

Sunjare Zulfiker
Electrical and Computer Engineering
North South University
Dhaka, Bangladesh
sunjare.zulfiker@northsouth.edu

A S M Jahid Hasan
Electrical and Computer Engineering
North South University
Dhaka, Bangladesh
jahid.hasan12@northsouth.edu

Hafiz Abdur Rahman*
Electrical and Computer Engineering
North South University
Dhaka, Bangladesh
hafiz.rahman@northsouth.edu
*Corresponding author

2024 8th International Conference on Smart Grid and Smart Cities (ICSGSC) | 979-8-3503-7740-8/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICSGSC62639.2024.10813893

***Abstract*—With the increasing complexity and integration of digital technologies in power grids, ensuring their security and reliability has become a critical challenge. Cyber-physical threats pose significant risks to the stability and functionality of these systems. To address these challenges, there is a need for comprehensive testbeds that can simulate real-world scenarios and assess the resilience of power grid operations under various cyber-physical attack vectors. This paper presents a remotely accessible cyber-physical system (CPS) testbed that we designed and built to study the security and reliability issues of power grids. Utilizing Node-RED in the front-end and integrating GridPACK, HELICS, and NS3 in the back-end, the testbed provides comprehensive capabilities for simulating, monitoring, and analyzing power grid performance under various scenarios, including various kinds of cyber-attack. The CPS testbed enables us to measure performance metrics such as network latency, packet loss, voltage stability, and system response time are monitored under normal and attack conditions through various simulations and real-time data analysis. This testbed provides a valuable tool for researchers and engineers to study and improve power grid security and resilience.**

***Index Terms*—Cyber-physical system, power system, CPS testbed, smart grid, Node-RED, GridPACK, HELICS, NS3, PMU**

I. Introduction

The security and reliability of power grids are critical for the continuous and stable delivery of electricity. As power grids become increasingly complex and interconnected through the integration of intelligent devices, they face numerous challenges, including the rising threat of cyber-physical attacks [1]. These attacks can disrupt operations, leading to significant economic losses and safety concerns. Therefore, advanced tools and methodologies are required to monitor, analyze, and enhance the security and reliability of modern power grids.

Traditionally, power grid monitoring and control have relied on Supervisory Control and Data Acquisition (SCADA) systerms [2]. However, SCADA systems, while effective, are relatively slow and often not GPS synchronized are also vulnerable to cyber threats and lack the flexibility needed for modern grid management. This necessitates the development of more resilient and adaptable systems capable of addressing both physical and cyber challenges. The integration of Information and Communication Technologies (ICT) with power systems, leading to the emergence of smart grids, has paved the way for enhanced monitoring and control capabilities [3].

In recent years, cyber-physical system (CPS) testbeds have emerged as valuable tool for simulating and evaluating the performance of power grids under various conditions. These testbeds allow researchers and engineers to model power grid components, simulate operational scenarios, and analyze the impact of potential threats [4]. However, the need for remotely accessible and comprehensive testbeds that can integrate advanced technologies for real-time monitoring and analysis remains unfulfilled.

The development of such testbeds is further driven by the increasing frequency and sophistication of cyber-attacks targeting critical infrastructure. Incidents such as the 2015 Ukrainian power grid attack highlight the devastating potential of coordinated cyber-physical attacks [5]. These events underscore the urgency of developing advanced tools and frameworks that can simulate and analyze such threats, providing valuable insights into grid vulnerabilities and enabling the development of effective mitigation strategies.

This paper presents a remotely accessible cyber-physical system testbed specifically designed and built by our group to address the challenges of power grid security and reliability. The testbed integrates Node-Red for frontend development and GridPACK, HELICS, and NS3 for backend processing. In addition, in this project, we built Phasor Measurement Unit (PMU) devices to capture and process real-time power network data in the CPS Testbed. This setup enables detailed simulations, synchronization of power grid and communication network interactions, and real-time visualization of results, thereby providing a comprehensive tool for monitor-

ing, analyzing, and enhancing power grid performance. Our contributions are as follows:

- **Development of a Comprehensive Testbed:** Creation of a robust testbed that integrates advanced technologies for real-time monitoring, simulation, and analysis.
- **Integration of Advanced Technologies:** Utilization of Node-RED for frontend modeling, and GridPACK, HELICS, and NS3 for backend processing, ensuring detailed simulations and synchronized interactions.
- **Detailed Modeling and Simulation:** Accurate modeling of the IEEE 14 bus system, with the ability to simulate complex operational scenarios and cyber-physical threats such as Distributed Denial of Service (DDoS) attacks.
- **Holistic View of Grid Performance:** Synchronization of power grid and communication network simulations, providing a comprehensive view of grid performance and vulnerabilities.
- **Real-time Visualization:** Implementation of real-time visualization through Node-RED, offering an intuitive interface for researchers and engineers to monitor and analyze results.

