frontiers | Frontiers in Energy Research

TYPE Original Research
PUBLISHED 31 July 2024
DOI 10.3389/fenrg.2024.1402566

OPEN ACCESS

EDITED BY
Yingjun Wu,
Hohai University, China

REVIEWED BY
Yuanshi Zhang,
Southeast University, China
Jianfeng Dai,
Nanjing University of Posts and Telecommunications, China
Jintao Han,
Opal-Rt Technologies, Canada
Neeraj Kumar Singh,
HCL Technologies, India

*CORRESPONDENCE
Xiaoke Wang,
xiaokewang2024@163.com

RECEIVED 17 March 2024
ACCEPTED 12 June 2024
PUBLISHED 31 July 2024

CITATION
Wang X, Ji Y, Sun Z, Liu C and Jing Z (2024), Improving cyber-physical-power system stability through hardware-in-loop co-simulation platform for real-time cyber attack analysis.
Front. Energy Res. 12:1402566.
doi: 10.3389/fenrg.2024.1402566

Improving cyber-physical-power system stability through hardware-in-loop co-simulation platform for real-time cyber attack analysis

Xiaoke Wang*, Yan Ji, Zhongwang Sun, Chong Liu and Zhichun Jing

Jiangsu Donggang Energy Investment Co., Ltd., Lianyun Gang, Jiangsu, China

With advancements in communication systems and measurement technologies, smart grids have become more observable and controllable, evolving into cyber-physical-power systems (CPPS). The impact of network security and secondary equipment on power system stability has become more evident. To support the existing grid toward a smart grid scenario, smart metering plays a vital role at the customer end side. Cyber-Physical systems are vulnerable to cyber-attacks and various techniques have been evolved to detect a cyber attack in the smart grid. Weighted trust-based models are suggested as one of the most effective security mechanisms. A hardware-in-loop CPPS co-simulation platform is established to facilitate the theoretical study of CPPS and the formulation of grid operation strategies. This paper examines current co-simulation platform schemes and highlights the necessity for a real-time hard-ware-in-the-loop platform to accurately simulate cyber-attack processes. This consideration takes into account the fundamental differences in modeling between power and communication systems. The architecture of the co-simulation platform based on RT-LAB and OPNET is described, including detailed modeling of the power system, communication system, and security and stability control devices. Additionally, an analysis of the latency of the co-simulation is provided. The paper focuses on modeling and implementing methods for addressing DDOS attacks and man-in-the-middle at-tacks in the communication network. The results from simulating a 7-bus system show the effectiveness and rationality of the co-simulation platform that has been designed.

KEYWORDS

active distribution networks, CPPs, smart grid, hardware-in-loop, cyber-attack, co-simulation

1 Introduction

With the development of the economy and society, the demand for energy is increasing. Traditional thermal power generation is unable to meet the electricity demand, and environmental issues such as greenhouse gas emissions are becoming more prominent. Guided by the national goal of reaching peak carbon emissions and achieving carbon neutrality, the integration and adoption of new energy sources have become an inevitable

trend in energy development. The development and utilization of distributed energy provide an important approach for adjusting and upgrading China's energy structure.

Distributed energy is a user-side energy supply method that can operate independently or be connected to the grid. It maximizes resource and environmental benefits and determines the method and capacity based on them. It represents an important direction for the future development of global energy technology. Compared to traditional power sources, distributed power sources have unique advantages including cost-effectiveness, environmental friendliness, and flexibility. They are usually located on the user side, which reduces the construction cost of transmission and distribution networks, minimizes energy loss, and has a short construction cycle and quick return on investment. Additionally, they are technologically advanced, flexible, and easy to maintain, allowing for rapid start-up and shutdown. They can also smooth out peak loads, providing great flexibility. With the integration of a large number of distributed power sources, the safe, reliable, and stable operation of the distribution network is influenced by multiple uncertain factors, primarily manifested in terms of voltage at network nodes, flow direction, fault current in lines, and system protection. The randomness and intermittency of distributed power sources exacerbate issues such as node voltage deviation, severe load fluctuations, and increased network losses in the distribution system, thereby potentially leading to a series of problems including deteriorated power quality, equipment overload, reverse power flow, and excessive terminal voltage (Zhang et al., 2020a; Zhang et al., 2021; Nguyen et al., 2022).

Cyber-Physical systems are vulnerable to cyber-attacks. Various techniques have been evolved to detect a cyber attack in the smart grid (Singh N K et al., 2020). With massive data transmission on the CEEO network, the trustworthiness of the service node exerts an enormous influence on data privacy. To realize securely share data and decrease the local storage, end-user prefer to encrypt data and upload it to the cloud (Fan et al., 2021). Integration of renewable resources and increased growth in energy consumption has created new challenges for the traditional electrical network. To adhere to these challenges, Internet of Everything (IoE) has transformed the existing power grid into a modernized electrical network called Smart Grid (Desai et al., 2019).

Active distribution networks (ADNs) serve as networks for energy exchange and distribution, facilitating the bidirectional flow of both power and fault currents. Traditional power distribution networks are no longer adequate for flow and fault analysis, reactive power control, relay protection methods, and operational management. They require corresponding adjustments and improvements. Referred to as active distribution networks (ADNs), the focus is on distributed energy resources actively regulating their reactive and active outputs and utilizing modern communication means for coordinated control over the distribution network. This enables the full optimization of network operations by harnessing the potential of distributed energy resources (Zhang et al., 2020b; Cao et al., 2023; Cao et al., 2024).

The key technologies of ADNs include ADN planning, flow and fault analysis computations, relay protection, reactive power control techniques, and operational scheduling of distributed energy resources (Jabr, 2013). For example, efficient demand-side management tools allow operators to have better control over the operation and management of distributed energy resources. Additionally, integrating energy storage facilities helps absorb excess output or mitigate load fluctuations from distributed energy resources.

The ongoing advancements in power electronics technology are enabling various control and regulatory equipment to better serve active distribution networks. This enhancement facilitates the utilization of new energy generation within distribution networks while ensuring safety and stability. Zhao and You (2021) introduces a multi-level adaptive robust optimization framework based on deep learning to tackle uncertainties arising from the high penetration of distributed energy sources into distribution networks. Moreover, adaptive optimization control methods, relying on real-time measurement data, effectively model the input-output relationship of the distribution network using live measurements.

Through iterative interactions with the distribution network, these methods effectively overcome the reliance on extensive training associated with neural network methods, thereby enabling real-time control of the distribution network (Hou and Xu, 2009; Zhang et al., 2022). Zhao et al. (2016) utilizes a controller comprising three modules—voltage regulation, reactive power control, and active-frequency regulation—that adapt locally without the need for frequency measurements. Guo et al. (2019) proposes an optimization control frame-work for interconnected AC-DC microgrids based on model-free adaptive control, effectively addressing issues of AC-DC coordinated power control. Addressing the time-series characteristics of controlled systems, Zhang et al. (2021) integrates predictive control principles into model-free adaptive control, achieving superior control performance through adaptive predictive control. Bi et al. (20223) introduces a data-physical fusion-driven adaptive voltage control method for active distribution networks, effectively curbing frequent voltage excursions and enhancing the adaptive optimization control level of the distribution network. In the smart grid substation each wireless sensor node can be modeled using graph theory. Then each node is assigned with predefined weight, which gets effected during cyber intrusion. Each sensor node monitors the trust value of neighboring nodes (Singh et al., 2020). Cyber-Physical systems are vulnerable to cyber-attacks. Various techniques have been evolved to detect a cyber attack in the smart grid. Weighted trust-based models are suggested as one of the most effective security mechanisms. A two-level hierarchical network is examined, with the smart wireless sensors at the bottom and server at the top of the network. The direct and indirect trust of the node is calculated using "One Time Code" to determine the overall trust of nodes. Trust depends on the performance of the sensors, communication between sensors, and the server of the nodes. It also depends on the previous communication between the nodes (Singh and Mahajan 2020). As a cyber-embedded infrastructure, it must be capable of detecting cyberattacks and responding appropriately in a timely and effective manner. Previous work tries to introduce an advanced and unique intrusion detection model capable of classifying binary-class, trinary-class, and multiple-class CDs and electrical network incidents for smart grids. It makes use of the gray wolf algorithm (GWA) for evolving training of artificial neural networks (ANNs) as a successful machine learning model for intrusion detection (Yu et al., 2022). The intrusion detection model is based on a whale optimization algorithm (WOA)-trained artificial neural network

(ANN). The WOA is applied to initialize and adjust the weight vector of the ANN to achieve the minimum mean square error (Haghnegahdar and Wang, 2020).

