IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 3, 2020, accepted April 30, 2020, date of publication May 19, 2020, date of current version June 3, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2995743

Design of a Cosimulation Platform With Hardware-in-the-Loop for Cyber-Attacks on Cyber-Physical Power Systems

ZENGJI LIU[1], (Member, IEEE), QI WANG[2], (Member, IEEE), AND YI TANG[2], (Senior Member, IEEE)

[1]School of Cyber Science and Engineering, Southeast University, Nanjing 210000, China
[2]School of Electrical Engineering, Southeast University, Nanjing 210000, China

Corresponding author: Qi Wang (wangqi@seu.edu.cn)

This work was supported in part by the National Key Research and Development Program of China (Basic Theories and Methods of Analysis and Control of the Cyber Physical Systems for Power Grids) under Grant 2017YFB0903000, in part by the Project of State Grid Corporation of China Research Program under Grant 8516000912, and in part by the National Natural Science Foundation of China under Grant 51707032.

ABSTRACT This paper presents a real-time cosimulation platform with hardware-in-the-loop (HIL) for performing cyber-physical power system (CPPS) analyses based on RT-LAB and OPNET software. The platform is capable of simulating a power grid and communication network while also reflecting the impact of actual devices and cyber-attacks on the power system. Furthermore, modelling and implementation methods focused on distributed denial of service (DDOS) and man-in-the-middle (MITM) attacks in a communication network are elaborated. A case study of DDOS and MITM attacks in a typical CPPS is demonstrated based on this platform. The simulation results validate the capability of the platform and also show the importance of considering the separate impacts of the communication system, actual devices and cyber-attack in power system simulations.

INDEX TERMS Cyber-physical system, cyber-attack, cosimulation, hardware-in-the-loop, smart grid.

I. INTRODUCTION

Great developments have occurred in power systems in recent years [1]. In such systems, a large number of sensors, communication equipment and control devices are integrated into the power grid and communication network, which offers the unique opportunity to transform power systems into cyber-physical power systems (CPPSs) [2], [3]. The acquisition and utilization of multiple sources provide data support for the analysis and control of power systems [4].

However, the increasing dependency on communication systems introduces additional risks to the CPPS [5]. Communication faults (e.g., interruptions, high latency and bit errors) caused by unreliable physical components or devices in the system may lead power systems to operate in a critical state that could progress to cascading failures [6]. Moreover, cyber-attacks carried out by hostile organizations or individuals may also result in power system blackouts over large areas [7].

Although not directly destroying the equipment of the physical power system, cyber-attacks can weaken or even completely devastate the normal functions of the communication system, thereby causing serious impacts on the overall system stability, economic operation and social stability. The Ukrainian blackout event in 2015 represents a typical case caused by a cyber-attack [8]. An attacker disguised Blackenergy, a kind of malware, as an office macro to infect a sub-station computer via email. Blackenergy built a back door for KillDisk to damage and overwrite files stored on infected computers to prevent the operating system from starting. Therefore, the impact of the communication system must be considered when studying traditional power service.

The main research points on CPPSs include the mechanism of interaction, methods of modelling and analysis and control theories for deeply integrated systems [9]. The traditional analytical methods for power systems and communication systems are basically fragmented because the power system is continuous while the communication system is discrete [10]. Thus, performing in-depth analyses of the impact of the communication system on the power system is difficult under the existing theoretical methods.

Although significant breakthroughs in the theoretical research on this topic are required, modelling and simulations based on the features of the CPPS can provide support

The associate editor coordinating the review of this manuscript and approving it for publication was Weixing Li.

for research on related theories and application issues [11]. Therefore, a tool that can deeply analyze the complex static and dynamic characteristics of the CPPS must be developed. Due to the essential differences between power systems and communication systems in the mathematical model, complete and reliable simulation software has not been developed [12]. Therefore, the co-simulation of CPPS has become a research hotspot.

In recent years, several research institutions have proposed different design strategies. However, co-simulation theory is not well established due to the difficulty in coordinating the time scales of different simulation tools. These design strategies can be divided into three kinds: uni-event axis synchronization, fixed timestamps synchronization and uni-timeline synchronization [13]–[16].