The rest of the paper is organized as follows. Section II provides the background on CPS testbed. Section III reviews related work on cyber-physical system testbeds for power grid security and reliability. Section IV explains the CPS testbed model. Section V details the implementation on the testbed. Section VI presents the results and performance analysis. Section VII highlights the contributions and compares them with existing works. Section VIII discusses limitations and future work, concluding the paper.

II. Background

This section provides an overview of the key concepts and simulators used in our cyber-physical system testbed such as Node-RED, NS3, GridPACK, and HELICS.

A. Node Red

Node-RED is a flow-based development tool for visual programming, designed for wiring together hardware devices, APIs, and online services [6]. Developed by IBM, it provides a browser-based editor that allows users to create flows using a wide range of nodes, which can be deployed to its runtime with a single click.

B. GridPACK

GridPACK (Grid Parallel Advanced Computational Kernel) is a high-performance computing framework designed for power grid simulations [7]. Developed by the Pacific Northwest National Laboratory (PNNL), GridPACK leverages parallel computing to handle large-scale power system models, enabling detailed analyses of grid stability, load flow, and contingency scenarios.

C. Network Simulator 3

NS3 (Network Simulator 3) is an open-source discrete-event network simulator primarily used for research and educational purposes [8]. It provides a simulation environment for networking research, supporting the design, implementation, and testing of network protocols.

D. HELICS

HELICS (Hierarchical Engine for Large-scale Infrastructure Co-Simulation) is a co-simulation framework developed by the U.S. Department of Energy [9]. It is designed to facilitate the integration of multiple simulation tools, enabling the study of complex systems that involve interactions between different domains such as power grids, communication networks, and cyber-physical systems.

In our proposed CPS testbed, these simulators collaborate to improve power grid security and reliability, enabling comprehensive monitoring, simulation, and analysis of grid operations.

III. Literature Review

This section reviews the existing literature on CPS testbeds, focusing on their design, functionality, and application in power system vulnerability assessment.

Mishchenko *et al.* (2024) [10] introduced a comprehensive CPS testbed developed at the Norwegian University of Science and Technology's National Smart Grid Laboratory. This testbed integrates physical, virtual, and cyber-physical components using real-time digital simulation to evaluate power system vulnerabilities against cyber-physical threats. The testbed examines the impact of various cyberattacks, providing a holistic view of power system operations. However, their limitation lies in its current focus on attack simulations without an equally detailed exploration of defensive mechanisms.

Zheng *et al.* (2024) [11] presented a co-simulation framework integrating two open-source power grid simulators, GridPACK for transmission grid simulation and GridLAB-D for distribution grid simulation, using HELICS. This setup allows for fast parallel dynamic simulation of transmission grids with enhanced system dynamics from interconnected distribution grids. However, the complexity of integrating different simulation tools and maintaining parallelism poses significant challenges.

Chamana *et al.* (2023) [12] introduces a comprehensive CPS testbed designed to support research and education in the field of smart grids. This testbed integrates real-time simulation with protection and automation devices and a supervisory control and data acquisition (SCADA) system. The testbed analyzes the system's performance before and after cyberattacks using packet-sniffing tools and network packet analyzers, providing insights into the complex interdependencies between the cyber and physical domains. However, a notable limitation is the testbed's reliance on hardware-specific software platforms, which can restrict accessibility and limit user access to a single user at a time.

M. Mustafa *et al.* (2021) [13] presents a comprehensive co-simulation framework integrating NS3 for communication network simulation, GridPACK for power grid simulation, and HELICS for co-simulation management. This framework enables detailed analysis of synchrophasor network performance and its impact on power system applications, using an IEEE 39-bus test system to demonstrate the effectiveness of the approach. A notable limitation of this framework is the complexity of integrating different simulation tools and ensuring synchronized, efficient data exchange across them, which may pose challenges in maintaining parallelism and scalability in large-scale simulations.