The impact of network security and secondary equipment on power system stability has become increasingly evident, emphasizing the urgent need for advanced simulation tools that can effectively model and mitigate these threats. To bridge this critical gap, a hardware-in-loop CPPS co-simulation platform is established to facilitate the theoretical study of CPPS and the formulation of grid operation strategies. A sophisticated HIL simulation environment is proposed in Riquelme-Dominguez et al. (2023), that addresses system frequency responses in power systems with low inertia. This aligns closely with our focus, demonstrating the importance of accurate real-time simulations under both normal and emergency conditions. The cybersecurity challenges in modern power systems are further emphasizes in Fu et al. (2023), which highlights the need for HIL simulations that not only handle physical system dynamics but also integrate cybersecurity threat scenarios. The method of virtualized environments complement HIL simulations is analyzed in Zhang et al. (2021), particularly in applying machine learning techniques for anomaly detection. This study supports our method of incorporating machine learning to enhance the predictive capabilities of our co-simulation platform. Specialized applications of HIL simulations for maritime control systems are described in Vu et al. (2023), highlighting the versatility and critical need for robust HIL environments across different sectors, including the specific challenges posed by cyber-physical threats. This paper examines current co-simulation platform schemes and highlights the necessity for a real-time hardware-in-the-loop platform to accurately simulate cyber-attack processes, considering the fundamental differences in modeling between power and communication systems. An independent, distributed, and lightweight trust evaluation model is proposed and evaluated. The trust model is implemented at two levels: first at the smart meter level, where nodes collect information on its neighbor nodes and forward it to the collecting node (Alnasser and Rikli, 2014). In previous work a Hierarchical Trust based Intrusion detection System (HTBID) has been proposed to effectively deal with various attacks in wireless sensor network. HTBID deals with different types of attack with the help of Hierarchical Trust evaluation protocol (HTEP). This work identifies different parameters and factors that affect trust of wireless sensor network. HTEP considers attributes derived from communication as well as social trust to calculate the overall trust of sensor node (Dhakne and Chatur, 2017).

The co-simulation platform based on RT-LAB and OPNET is proposed, including detailed modeling of the power system, communication system, and security and stability control devices. Our approach significantly advances the state of the art by enabling more precise and dynamic responses to cybersecurity threats within CPPS environments. Our solution leverages cutting-edge advancements in real-time simulation technology and cyber-attack modeling to provide a comprehensive tool for power system operators. This enables the proactive identification of vulnerabilities and the testing of countermeasures under controlled yet realistic conditions, which was not feasible with previous methodologies. This paper focuses on modeling and implementing methods for addressing DDOS attacks and man-in-the-middle attacks in the communication network. The results from simulating a 7-bus system show the superiority and practicality of the co-simulation platform that has been designed.

2 Co-simulation platform framework and design

2.1 Platform framework

Advanced sensors and high-speed networks have enabled real-time monitoring of power grids, providing data on various electrical measurements such as voltage, current, and frequency, as well as environmental information like temperature, humidity, and light (Luo, 2016; Zhang et al., 2021; Mittal et al., 2023). This data is utilized to support grid monitoring, protection, regulation, and other functions.

The smart grid control system in CPPS consists of three main components: the power system as dipicted in Figure 1 (including generators, loads, power electronic equipment, energy storage systems, measuring units, and control units), the communication system (comprising routers, optical fibers, servers, and other devices), and the security and stability control device (a decision-making system with a master station and substation).

Measuring units collect data on the grid's status and transmit it to the master station via a wide-area communication network (Osanaiye et al., 2016; Zhang et al., 2020c). The master station calculates control commands based on a strategy and sends them to each substation. Substations then execute specific operations using control units based on local control strategies (Othman et al., 2018; Menezes et al., 2023).

This paper utilizes a modular design to integrate discrete event simulation and continuous-time simulation. The co-simulation platform comprises four modules: power system, communication system, master station, and substation. These modules are connected via Ethernet to streamline data interface design and enhance modeling efficiency. Real-time performance is ensured through the use of appropriate simulation tools for the power system and communication system. Figure 2 illustrates the architecture of the co-simulation platform.

2.2 Power system

The real-time requirements of the co-simulation platform present a challenge, as most power simulation systems are PC-based and cannot handle large-scale simulations in real-time with small time steps (Zhang et al., 2024). To tackle this problem, the OPAL-RT modeling software RT-LAB was chosen as the power system simulator (Amaizu et al., 2021). Simulink models can be compiled into multiple subroutines that can be executed in parallel using RT-LAB.

Modeling in RT-LAB involves four main components: the power grid, a measuring unit, a control unit, and a network interface (Cil et al., 2021), as shown in Figure 1. The original power grid is simplified into an equivalent network for real-time simulation, and the grid model is designed accordingly and verified through offline simulations (Mittal et al., 2023). Regarding the

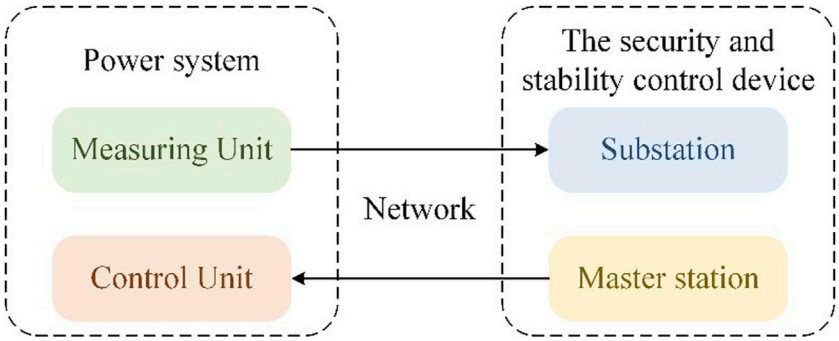

FIGURE 1
The structure of smart grid control system.

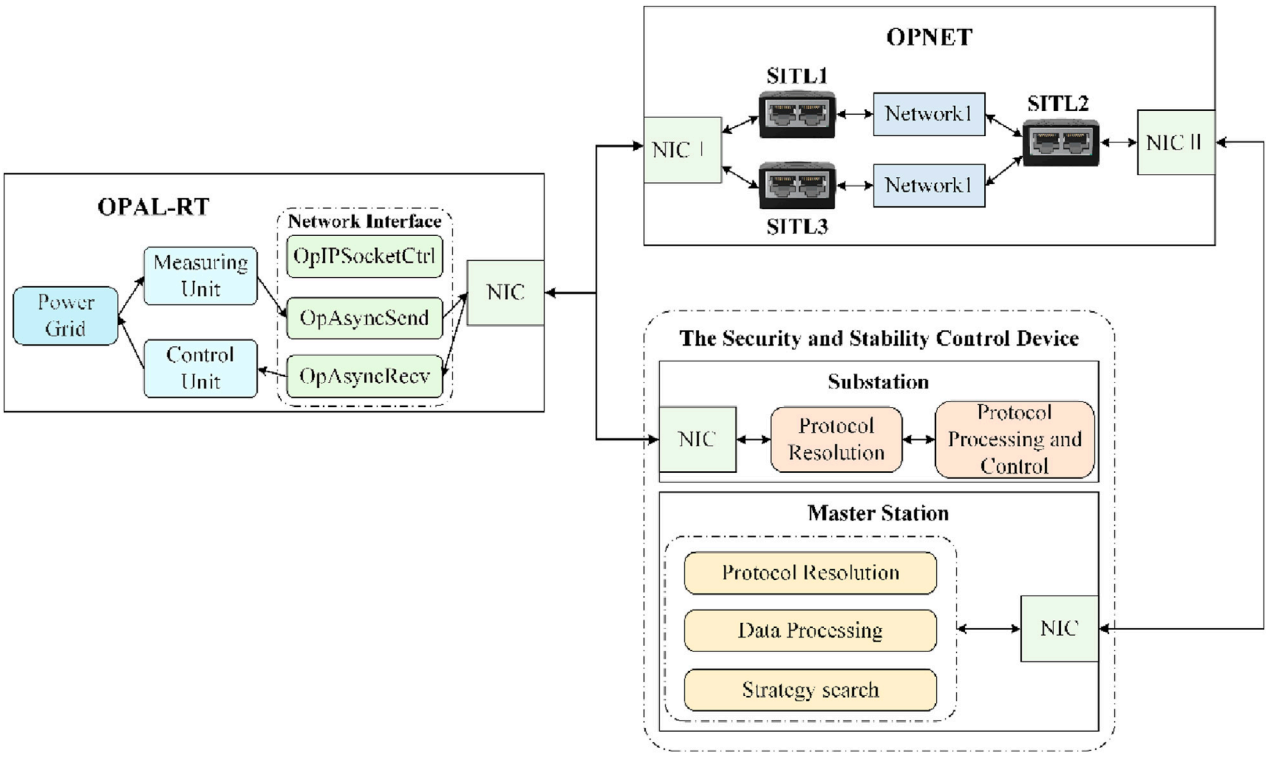

FIGURE 2
The architecture of co-simulation platform.

measuring unit, it is essential to define the sampling frequency and data type of the packets, which include parameters such as voltage, current, frequency, and power-angle (Alnasser and Sun, 2017; Singh and Mahajan, 2020; Singh and Mahajan, 2021; Yu et al., 2022; Zhang et al., 2021a; Zhang et al., 2021b; Zhang et al., 2021c). Additionally, timestamps are included to analyze latency. In the control unit, it is crucial to determine the target and structure of commands sent from the substation. The control unit is responsible for converting these commands into control quantities and outputting them to the control target. OPAL-RT uses TCP and UDP protocols for external communication. The network interface consists of three modules: OpIPSocketCtrl, which controls the communication protocol, port, and IP address; OpAsyncRecv, for receiving packets; and OpAsyncSend, for sending packets. Multiple sets of network interfaces can be included in the power system model, distinguished by port numbers.