Uni-event axis synchronization involves adding events from both the power and cyber system that require responses on the same event axis to achieve simulation synchronization. The power system simulation result at each time step is added to the event axis in the form of an event. This scheme does not require the two systems to be absolutely synchronous in terms of simulation time. A typical application is combining PSLF and NS2 software with a simulation manager [13]. However, the enormous difference in the step size between the two systems would cause a decrease in the accuracy because the emergency would not be handled in sufficient time during the simulation.

Fixed timestamps synchronization involves setting timestamps for data exchange before running the simulations. The simulations stop at the timestamps for data transmission and continue to execute after transmission. Typical schemes include VPNET [17], GECO [18], RoboNetSim [19], EOPCHS [20], INSPIRE [21]. This kind of strategy performs well in situations where all events are set at an exact timestamp. However, the results may present errors when unpredictable emergencies occur.

Uni-timeline synchronization involves setting the same timeline for the power system and cyber system in the simulation so that the behaviors of both systems can be simulated with high accuracy. However, developing this kind of platform is difficult and costly. Some successful examples such as the platform based on OPAL-RT and OPNET which is applied to test power system protection systems [22], and the platform based on RTDS and OPNET which is used to study the impact of the cyber-attacks [23].

The modelling of cyber-attacks focuses on the behavior of the attacker and the consequences of the attack, including adversary action model, intrusion activity model, strategy competition between adversary and defender [24]. The efforts for modelling adversary cyber actions to controls in power system have been reviewed in [25]. The methods such as attack tree, petri nets [26] and attack graph [27] were used to evaluate the security of power system.

To simulate cyber-attacks, the power system and communication system need to be simulated in real time because packet transmission and cyber-attack data processes are real time events. Moreover, to truly reflect the process of cyber-attacks, the hardware devices need to be introduced in the platform. Therefore, the real-time simulation of the uni-timeline synchronized strategy with the security and stability control device is built to form the cosimulation platform.

The cosimulation platform in this paper can improve the simulation accuracy of a CPPS compared with that of traditional power simulation methods, and it can be used to study the process of cyber-attacks with HIL, including the start and propagation of consequent faults, thereby providing a reference for the development of security defence measures.

The remainder of the paper is organized as follows. Section 2 introduces the CPPS structure and cosimulation platform framework as well as the modelling methods for power systems, communication systems and security and stability control devices in detail. Section 3 introduces the implementation of distributed denial of service (DDOS) and man-in-the-middle (MITM) attacks in the proposed platform. Section 4 provides a case study of a CPPS and presents the simulation results of cyber-attacks. Finally, Section 5 presents the summary and conclusions.

II. COSIMULATION PLATFORM FRAMEWORK

A. CPPS STRUCTURE

The architecture of the CPPS can be divided into the following four parts as shown in Figure 1: the power system, smart terminals, communication network and the control centre.

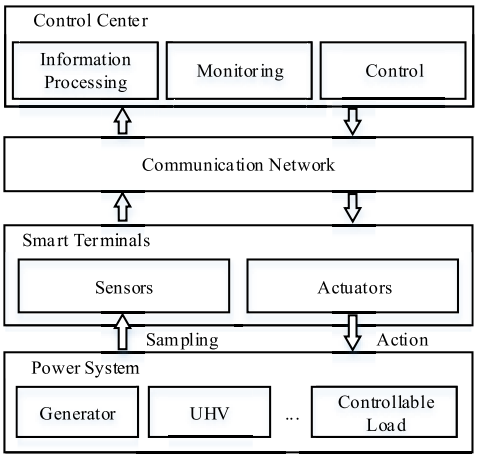

FIGURE 1. Structure of the CPPS.

The power system contains various types of power sources (thermal power, hydropower, nuclear power, wind power, photovoltaics, etc.), distribution and transmission networks (UHV AC/DC transmission line, flexible AC/DC transmission system, power electronic equipment, etc.) and power load (traditional load, controllable load).