Becejac *et al.* (2020) [14] introduced the PRIME testbed developed at the Pacific Northwest National Laboratory. This testbed integrates real-time transmission system simulation with industry-grade energy management system software and remote hardware-in-the-loop (RHIL) capabilities. However, the PRIME testbed faces limitations in scalability and flexibility, particularly in modeling larger power systems and ensuring consistent real-time performance across complex setups.

IV. The CPS TESTBED Model

In this section, we describe our model of a comprehensive system proposal that leverages the CPS testbed. To create an effective CPS testbed for enhancing power grid security and reliability, we employ Node-RED for front-end development and integrate GridPACK and NS3 for back-end processing using HELICS which is shown in Fig. 1. This integration enables seamless data exchange and synchronized operation, essential for accurate simulation and analysis of power grid scenarios.

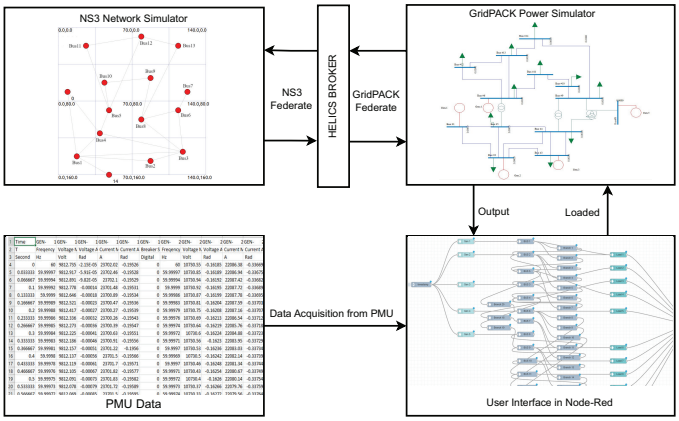

Fig. 1. System model of the proposed scheme

1) **System Initialization and Front-end Configuration**
   - **Data Acquisition from PMU:** Node-RED is configured to receive real-time data from Phasor Measurement Units (PMUs). These PMUs data can be collected from PMU device or user can use custom data based on preference.
   - **Node-RED Setup:** The IEEE 14 bus system is modeled in Node-RED, consisting of 14 buses, 5 generators, and 11 loads. Node-RED generates a JSON file representing the system configuration.
   - **Data Conversion:** The JSON file is converted into RAW data, which is then loaded into GridPACK for backend processing.
2) **Back-end Configuration and Integration**
   - **GridPACK Setup:** GridPACK loads the RAW data and starts the physical simulation of the power grid.
   - **NS3 Setup:** NS3 is configured to simulate the communication network within the power grid. It uses HELICS to receive the initial state of the grid from GridPACK, allowing it to simulate network conditions accurately. In NS3, we defined the specific parameters of the DDoS attack, including which buses (nodes) will be targeted, the nature of the attack (e.g., flooding with network packets), and the attack duration.
   - **HELICS Setup:** Both GridPACK and NS3 are integrated with HELICS, making them HELICS federates. This integration ensures efficient data exchange and synchronization between the simulations.
3) **Data Exchange Definition** In this setup, two HELICS Value Federates are created for both the GridPACK and NS3 simulators to simulate their respective subsystem behaviors. A central HELICS Broker is established to ensure synchronization within the federation and facilitate their communication via a publication and subscription mechanism which is illustrated in Fig. 2.