2.3 Communication system

To ensure real-time performance, this paper utilizes OPNET to simulate the communication system. The modeling in OPNET is categorized into three layers: net-work, node, and process, depending on the level of the communication network. This

three-level modeling allows for the construction of communication networks, protocols, algorithms, and equipment. OPNET also offers a range of standard applications, such as Database, E-mail, HTTP, Print, Remote Login, Video Conferencing, and Voice, which can be combined to cover most power services (Kaur et al., 2021; Zhang et al., 2023). For unique power businesses, the standard application model can be modified at the process layer to create a customized application model.

To establish end-to-end business connections between real and virtual networks, a semi-physical simulation interface can be employed (Priyadarshini and Barik, 2022). OPNET offers three types of such interfaces: HLA-API, ESA-API, and System in the loop (SITL). While HLA-API and ESA-API require defining process and node models and designing corresponding interface programs, SITL is an existing model provided by OPNET. Although it supports limited protocols and requires mapping real packets to virtual ones, it enables easy access to external devices in the simulation system. As communication between modules uses the UDP protocol, we have chosen SITL as the data interface to simplify model design.

Data is exchanged between measuring units and substations with the master station through a communication system. Control units exchange data with substations directly through a switch. To facilitate this, two network interface cards (NICs) are inserted into the OPNET host. NIC1 communicates with the OPAL-RT and substation via the switch, while NIC2 communicates directly with the master station. The network model includes multiple SITL modules that correspond to the master station, substation, and measuring units by setting filters. Network 1 connects measuring units to the master station, while network 2 connects the substation to the master station.

2.4 The security and stability control device

The security and stability control device plays a crucial role as the second and third lines of defense for the power grid. It is responsible for responding to emergencies such as load shedding, generator trips, or valve fast shutdowns in order to prevent further spread of faults in the grid. This device consists of both a master station and substations. The master station monitors the power grid's status through measuring units and compares any faults found with the security control strategy based on the fault type and location. Once the optimal control strategy is determined, the master station sends control commands to the substations. The substations report the controllable load amount to the master station and receive control commands from it. Finally, the substations send commands to the control units and execute the actual operation according to the local control strategy.

The master station is constructed on the Linux platform and is programmed using the C language, allowing it to perform complex operations. It retrieves real-time power grid status information from OPAL_RT and receives control commands from the security and stability control device to efficiently monitor and manage the power system. The master station consists of four modules, which are as follows:

2.4.1 Protocol analysis module

The protocol analysis module is responsible for examining packets sent by the measuring unit and the substation. Each packet consists of a padding section and a data section. The data section includes a header, a command code, and a checksum. Upon receiving a packet, the master station extracts the data section using a preset offset and verifies its accuracy. Then, the header is read to identify the message type and source, and subsequently, the corresponding operation is executed based on the command code. I have improved the grammar, added transitional phrases, and simplified certain words and phrases for better clarity without altering their original meaning.

2.4.2 Grid status database

The purpose of this module is to store up-to-date information on the power grid's status, including the status of breakers, positions of transformer taps, as well as voltage and frequency levels.

2.4.3 Fault detection module

This module is triggered whenever there is an update to the grid status in the database, and it sends an alarm in case of system failure.

2.4.4 Control module

Upon receiving an alarm from the fault detection module, the control module formulates multiple coordinated control strategies according to the pre-established plan. It assesses their effectiveness and determines the optimal scheme to create a control queue for the substation.

The master station operates in parallel and dynamically assigns individual processes to each client. The client's type can be automatically identified by the master station based on the self-descriptive packet. There are four types of commands: retrieving grid status from the database, updating grid status in the database, accessing control commands in the control queue, and adding control commands to the control queue. The master station can synchronize, analyze, and manage the power system, communication system, and substation.

This paper presents a substation that utilizes embedded Linux and comprises five components, as depicted in Figure 3: a control module, an input/output (I/O) module, a measuring module, a man-machine interface, and a communication module. The substation communicates with the master station every 0.833 ms. During a control cycle, the substation performs four steps:

Initially, the substation dispatches a packet that includes the controllable load quantity to the master station and then awaits the response packet.

After receiving the packet from the master station, the substation identifies its type by analyzing the packet header.

The substation performs different actions depending on the type of packet received. For synchronization packets, it revises the system clock. For command packets, it generates a control queue based on the local control strategy. If an abnormal packet is received, it is returned to the master station. If the control queue is not empty, all commands will be sent to the control unit.

2.5 System latency

Figure 4 illustrates the real-time simulation timeline of a co-simulation platform that includes a power system, communication

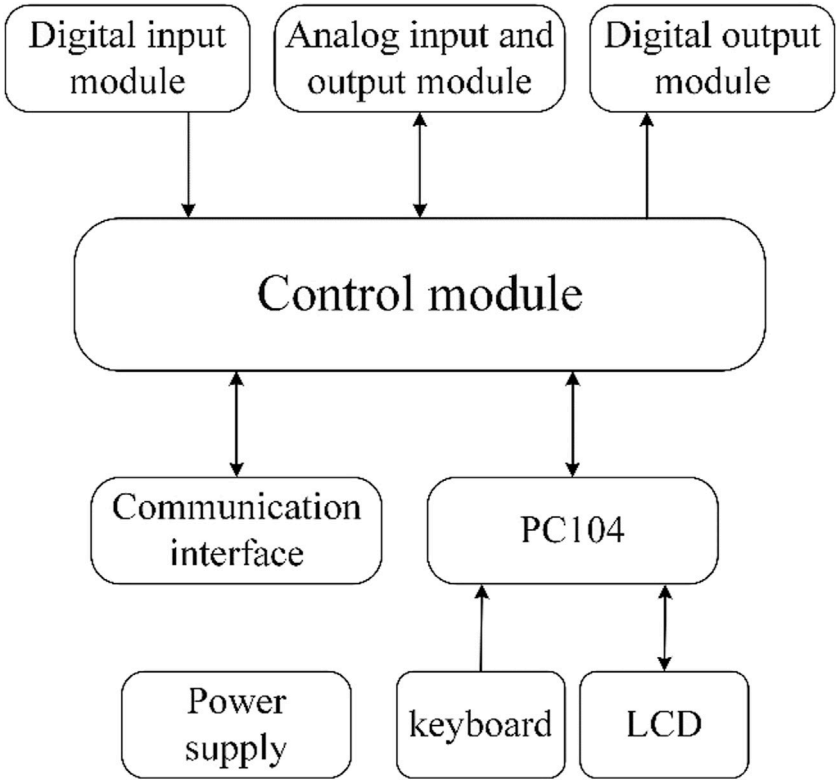

FIGURE 3
Structure of substation.

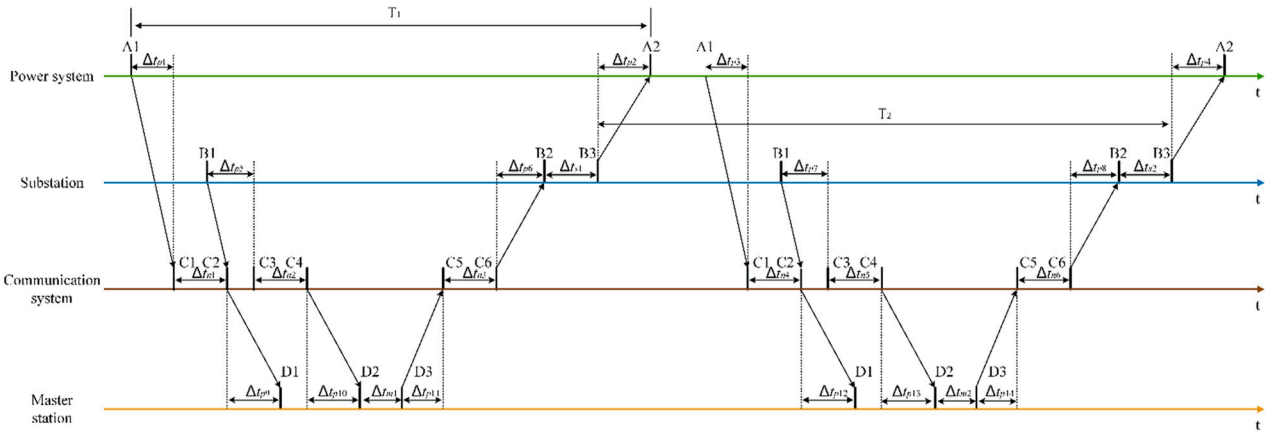

FIGURE 4
Timeline of real-time simulation.

system, master station, and substation. This timeline considers the simplified structure of the control system in the power grid.