Smart terminals include different kinds of measuring equipment and control equipment (distribution terminal, monitoring terminal, load control terminal, etc.) that improve the real-time perception and control capabilities of the power system.

The communication network is a private or public network composed of multiple types of information and communication equipment with different bandwidths and transmission protocols, and it provides real-time and reliable communication services for different requirements of the power service. Disturbances or faults in the communication network in the CPPS will have an impact on the power system. The control centres monitor several types of data for decision-making (system scheduling, fault monitoring, security and stability control, etc.).

Smart terminals collect data from the power system and upload these data to the servers of the power service through the communication network. The servers generate the control commands and send them to the smart terminals. Finally, the power system's physical devices are operated by smart terminals.

B. PLATFORM FRAMEWORK

For different power services, the simulation requirements and the structure of the control system vary. This paper focuses on the security and stability control system, and the structure is shown in Figure 2.

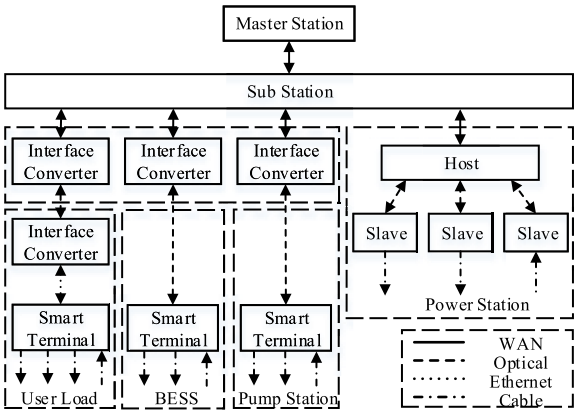

FIGURE 2. Structure of the security and stability control system.

The security and stability control device is a decision-making system with a master station and a sub-station. Interface converters are used to connect different kinds of communication lines or convert data packets between different kinds of communication protocols. Smart terminals can be divided into measuring units and control units that perform the functions of data acquisition and control. The function of a slave in the power station is similar to that of the smart terminal, and the host is used for data collection and conversion. The states of the grid are collected by the measuring unit and transmitted to the master station through the communication network. The master station calculates and generates control commands according to the strategy and sends them to each sub-station. The sub-station selects the control unit and sends the command based on the local control strategy. Finally, the specific operations are implemented by the control units.

To coordinate discrete and continuous simulations, a modular design is adopted in this paper. The cosimulation platform can be divided into four modules: power system, communication system, master station and sub-station. These modules are connected via the Ethernet to simplify the design of the data interface and improve the efficiency of modelling. OPAL-RT and OPNET are simulation tools for simulating the power system and the communication system. The master station and sub station are hardware device for generating control commands which can reflect the real working state of the control system. The architecture of the cosimulation platform is shown in Figure 3.

C. MODELLING AND DESIGNING OF EACH PART

1) POWER SYSTEM SIMULATOR

The cosimulation platform has high real-time requirements. However, most of power simulation tools are based on PCs, and a large-scale simulation cannot perform in real time when the step size is small. Therefore, OPAL-RT is chosen as the power system simulator along with its modelling software RT-LAB.

The modelling in RT-LAB can be divided into four parts: power grid, measuring unit, control unit and network interface. The original power grid must first be simplified to the equivalent network for real-time simulation. The grid model is designed according to the equivalent network and verified by offline simulations. The measuring unit, sampling frequency and data type of the packet need to be defined, such as the voltage, current, frequency and power-angle. For the control unit, the target and structure of commands sent from the sub-station must be determined when modelling. The control unit is set up to convert the control commands into control quantities and output them to the control target. The network interface consists of the OpIPSocketCtrl module, the OpAsyncRecv module and the OpAsyncSend module, which are responsible for controlling, receiving and sending, respectively. Multiple sets of network interfaces are included in the power system model, and they can be distinguished by port numbers.

2) COMMUNICATION SYSTEM SIMULATOR

The communication system is simulated by OPNET to ensure the real-time performance. For different levels of communication networks, the modelling in OPNET is divided into three layers: network layer, node layer and process layer. The communication network, protocol, algorithm and equipment can be constructed via three-level modelling.