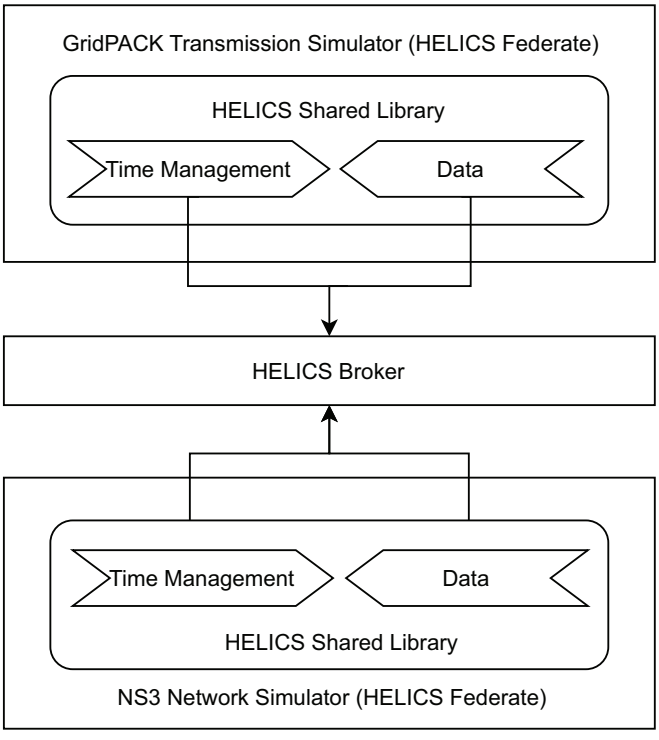

Fig. 2. Schematic of HELICS federated simulation environment for GridPACK and NS3 integration

- **GridPACK Federate:** Publishes grid status updates,

including operational states and performance metrics of buses, generators, and loads.

- **NS3 Federate:** Subscribes to grid status updates to understand the state of the power grid and simulate network conditions accordingly.
- **NS3 Federate:** Publishes network performance data (e.g., latency, packet delivery status) and any network-related events affecting the grid.
- **GridPACK Federate:** Subscribes to network performance data to adjust the power grid simulation based on communication network conditions.

4) **Synchronization Mechanism**
   - HELICS manages the synchronization between GridPACK and NS3, ensuring that both federates proceed in lockstep. This involves exchanging data at each simulation step or upon specific event triggers.

V. Implementation

The implementation of CPS testbed involves several key stages to ensure comprehensive monitoring, simulation, and analysis of power grid operations. Here are the detailed steps:

1) **Initialization:** Node-RED models the IEEE 14 bus system, consisting of 14 buses, 5 generators, and 11 loads, and generates the initial JSON configuration. This JSON file is then converted into RAW data and loaded into GridPACK.
2) **Simulation Coordination:**
   - **Step 1:** GridPACK runs the power grid simulation, shows the real and reactive power generated by various generators connected to different buses in the power grid. It also presents the phase angles and voltage magnitudes at each bus, which is shown in Fig. 3.

Generator Power

Bus Number	GenID	Pgen	Qgen
1	1	232.393272	-16.549301
2	1	40.000000	43.557100
3	1	0.000000	25.075348
6	1	0.000000	12.730944
8	1	0.000000	17.623451

Bus Voltages and Phase Angles

Bus Number	Phase Angle	Voltage Magnitude
1	0.000000	1.060000
2	-4.982589	1.045000
3	-12.725100	1.010000
4	-10.312901	1.017671
5	-8.773854	1.019514
6	-14.220946	1.070000
7	-13.359627	1.061520
8	-13.359627	1.090000
9	-14.938521	1.055932
10	-15.097288	1.050985
11	-14.790622	1.056907
12	-15.075585	1.055189
13	-15.156276	1.050382
14	-16.033645	1.035530

Fig. 3. Bus voltage and phase angles in GridPACK

   - **Step 2:** NS3 receives the state information from HELICS, simulates the communication network conditions, and publishes network performance data back to HELICS.
   - **Step 3:** GridPACK receives the network performance data from HELICS and adjusts the grid simulation to reflect any communication impacts.
   - **Step 4:** Both simulations proceed to the next step in a synchronized manner, with HELICS ensuring timing and data consistency.
3) **DDoS Attack Simulation:**
   - **Attack Initialization:** NS3 is configured to simulate a Distributed Denial of Service (DDoS) attack targeting multiple buses in the grid is shown in Fig. 4.