To simplify the modeling process and clarify the function of each module, the measuring unit is limited to sending data only, while the control unit can only receive data. The communication cycle between the measuring unit and the master station is T_1, and the cycle between the control unit and the substation is T_2. At moment A1 in the simulation, the measuring unit sends sampled data to the master station, which receives the data at D1. At moment B1, the substation system sends the data of controllable load to the master station. After processing the data upon receiving them at D2, the master station issues a synchronization message or control order message to the substation. The substation analyzes the message and issues a control order to the control unit at B3. Finally, the control unit updates the relevant parameters in the power system node at A2.

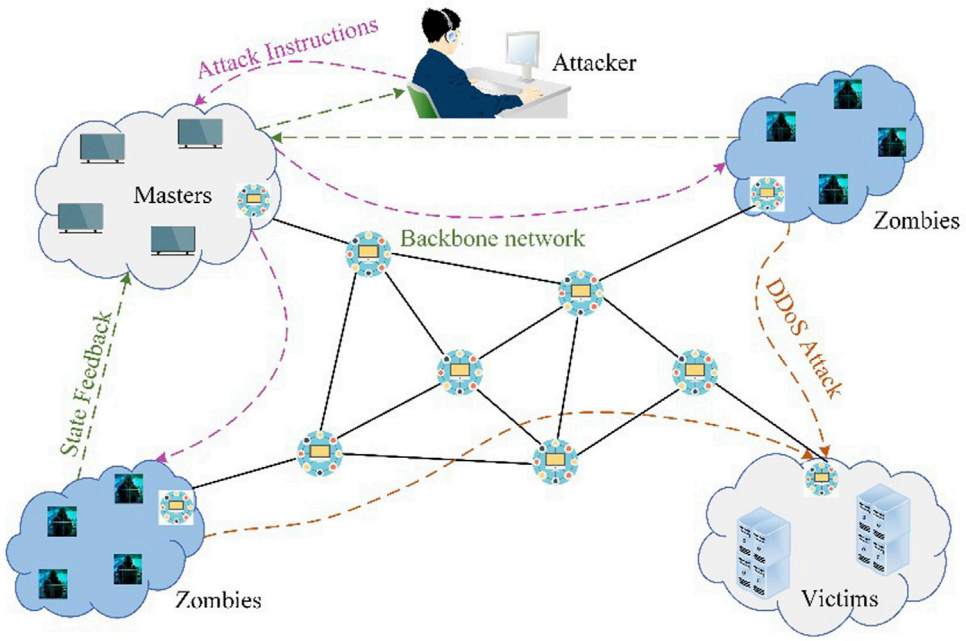

FIGURE 5
Attack steps of DDOS.

The system latency consists of four main components: network latency, master station latency, substation latency, and inherent simulation platform latency. Network latency is the delay caused by communication systems, including issues such as packet loss, bit errors, routing problems, bandwidth limitations, and server performance. Master station latency is a result of hardware and software limitations, encompassing hardware latency and software latency. Hardware latency involves delays within the master station system, including network card performance and data transfer. Software latency refers to the time required for power service computations, such as state estimation, measurement information management, and power quality monitoring. Substation latency is similar to master station latency, involving hardware and software limitations that lead to delays. Inherent simulation platform latency arises from communication between modules in the platform. This includes factors like OPAL-RT operating system latency, OPAL-RT network card latency, OPNET operating system latency, OPNET host network card latency, switch latency, and more.

In actual CPPS, the platform's inherent latency cannot be eliminated and varies randomly depending on the amount of data flow between modules. When data packets are less than 64 bytes, the inherent latency is approximately 1–2 ms. However, as the total latency of network, master station, and substation is already in the range of tens to hundreds of milliseconds, the impact of inherent latency is negligible and will not significantly affect the simulation accuracy. To further minimize the influence of inherent latency, one common approach is to use the Ping command to measure the communication latency between modules, record it as inherent latency, and subtract it from the controllable latency in the master station system.

3 Cyber-attack modeling

3.1 DDOS attack

A Distributed Denial of Service (DDOS) attack is a form of resource-exhaustion attack. Attackers employ Client/Server techniques to manipulate multiple computers as sources of attack, thereby enhancing the attack's effectiveness. There are various types of DDOS attacks, including Sy flood, Smurf, and Land-based attacks. When a host is targeted by a DDOS attack, it experiences a high volume of pending connections, causing the network to be flooded with useless packets, leading to network congestion. Consequently, the target of the attack becomes incapable of communicating with the outside world.

Figure 5 illustrates the DDOS attack scheme, consisting of four components: the attacker, control puppet, attack puppet, and target. Attackers gain either partial or complete control of both the control puppet and attack puppet. The control puppet transmits the attack program to the attack puppet. Through the control puppet, the attacker instructs the attack puppet to send actual attack packets to the target.

This paper deploys an attacker node in an OPNET simulation. The attacker randomly scans and attacks all terminals in phase one, and infected computers send confirmations back to the attacker. In phase two, the infected computers flood the network connecting to the target with tons of meaningless packets.

3.2 MITM attack

The Man in the Middle (MITM) attack is an indirect method of gaining control over a target. By spoofing IP addresses and ports, the

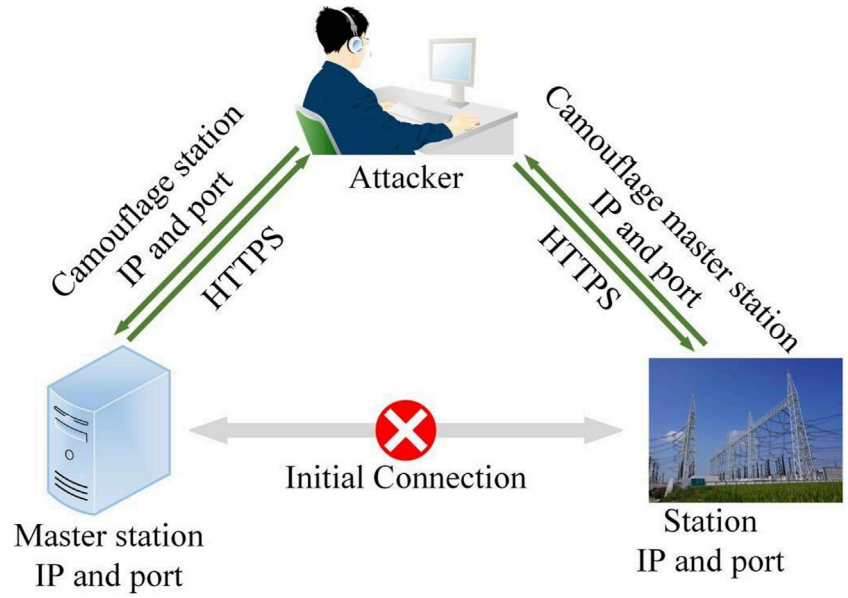

FIGURE 6
Man-in-the-middle attack.

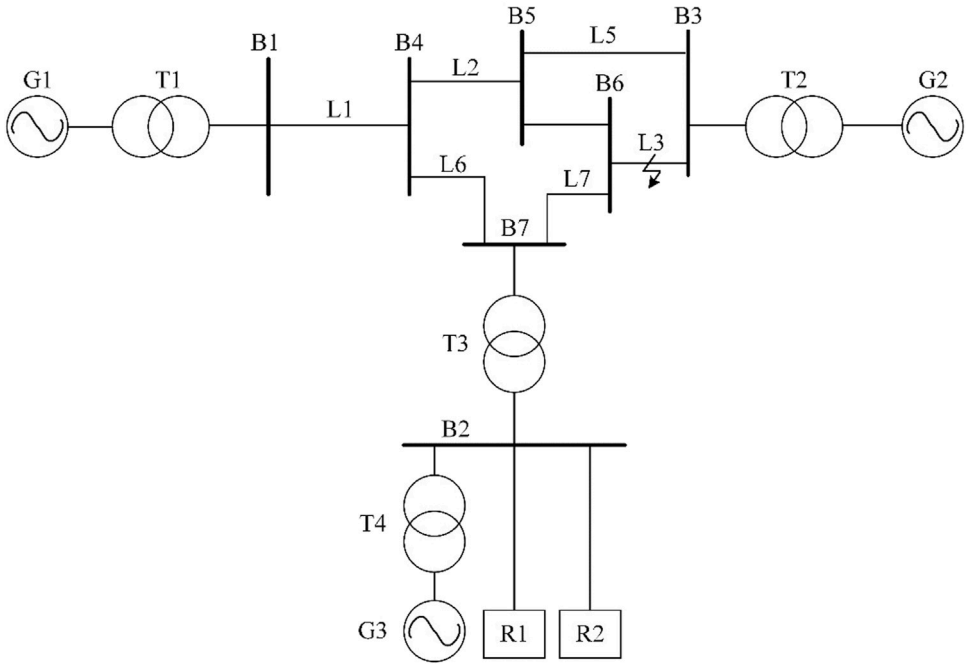

FIGURE 7
Structure of 7-bus system.

attacker can invade and take control of a virtual computer, creating a new communication channel between the original nodes. This new channel allows packets to be easily modified, leading the target to make incorrect decisions. Common examples of MITM attacks include Careto, Crypto locker, Dexter, and Fin Fisher.