For certain end-to-end services, the semi-physical simulation interface can be used to connect the real network with the virtual network. OPNET provides three kinds of semi-physical simulation interfaces: HLA-API, ESA-API and System in the loop (SITL). HLA-API and ESA-API need to define the process model and node model and design the corresponding interface program. Although the freedom is high, the development is cumbersome. SITL is the model provided by OPNET. Although the supported protocols are limited and the mapping model needs to be designed to map

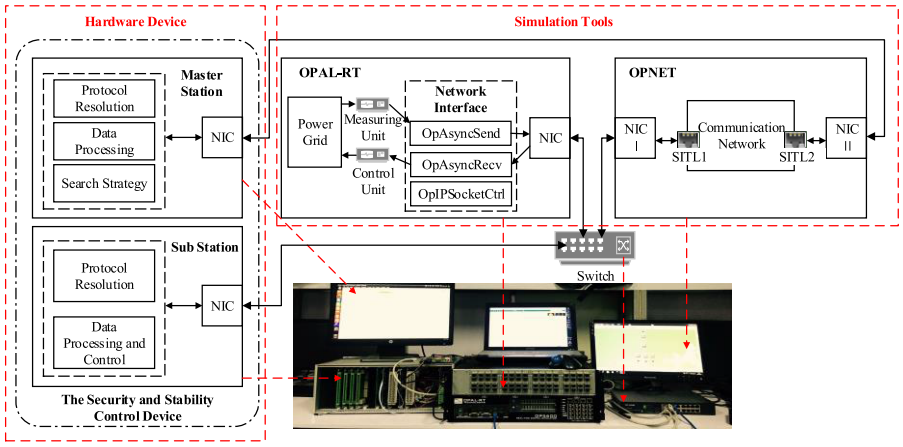

FIGURE 3. Architecture of the cosimulation platform.

real packets into virtual packets, external devices can be easily accessed by the simulation system. To simplify the model design, SITL is selected as the data interface in this paper.

The measurement units and sub-station exchange data with the master station via the communication system, and the control units exchange data with the sub-station directly through a switch. Therefore, two network interface cards (NICs) are inserted in the OPNET host. NIC1 communicates with the OPAL-RT and the sub-station through the switch, and NIC2 communicates with the master station directly. The network model contains multiple SITL modules which can be matched to the master station, sub-station and measuring units by setting filters.

In order to connect the hardware device to the simulation platform, the simulation modules use the IEC 60870-104 protocol for communication. Because this protocol is based on the TCP protocol, the data packet of it can be directly mapped to the virtual network in OPNET. For other protocols (Modbus, IEC61850, IEC61970, DNP3, etc.), the corresponding packet models and communication process models need to be designed in OPNET. The packets of IEC 60870-104 protocol can be mapped into packets of the required protocol in SITL module. The communication distance between modules in the platform is short, so the kind of protocol used between them has less influence on the simulation results. While the network simulated in OPNET is WAN, different protocols have great influence on the simulation results.

3) THE SECURITY AND STABILITY CONTROL DEVICE

The security and stability control device is the second and third defensive line of the power grid, and it is responsible for emergency control after a fault, such as load shedding, generator tripping or rapid valve shutting, to restrain the further spreading of the grid fault. This device is divided into a master station and a sub-station. The master station monitors the status of the power grid through the measuring unit. After identifying the fault, the master station compares it with the security control strategy according to the fault type and fault location. The master station selects the optimal control strategy and sends control commands to the sub-station. The sub-station reports the amount of controllable load to the master station and receives the control commands. The sub-station then sends the commands to the control units according to the local control strategy to execute the actual operation.

The master station is designed based on Linux and C programming language and has the ability to implement complex services. The master station obtains the real-time status of the power grid from OPAL_RT and receives the control command from the security and stability control device to monitor and control the power system. The master station can be divided into the following four modules.

The protocol analysis module is used to analyse the packets sent by the measuring unit and sub-station. Master station first intercepts the data section according to the pre-set offset and verifies the correctness of the message. And then, the header is read to determine the message type and source. Finally, the master station performs the operation according to the command code.