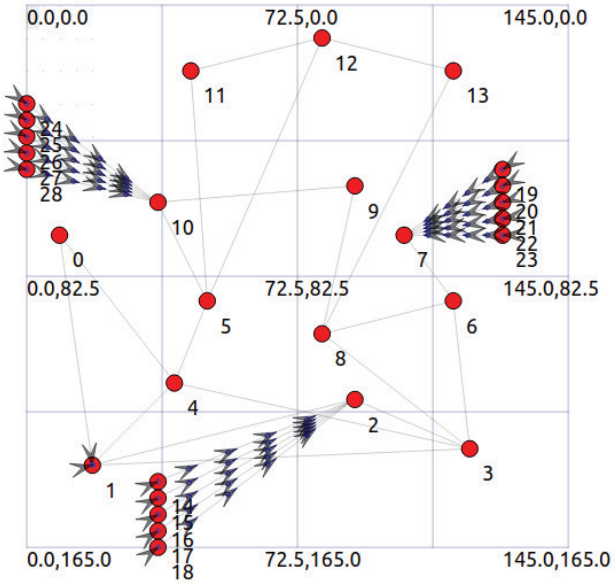

Fig. 4. DDOS attack on multiple buses scenario

   - **Attack Execution:** During the simulation, NS3 launches the DDoS attack by flooding the targeted buses with excessive network packets.
   - **Impact Analysis:** NS3 publishes the impact of the DDoS attack, such as increased latency and packet loss, to HELICS.
   - **GridPACK Adjustment:** GridPACK receives the attack impact data and adjusts the power grid simulation to reflect the disrupted communication and operational impacts.
4) **Real-time Visualization:** Node-RED receives the final simulation results from GridPACK via HELICS, visualizing the performance and interactions of the power grid and communication network in real-time, including the impact of the DDoS attack.
5) **End of Simulation:** The simulation concludes once all scenarios, including the DDoS attack, are fully simulated and results are analyzed. Both GridPACK and NS3 finalize their processes through HELICS.

VI. Results and Performance Analysis

This section presents the results of the simulations and a detailed performance analysis.

A. Results

- **Simulation of Normal Operations:** In the initial phase, the IEEE 14 bus system was modeled using Node-RED, and the normal operations of the power grid were simulated using GridPACK. The performance metrics such as voltage levels, power flows, and generator outputs were monitored and analyzed.
- **Simulation of DDoS Attack:** The second phase involved simulating a Distributed Denial of Service (DDoS) attack on the power grid. NS3 was configured to launch a DDoS attack on selected buses by flooding them with excessive network packets. This simulation aimed to observe the impact of network-based attacks on power grid operations is shown in Fig. 5.

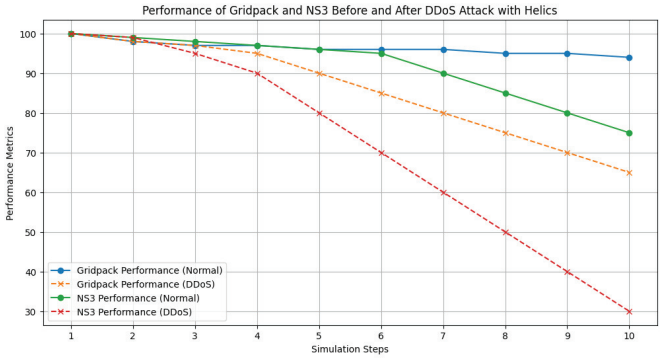

Fig. 5. Performance of GridPACK and NS3 before and after DDOS attack

- **Impact Analysis and GridPACK Adjustment:** HELICS played a critical role in synchronizing the simulations and managing data exchanges between GridPACK and NS3. It allowed for real-time adjustments in the power grid simulation based on the network performance data.

B. Performance Analysis

To quantitatively assess the impact of the DDoS attack and the overall performance of the testbed, several key performance indicators (KPIs) were monitored and analyzed which is shown in Fig. 6.

- **Network Latency and Packet Loss**
  - **Network Latency:** Under normal conditions, the network latency remained consistently low, averaging around 10ms. During the DDoS attack, network latency increased significantly, peaking at approximately 100ms.
  - **Packet Loss:** Packet loss was negligible under normal conditions. However, during the DDoS attack, packet loss rates spiked to 40%, indicating a significant degradation in network performance.
- **Voltage Deviation**