In the research depicted in Figure 6, a computer is utilized as the attacker and equipped with two network interface cards (NICs). One NIC connects to OPNET while the other connects to the substation. The IP address of the NIC connected to the substation serves as the gateway IP address for the substation, while a virtual NIC is established within the computer and assigned the IP of the

TABLE 1 Parameters of the device.

Bus number	Device number	Device type	Voltage (kV)	Capacity
B1	G1	Generator	13.8	100MVA
	T1	Transformer	13.8/218.5	100MVA
B2	G3	Generator	13.8	100MVA
	T4	Transformer	13.8/110	100MVA
	R1	Controllable load	110	80MVA
	R2	Controllable load	110	40MVA
B3	G2	Ideal voltage source	13.8	∞
	T2	data	13.8/218.5	100MVA
B7	T3	data	110/230	100MVA

master station. The IP address of the NIC connected to the substation is configured as the substation's IP address.

Two methods of Man-in-the-Middle (MITM) attack are proposed as follows:

3.2.1 Data interception

In this method, the attacker intercepts packets from both the substation and master station, analyzes the packet header to determine its function, and copies any time packets to a buffer which is then sent to the substation. If a command packet is detected, it will be replaced by the time packet in the buffer. This attack prevents the substation from receiving commands from the master station.

3.2.2 Data modification

Similarly, in this method, once a command packet is detected, all subsequent packets will be replaced by a modified command packet that forces the substation to execute unreasonable load shedding and casting actions.

4 Case study

4.1 Model description

To verify the impact of communication systems and devices on power system simulations, as well as the necessity of co-simulation platforms in power system analysis, a 7-bus system was constructed in RT-Lab, as shown in Figure 7. The system includes seven buses, two controllable loads, two generators, one ideal voltage source, four transformers, and seventeen circuit breakers. Measuring units monitor buses B1, B2, and B3. The protection unit and control unit jointly manage the controllable load and generator, with the protection unit preventing the control unit from operating the protected device once it has been broken out. The simulation is based on a reference AC voltage of 230 kV, frequency of 60 Hz, and a simulation step of h = 2.5 × 10^(−5) s. Table 1 provides the parameters for each device.

The strategy for system protection and security control during a three-phase short-circuit fault on transmission line L3 is as follows: The short-circuit protection unit will disconnect L3 within 0.1 s of the fault occurring. The over-current protection unit will disconnect L1 after a 2-second delay and disconnect L5 after a 3.5-second delay from the occurrence of the fault. Additionally, the security and stability control device will disconnect R2 after a 2-second delay following the short-circuit fault.

Figure 8 illustrates the communication network constructed in OPNET, which comprises eight router nodes, multiple servers, and terminals designed to simulate data transmission across various services. Notably, the measuring unit, master station, and substation do not directly correspond to individual nodes within this network. Instead, these physical components are interconnected to the OPNET communication network at specific boundary nodes using the SITL (System-in-the-Loop) module. This setup reflects the hierarchical nature of our system, where multiple physical devices may connect to a single communication node that serves as a gateway or aggregation point, rather than having a direct one-to-one mapping with the communication nodes.

Furthermore, the control unit is integrated into the network via a connection to the substation through a switch, emphasizing the layered interaction between control operations and network communication. The routers in this network are linked by a 2 Mbps optical fiber, ensuring a consistent communication delay of 1 ms across the system.

After the occurrence of a three-phase short-circuit fault on L3, a DDOS attack and MITM attack are conducted to assess the effects of cyber-attacks on the power system.

4.2 DDOS attack

In this scenario, there is an attacker node connected to router A, as shown in Figure 9. The attacker sends malware to all terminals in the network and infects approximately 70% of them randomly. The infected terminals are then controlled by the attacker to send meaningless requests to the server, causing a congestion in network traffic.

All the loads in the system are connected to B2. However, the output of G3 is insufficient to meet the load requirements. As a result, the current of B2 directly indicates the behavior and stability of the system. The comparison of B2 current in three scenarios is illustrated in Figure 10.

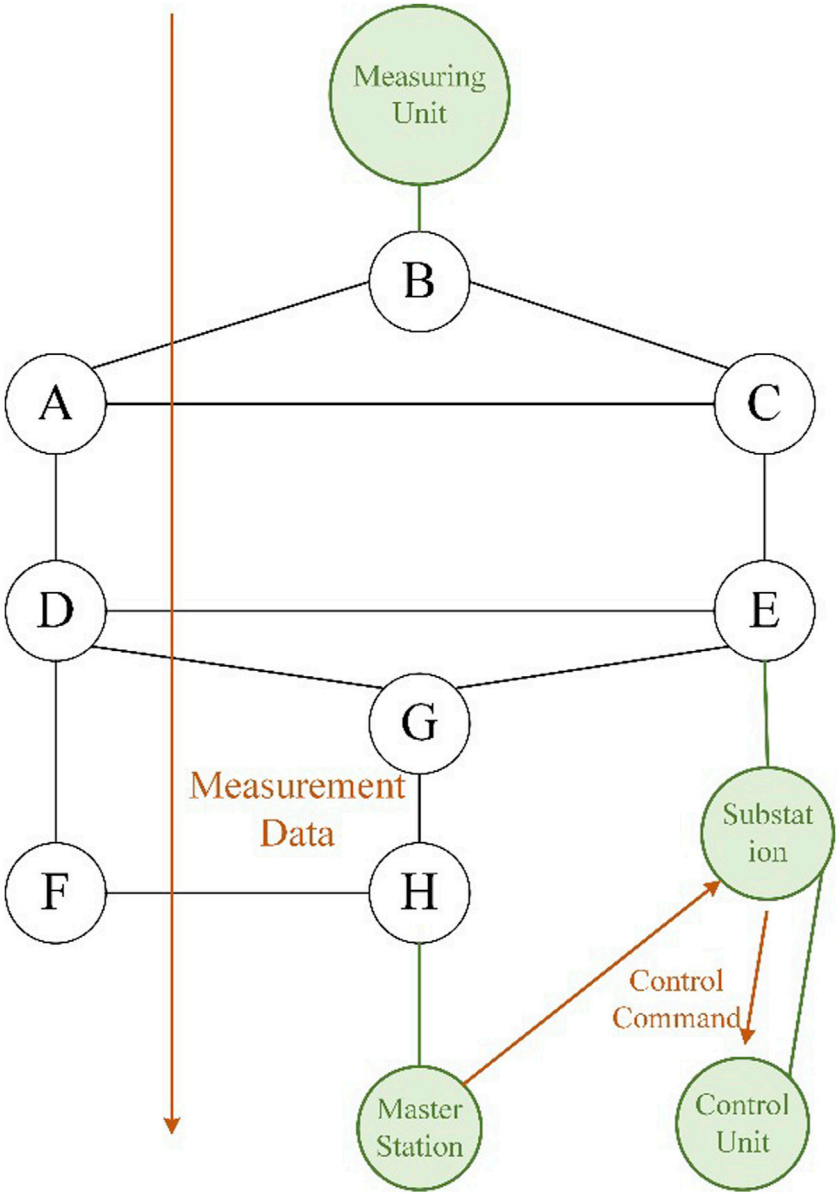

FIGURE 8
Structure of communication network.

Under ideal conditions, without taking into account the communication system and actual devices, the security and stability control device had a response delay of 0 ms. As a result, the control unit disconnected R2 within 2 s of the occurrence of a short-circuit fault, ensuring the stability of the system.

Taking into account the communication system and the actual devices, the channel remained unobstructed and free from congestion in typical situations. The average latency between the substation and the master station was 233.9 ms. The substation promptly disconnected R2, resulting in a reduction of current in L5. This action effectively curbed the further spread of the fault.

During the DDOS attack, the average latency between the substation and the master station significantly increased to 2,136.7 ms due to a high volume of meaning-less packets congesting the channel. Despite the substation responding to the commands from the master station, the prolonged latency resulted in system instability and further propagation of the fault by the protection device.

Figure 11 illustrates the average latency between the substation and the master station for various levels of attack intensity, including infection rates of 30%, 50%, 70%, and 90%. In the case of a mild DDOS attack, the communication system exhibited the capacity to handle the packets sent by the compromised machines, resulting in minimal changes in latency. However, as the number of infected terminals grew, the communication system's resources were depleted, leading to a significant increase in latency.

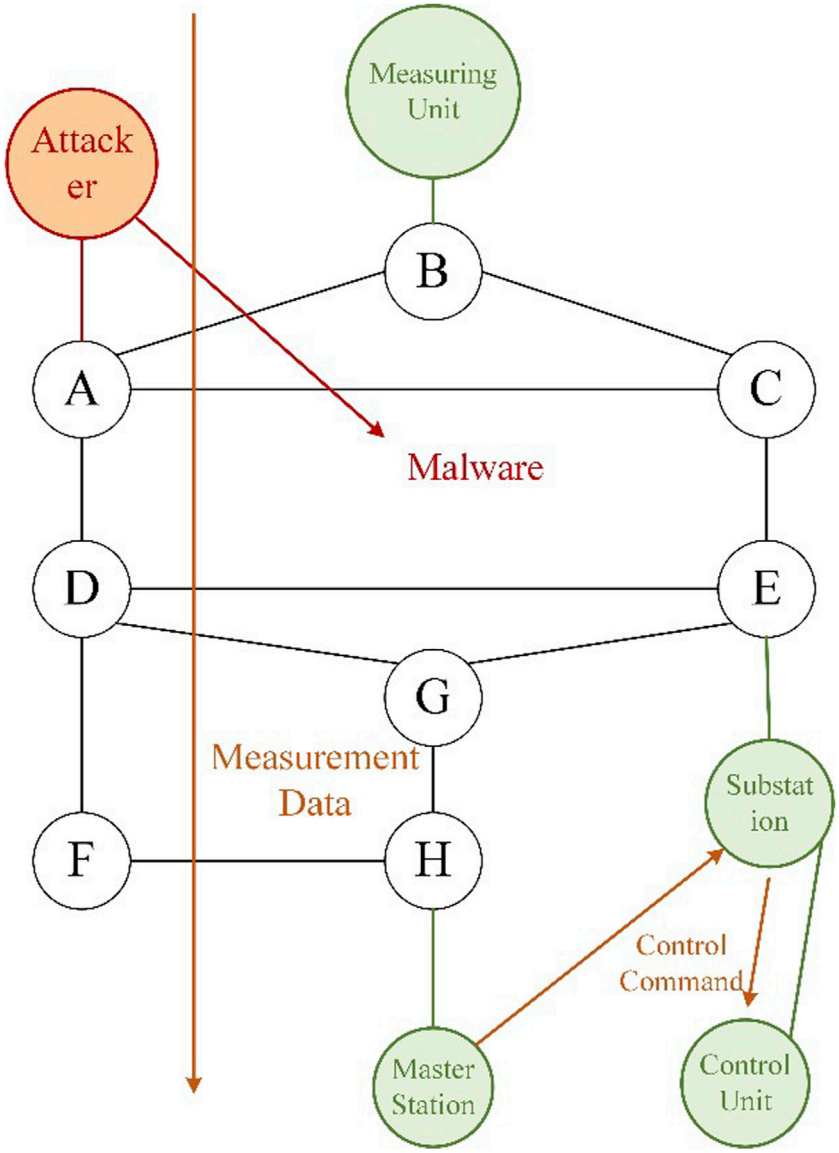

FIGURE 9
DDOS attack.

4.3 MITM attack in mode 1

In this situation, the attacker intercepted the packet sent from the master station to the substation. This prevented the substation from receiving the command, resulting in a missed trip. Table 2 displays the breaker's operating time under both normal conditions and attack conditions following the occurrence of a three-phase short-circuit fault.

As depicted in Figures 12, 13 the attacker intercepted and filtered the control commands sent by the master to the substation, resulting in a missed trip and preventing the breaker from disconnecting R2. As a consequence, the overcurrent protection disconnected L5 at 12.74s and L1 at 15.25s. Unfortunately, the failure continued to spread, eventually causing G3 to go out of step.

4.4 MITM attack in mode 2

In this scenario, the attacker eavesdropped on the packets sent by the master station. Upon detecting a command packet, the attacker intercepted all subsequent packets and randomly sent switching load commands to the substation. As depicted in Figures 14, 15, the current of B2 and the speed of G3 exhibited differences under the MITM attack compared to normal conditions. In the absence of an attack, the substation would disconnect R2, resulting in a gradual decline and stabilization of the current in B2, with only occasional fluctuations in the speed of G3 during load shedding. However, during the attack, the substation indiscriminately switched the load, causing sharp fluctuations in both the current of B2 and the speed of G3. Although the system did not become destabilized in this particular example, the continuous

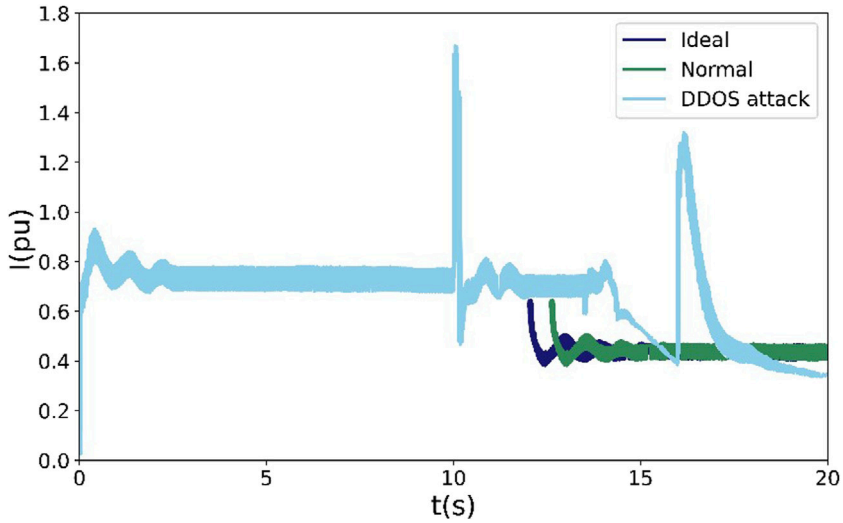

FIGURE 10
Current comparison of B2.

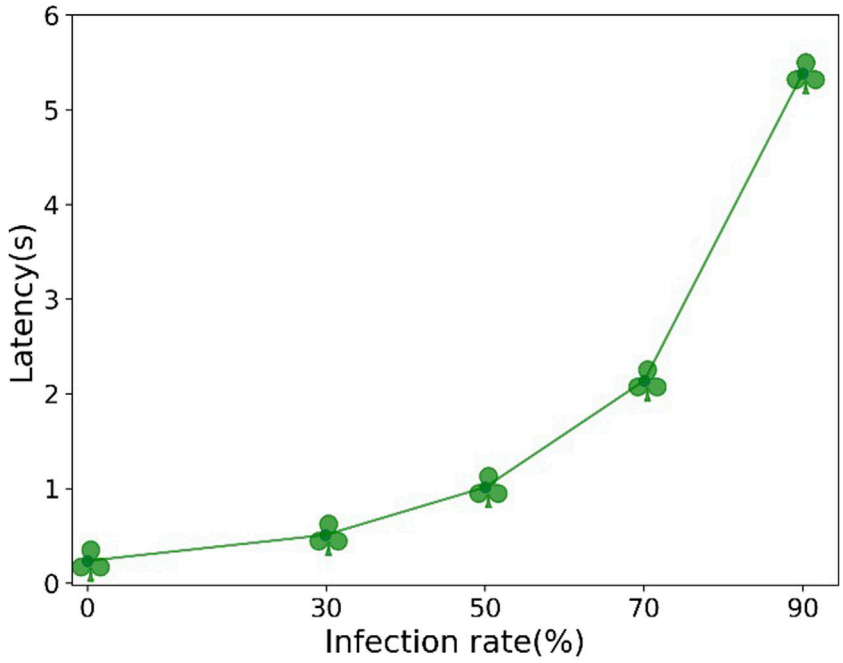

FIGURE 11
Communication latency under different DDOS attack intensity.

injection of disturbances by the malfunctioning substation compromised the stability of the overall system.

In conclusion, the integration of communication networks and cyber-attack considerations greatly enhances the security and stability control of smart grid operations. Without simulating the communication network and utilizing actual devices, it becomes challenging to accurately predict system responses. The co-simulation platform proposed in this study successfully integrates the power system, communication system, and actual devices, providing an effective method for studying Cyber-Physical Systems (CPS) in smart grids.

5 Conclusion

The co-simulation platform proposed in this paper, based on hardware-in-loop, offers several advantages compared to traditional power system simulation:

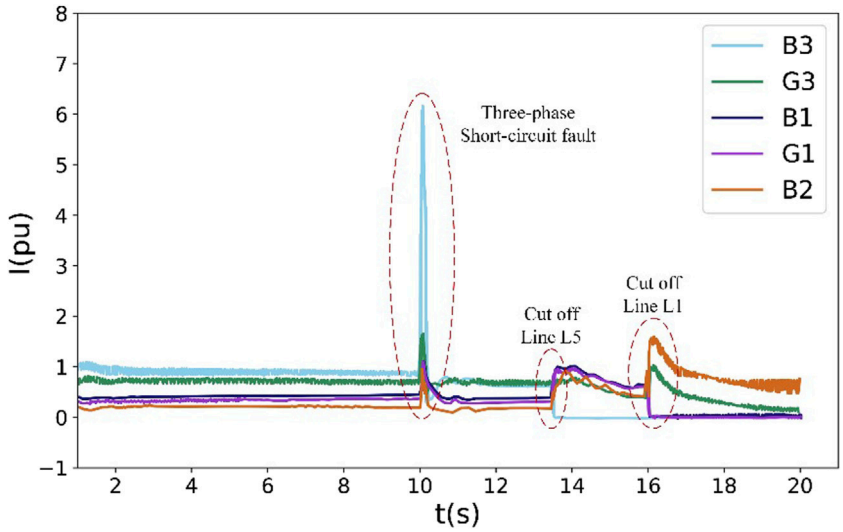

FIGURE 12
Bus current under MITM attack in mode1.