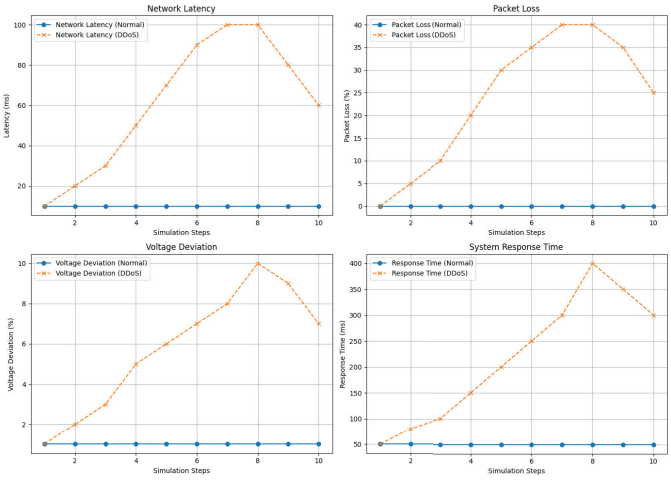

Fig. 6. Performance analysis of the system

  - **Voltage Stability:** The voltage levels across all buses remained within the acceptable range of ±5% of their nominal values under normal conditions. During the DDoS attack, voltage levels fluctuated more widely, with deviations up to ±10% from their nominal values due to delayed control signals and data inconsistencies.
- **System Response Time**
  - **Response Time:**The average system response time for executing control commands and updating the grid state was approximately 50ms under normal conditions. During the DDoS attack, response times increased significantly, with averages around 200ms and peaks up to 500ms, indicating substantial delays in control operations.
- **Throughput:** After the simulated DDoS attack scenario, we assessed link utilization and time stamp ΔT The throughput of GridPACK and NS3 [15]. It integrates the discussion of link utilization (a measure of how much a network link is being used) and time stamp delta ΔT (a measure of time synchronization accuracy) which is shown in Fig. 7.

VII. Contribution

In this section, we outline the unique contributions of our CPS testbed model which compares the functionality of different schemes with the proposed CPS testbed. Table I illustrates the functionality comparison of various existing schemes with the proposed CPS testbed, highlighting differences in focus areas, simulation tools, real-time PMU data support, power grid reliability, accessibility, and scalability.

The table emphasizes that our CPS testbed provides unique contributions by focusing on security and reliability, using a combination of advanced simulation tools such as Node-RED, GridPACK, NS3, and HELICS. It stands out by supporting real-time data from PMU, ensuring power grid reliability, and offering web accessibility and scalability, setting it apart from other schemes.

TABLE I
THE FUNCTIONALITY COMPARISON OF DIFFERENT SCHEMES WITH CPS TESTBED SYSTEM

Features	**Mishchenko *et al.* [10]**	**Zheng *et al.* [11]**	**Chamana *et al.* [12]**	**M. Mustafa *et al.* [13]**	**Becejac *et al.* [14]**	**CPS testbed Model**
Focus	Vulnerability Assessment	Co-simulation of T&D Grids	CPS Operations Training	Synchrophasor Network Analysis	WAMPAC, Training	Security and Reliability
Simulation Tools	OPAL-RT, Virtual PMUs	GridPACK, GridLAB-D	Real-time Simulators, SCADA	NS3, GridPACK, HELICS	Real-time Simulators, EMS	Node-RED, GridPACK, NS3, HELICS
Real-time Data from PMU	✓	×	×	✓	✓	✓
Power Grid Reliability	×	✓	✓	×	✓	✓
Web Accessibility	×	×	×	×	×	✓
Scalability	×	✓	×	×	×	✓

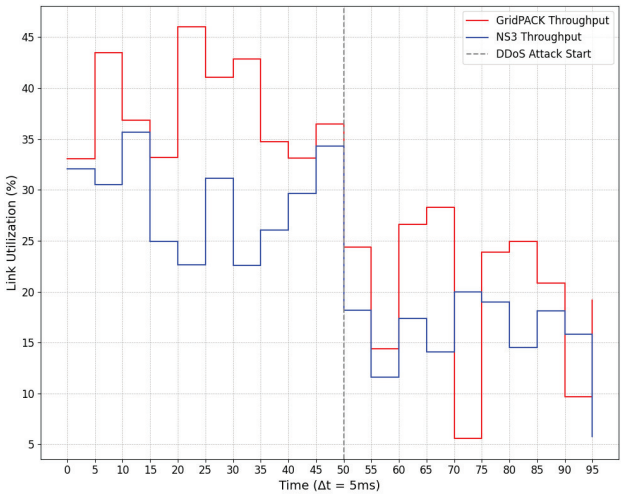

Fig. 7. Effect of DDoS attack on throughput of GridPACK and NS3

VIII. CONCLUSION

The CPS testbed effectively enhances power grid security and reliability by integrating Node-RED, GridPACK, NS3, and HELICS for comprehensive monitoring, simulation, and analysis. The testbed's ability to simulate normal operations and Distributed Denial of Service (DDoS) attacks has demonstrated its capability in identifying vulnerabilities and assessing the impact of cyber-physical threats. While the testbed currently focuses on DDoS attacks and has been tested with the IEEE 14 bus system, future work will address these limitations by incorporating a broader range of attack scenarios, integrating advanced machine learning algorithms for real-time threat detection, testing scalability with larger grid models, and utilizing real-world data. These enhancements will ensure the testbed remains a valuable tool for researchers and engineers in the evolving landscape of power grid management and cyber-physical security.