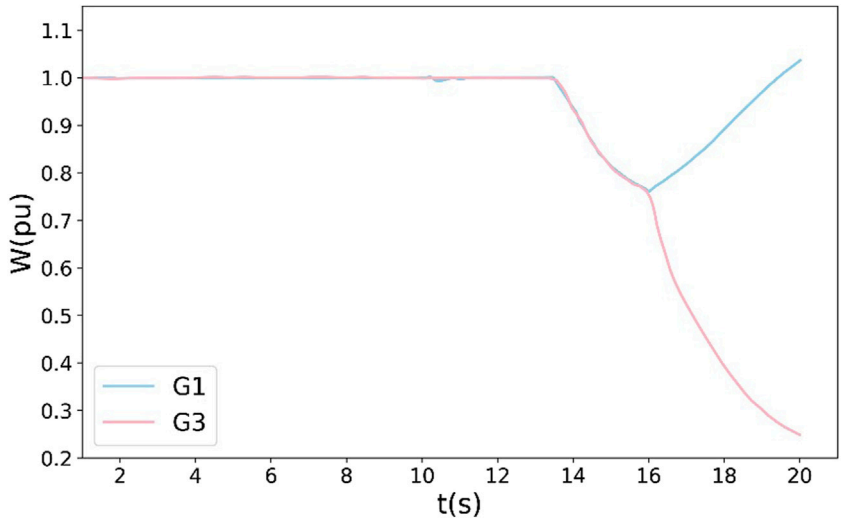

FIGURE 13
Generator speed under MITM attack in mode1.

TABLE 2 The comparison of breaker action moment.

Position	Action	Normal	MITM attack
L3	Off	10.10s	10.10s
R2	Off	12.49s	~
L5	Off	~	13.47s
L1	Off	~	15.98s

1) The co-simulation platform considers the communication system and actual devices present in a typical Cyber-Physical Power System (CPPS). This enables the analysis of various factors such as communication latency, data loss, bit errors, device response delays, and their impact on the power system. The simulation environment closely resembles reality, allowing for comprehensive vulnerability assessments of the entire system,as depicted in Figures 12, 13.
2) Unlike traditional power system simulation that relies on simplified control system models with limited functionality, the co-simulation platform with hardware-in-loop allows for flexible deployment and the accomplishment of complex power system services by incorporating actual devices into the control loop.
3) By integrating security and stability control systems into the co-simulation platform, it becomes possible to simulate cyber-

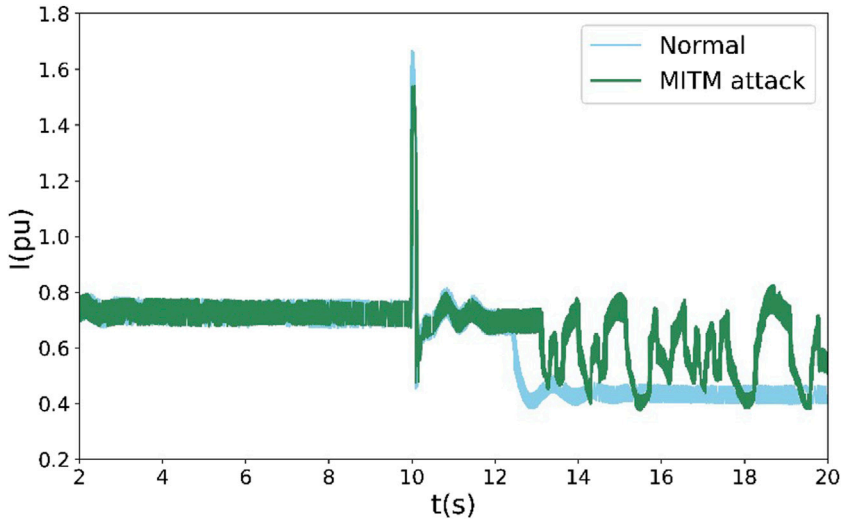

FIGURE 14
Current comparison of B2.

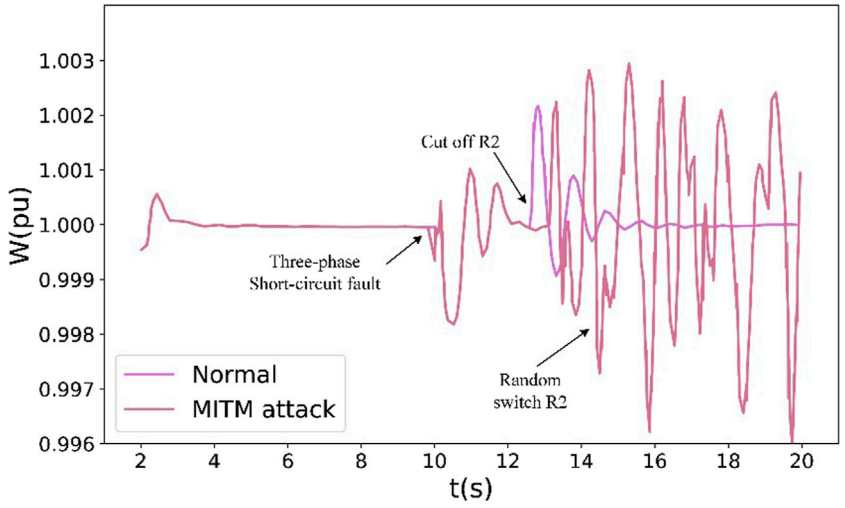

FIGURE 15
Speed comparison of G3.

attacks and assess the propagation of failures for studying security defenses.

However, it is important to note that due to inherent latency in the simulation platform, errors may occur in the results if the network, master station, and device latencies significantly exceed the inherent latency. To address this, further research and development of the co-simulation platform are underway, focusing on the following areas:

1) Studying interface technology and synchronization techniques to reduce or eliminate the inherent latency of the simulation platform, thereby improving the accuracy of simulation results.
2) Quantitatively analyzing communication latency and establishing simulation models to characterize its effects.
3) Expanding the application of the platform to analyze the generation of cyber-attacks and the propagation of failures within CPPS.

Data availability statement

The original contributions presented in the study are included in the article/Supplementary Material, further inquiries can be directed to the corresponding author.

Author contributions

XW: Investigation, Methodology, Writing–original draft. YJ: Formal Analysis, Project administration, Writing–review and editing. ZS: Validation, Writing–review and editing. CL: Resources, Validation, Writing–review and editing. ZJ: Data curation, Writing–review and editing.

Funding

The authors declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest

Authors XW, YJ, ZS, CL, and ZJ were employed by Jiangsu Donggang Energy Investment Co., Ltd.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Alnasser, A., and Rikli, N. E. (2014). "Design of a trust security model for smart meters in an urban power grid network," in *Proceedings of the 10th ACM symposium on QoS and security for wireless and mobile networks*, 105–108.

Alnasser, A., and Sun, H. (2017). A fuzzy logic trust model for secure routing in smart grid networks. *IEEE access* 5, 17896–17903. doi:10.1109/access.2017.2740219

Amaizu, G. C., Nwakanma, C. I., Bhardwaj, S., Lee, J. M., and Kim, D. S. (2021). Composite and efficient DDoS attack detection framework for B5G networks. *Comput. Netw.* 188, 107871. doi:10.1016/j.comnet.2021.107871

Bi, J., Li, J., Wu, K., Gao, Y., Chen, Z., Feng, D., et al. (2023). A data-driven flow surrogate model based on a data-driven and physics-driven method. *Petr. Geol. Rec. Effi* 30 (3), 104–114. doi:10.13673/j.pgre.202205049

Cao, Y., Zhou, B., Chung, C. Y., Shuai, Z., Hua, Z., and Sun, Y. (2023). Dynamic modelling and mutual coordination of electricity and watershed networks for spatio-temporal operational flexibility enhancement under rainy climates. *IEEE Trans. Smart Grid* 14 (5), 3450–3464. doi:10.1109/tsg.2022.3223877

Cao, Y., Zhou, B., Chung, C. Y., Wu, T., Ling, Z., and Shuai, Z. (2024). A coordinated emergency response scheme for electricity and watershed networks considering spatio-temporal heterogeneity and volatility of rainstorm disasters. *IEEE Trans. Smart Grid*, 1. doi:10.1109/TSG.2024.3362344

Cil, A. E., Yildiz, K., and Buldu, A. (2021). Detection of DDoS attacks with feed forward based deep neural network model. *Expert Syst. Appl.* 169, 114520. doi:10.1016/j.eswa.2020.114520

Desai, S., Alhadad, R., Chilamkurti, N., and Mahmood, A. (2019). A survey of privacy preserving schemes in IoE enabled smart grid advanced metering infrastructure. *Clust. Comput.* 22, 43–69. doi:10.1007/s10586-018-2820-9

Dhakne, A. R., and Chatur, P. N. (2017). Design of hierarchical trust based intrusion detection system for wireless sensor network. *Int. J. Appl. Eng. Res.* 12 (8), 1772–1778.

Fan, K., Chen, Q., Su, R., Zhang, K., Wang, H., Li, H., et al. (2021). Msiap: a dynamic searchable encryption for privacy-protection on smart grid with cloud-edge-end. *IEEE Trans. Cloud Comput.* 11 (2), 1170–1181. doi:10.1109/tcc.2021.3134015

Fu, R., Lichtenwalner, M. E., and Johnson, T. J. (2023). A review of cybersecurity in grid-connected power electronics converters: vulnerabilities, countermeasures, and testbeds. *IEEE Access* 11, 113543–113559. doi:10.1109/access.2023.3324177

Guo, Y., Hou, Z., Liu, S., and Jin, S. (2019). Data-driven model-free adaptive predictive control for a class of MIMO nonlinear discrete-time systems with stability analysis. *IEEE Access* 7, 102852–102866. doi:10.1109/access.2019.2931198

Haghnegahdar, L., and Wang, Y. (2020). A whale optimization algorithm-trained artificial neural network for smart grid cyber intrusion detection. *Neural Comput. Appl.* 32 (13), 9427–9441. doi:10.1007/s00521-019-04453-w

Hou, Z. S., and Xu, J. X. (2009). On data-driven control theory: the state of the art and perspective. *Acta. Autom. Sin.* 35, 650–667. doi:10.3724/sp.j.1004.2009.00650

Jabr, R. A. (2013). Adjustable robust OPF with renewable energy sources. *IEEE Trans. Power Syst.* 28, 4742–4751. doi:10.1109/tpwrs.2013.2275013

Kaur, S., Kumar, K., Aggarwal, N., and Singh, G. (2021). A comprehensive survey of DDoS defense solutions in SDN: taxonomy, research challenges, and future directions. *Comput. Secur* 110, 102423. doi:10.1016/j.cose.2021.102423

Luo, G. (2016). A review of automatic selection methods for machine learning algorithms and hyper-parameter values. *Netw. Model. Anal. Health Inf. Bioinforma.* 5, 18. doi:10.1007/s13721-016-0125-6

Menezes, G. K., Astolfi, G., Martins, J. A. C., Tetila, E. C., Junior, A. D. S. O., Gonçalves, D. N., et al. (2023). Pseudo-label semi-supervised learning for soybean monitoring. *Smart Agri. Tech.* 4, 100216. doi:10.1016/j.atech.2023.100216

Mittal, M., Kumar, K., and Behal, S. (2023). DDoS-AT-2022: a distributed denial of service attack dataset for evaluating DDoS defense system. *Proc. Indian Natl. Sci. Acad.* 89 (2), 306–324. doi:10.1007/s43538-023-00159-9

Mittal, M., Kumar, K., and Behal, S. (2023). DL-2P-DDoSADF: deep learning-based two-phase DDoS attack detection framework. *J. Inf. Secur. Appl.* 78, 103609. doi:10.1016/j.jisa.2023.103609

Nguyen, T. T., Nguyen, T. T., and Le, B. (2022). Artificial ecosystem optimization for optimizing of position and operational power of battery energy storage system on the distribution network considering distributed generations. *Expert Syst. Appl.* 208, 118127. doi:10.1016/j.eswa.2022.118127

Osanaiye, O., Choo, K. K. R., and Dlodlo, M. (2016). Distributed denial of service (DDoS) resilience in cloud: review and conceptual cloud DDoS mitigation framework. *J. Netw. Comput. Appl.* 67, 147–165. doi:10.1016/j.jnca.2016.01.001

Othman, S. M., Ba-Alwi, F. M., Alsohybe, N. T., and Al-Hashida, A. Y. (2018). Intrusion detection model using machine learning algorithm on Big Data environment. *J. Big Data* 5 (1), 34–12. doi:10.1186/s40537-018-0145-4

Priyadarshini, R., and Barik, R. K. (2022). A deep learning based intelligent framework to mitigate DDoS attack in fog environment. *J. King Saud University-Computer Inf. Sci.* 34 (3), 825–831. doi:10.1016/j.jksuci.2019.04.010

Riquelme-Dominguez, J. M., Gonzalez-Longatt, F., Melo, A. F. S., Rueda, J. L., and Palensky, P. (2023). Cyber-physical testbed Co-simulation real-time: normal and abnormal system frequency response. *IEEE Trans. Ind. Appl.* 60 (2), 2643–2652. doi:10.1109/tia.2023.3342764

Singh, N. K., Gupta, P. K., and Mahajan, V. (2020). Intrusion detection in wireless network of smart grid using intelligent trust-weight method. *Smart Sci.* 8 (3), 152–162. doi:10.1080/23080477.2020.1805679

Singh, N. K., and Mahajan, V. (2020). Detection of cyber cascade failure in smart grid substation using advance grey wolf optimization. *J. Interdiscip. Math.* 23 (1), 69–79. doi:10.1080/09720502.2020.1721664

Singh, N. K., and Mahajan, V. (2021). End-user privacy protection scheme from cyber intrusion in smart grid advanced metering infrastructure. *Int. J. Crit. Infrastructure Prot.* 34, 100410. doi:10.1016/j.ijcip.2021.100410

Vu, L., Nguyen, T. L., Abdelrahman, M. S., Vu, T., and Mohammed, O. A. (2023). A cyber-HIL for investigating control systems in ship cyber physical systems under communication issues and cyber attacks. *IEEE Trans. Ind. Appl.* 60 (2), 2142–2152. doi:10.1109/tia.2023.3311429

Yu, T., Da, K., Wang, Z., Ling, Y., Li, X., Bin, D., et al. (2022). An advanced accurate intrusion detection system for smart grid cybersecurity based on evolving machine learning. *Front. Energy Res.* 10, 903370. doi:10.3389/fenrg.2022.903370

Zhang, D., Kang, C., Lu, X., Liu, X., Zhang, N., and Xu, Y. (2021). Demonstration on the scale of energy storage deployment in high-proportion new energy power system. *South. Power Syst. Technol.* 16, 3–11.

Zhang, Y., Meng, X., Malik, A., and Wang, L. (2022). The use of analytical converter loss formula to eliminate DC slack/droop bus iteration in sequential AC-DC power flow algorithm. *Int. J. Electr. Power and Energy Syst.* 137, 107596. doi:10.1016/j.ijepes.2021.107596

Zhang, Y., Meng, X., Shotorbani, A. M., and Wang, L. (2020a). Minimization of AC-DC grid transmission loss and DC voltage deviation using adaptive droop control and improved AC-DC power flow algorithm. *IEEE Trans. Power Syst.* 36 (1), 744–756. doi:10.1109/tpwrs.2020.3020039

Zhang, Y., Mohammadpour Shotorbani, A., Wang, L., and Mohammadi-Ivatloo, B. (2021a). Enhanced PI control and adaptive gain tuning schemes for distributed

secondary control of an islanded microgrid. *IET Renew. Power Gener.* 15 (4), 854–864. doi:10.1049/rpg2.12074

Zhang, Y., Qian, W., Shao, J., Zhang, F., Wang, L., Hu, Q., et al. (2024). Adaptive voltage reference based controls of converter power sharing and pilot voltage in HVDC system for large-scale offshore wind integration. *IEEE Open Access J. Power Energy* 11, 55–67. doi:10.1109/oajpe.2024.3354079

Zhang, Y., Qian, W., Ye, Y., Li, Y., Tang, Y., Long, Y., et al. (2023). A no*vel non*-intrusive load monitoring method based on ResNet-seq2seq networks for energy disaggregation of distributed energy resources integrated with residential houses. *Appl. Energy* 349, 121703. doi:10.1016/j.apenergy.2023.121703

Zhang, Y., Shotorbani, A. M., Wang, L., and Li, W. (2020b). Distributed voltage regulation and automatic power sharing in multi-terminal HVDC grids. *IEEE Trans. Power Syst.* 35 (5), 3739–3752. doi:10.1109/tpwrs.2020.2986168

Zhang, Y., Shotorbani, A. M., Wang, L., and Li, W. (2021b). A combined hierarchical and autonomous DC grid control for proportional power sharing with minimized voltage variation and transmission loss. *IEEE Trans. Power Deliv.* 37 (4), 3213–3224. doi:10.1109/tpwrd.2021.3125254

Zhang, Y., Shotorbani, A. M., Wang, L., and Mohammadi-Ivatloo, B. (2021c). Distributed secondary control of a microgrid with a generalized PI finite-time controller. *IEEE Open Access J. Power Energy* 8, 57–67. doi:10.1109/oajpe.2021.3056507

Zhang, Y., Wang, L., and Li, W. (2020c). Autonomous DC line power flow regulation using adaptive droop control in HVDC grid. *IEEE Trans. Power Deliv.* 36 (6), 3550–3560. doi:10.1109/tpwrd.2020.3044978

Zhao, N., and You, F. (2021). New York State's 100% renewable electricity transition planning under uncertainty using a data-driven multistage adaptive robust optimization approach with machine-learning. *Adv. Appl. Ene* 2, 100019. doi:10.1016/j.adapen.2021.100019

Zhao, Y., Yuan, Z., Lu, C., Zhang, G., Li, X., and Chen, Y. (2016). Improved model-free adaptive wide-area coordination damping controller for multipleinput-multiple-output power systems. *IET Gener. Transm. Distrib.* 10, 3264–3275. doi:10.1049/iet-gtd.2016.0069