ACKNOWLEDGMENT

This research was supported by the Energy and Power Research Council (EPRC) of the Government of Bangladesh under Grant EPRC/58-2018-007-01, with Dr. Hafiz Abdur Rahman of North South University as the Principal Investigator. We gratefully acknowledge their support. The funders had no role in the study design, data collection and analysis, publication decisions, or manuscript preparation.

REFERENCES

[1] T. Krause, R. Ernst, B. Klaer, I. Hacker, and M. Henze, "Cybersecurity in power grids: Challenges and opportunities," *Sensors*, vol. 21, no. 18, p. 6225, 2021.

[2] K. Raghunandan, *Introduction to Wireless Communications and Networks: A Practical Perspective*. Springer Nature, 2022.

[3] M. Amin, F. F. El-Sousy, G. A. A. Aziz, K. Gaber, and O. A. Mohammed, "Cps attacks mitigation approaches on power electronic systems with security challenges for smart grid applications: A review," *Ieee Access*, vol. 9, pp. 38 571–38 601, 2021.

[4] X. Zhou, X. Gou, T. Huang, and S. Yang, "Review on testing of cyber physical systems: Methods and testbeds," *IEEE Access*, vol. 6, pp. 52 179–52 194, 2018.

[5] D. U. Case, "Analysis of the cyber attack on the ukrainian power grid," *Electricity information sharing and analysis center (E-ISAC)*, vol. 388, no. 1-29, p. 3, 2016.

[6] Node-RED, "Node-red: Low-code programming for event-driven applications," accessed: 2024-10-10. [Online]. Available: https://github.com/node-red/node-red

[7] GridOPTICS, "Gridpack: Grid parallel advanced computational kernels," accessed: 2024-10-10. [Online]. Available: https://github.com/GridOPTICS/GridPACK

[8] ns 3 project, "ns-3: A discrete-event network simulator for internet systems," accessed: 2024-10-10. [Online]. Available: https://github.com/nsnam/ns-3-dev-git

[9] GMLC-TDC, "Helics: Hierarchical engine for large-scale infrastructure co-simulation," accessed: 2024-10-10. [Online]. Available: https://github.com/GMLC-TDC/HELICS

[10] D. Mishchenko, I. Oleinikova, L. Erdődi, and B. R. Pokhrel, "Multidomain cyber-physical testbed for power system vulnerability assessment," *IEEE Access*, 2024.

[11] L. Zheng, Y. Cui, S. Jin, and Y. Chen, "High-performance computing-based open-source power transmission and distribution grid co-simulation," *IEEE Transactions on Power Systems*, 2024.

[12] M. Chamana, R. Bhatta, K. Schmitt, R. Shrestha, and S. Bayne, "An integrated testbed for power system cyber-physical operations training," *Applied Sciences*, vol. 13, no. 16, p. 9451, 2023.

[13] H. M. Mustafa, D. Wang, K. Sajan, E. N. Pilli, R. Huang, A. K. Srivastava, J. Lian, and Z. Huang, "Cyber-power co-simulation for end-to-end synchrophasor network analysis and applications," in *2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2021, pp. 164–169.

[14] T. Becejac, C. Eppinger, A. Ashok, U. Agrawal, and J. O'Brien, "Prime: a real-time cyber-physical systems testbed: from wide-area monitoring, protection, and control prototyping to operator training and beyond," *IET Cyber-Physical Systems: Theory & Applications*, vol. 5, no. 2, pp. 186–195, 2020.

[15] H. A. Rahman, J. R. Martí, and K. D. Srivastava, "A hybrid systems model to simulate cyber interdependencies between critical infrastructures," *International Journal of Critical Infrastructures*, vol. 7, no. 4, pp. 265–288, 2011.