The grid status database is designed to store the real-time status of the power grid, including the breaker status, transformer tap positions, voltage and frequency. Whenever the status of the grid in the database is updated, the fault detection module is executed and sends an alarm if system failure occurs. When the fault detection module sends an alarm, the control module develops a variety of coordinated control schemes according to the strategy, and it then analyses the implementation effects and selects the optimal scheme to generate the control queue for the sub-station.

The sub-station in this paper is developed based on embedded Linux and consists of the following five parts as shown in Figure 4: control module, input/output (I/O) module, measuring module, man-machine interface and communication module. The sub-station communicates with the master station with a period of 0.833 ms. In a control cycle, the sub-station completes the following four steps.

Step 1: The sub-station sends a packet containing the amount of controllable load to the master station and waits for the return packet.

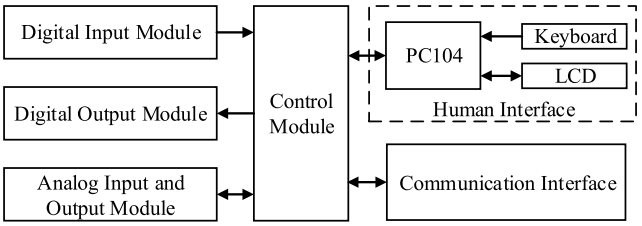

FIGURE 4. Structure of the sub-station.

Step 2: The sub-station receives the packet from the master station and determines the type according to the packet header.

Step 3: For a synchronization packet, the sub-station revises the system clock. However, for a command packet, the sub-station generates the control queue according to the local control strategy. Otherwise, the abnormal packet is returned to the master station.

Step 4: All the commands are distributed to the control unit if the queue is not empty.

4) TIME STEPS OF THE COSIMULATION

The timeline of a real-time simulation in the platform consisting of a power system, communication system, master station and sub-station is shown in Figure 5. The communication cycle between the measuring unit and master station is T_1, whereas the cycle between the control unit and sub-station is T_2. When the simulation reaches the moment A1, the measuring unit sends the sampled data to the master station, and at moment D1, the data are received by the master station. The sub-station system sends the data of the controllable load to the master station at moment B1. Upon receiving the data at D2, the master station processes the data and sends a synchronization message or control order message to the sub-station. After analysis, the sub-station transmits control orders to the control unit at B3. After receiving the order, the control unit updates the related parameters in the power system node at A2.

The system latency is composed of 4 parts: network latency Δt_n, master station latency Δt_m, sub-station latency Δt_s and the inherent latency of the simulation platform Δt_p. The network latency is the latency caused by the communication system, which is determined by the OPNET simulation. Network latency includes the time delay caused by packet loss, bit errors, routing, bandwidth limitations and servers. The master station latency is the latency caused by limited capabilities of the hardware and software used in the master station system and mainly consist of hardware latency Δt_{hd} and software latency Δt_{sf}. Hardware latency includes the latency of the master station system server network card, data transfer latency inside the master station, etc. Software latency is the time consumed by power service computations carried out in the master station, such as state estimations, measurement information management, power quality monitoring, etc. Sub-station latency is the latency caused by limited capabilities of the hardware and software used in the sub-station system and primarily consists of hardware latency and software latency. The inherent latency is caused by the data processing in NICs and the communication between each simulation module in the platform.

The platform inherent latency does not occur in the actual CPPS and cannot be eliminated. The latency is also random and varies in accordance with the data flow amount between modules. When the data packet length is less than 64 bytes, the inherent latency is approximately $1 \sim 2$ ms. Because the total latency of network, master station and sub-station is tens to hundreds of milliseconds, the inherent latency is negligible and will not have a significant influence on the simulation accuracy. To further reduce the influence of inherent latency, the communication latency is obtained between modules using the Ping command, the time delay is considered the inherent latency, and the inherent latency is subtracted from the controllable latency in the master station system.

III. CYBER-ATTACK MODELING

A. DISTRIBUTED DENIAL OF SERVICE ATTACK

A DDOS attack is a kind of resource-exhaustion attack in which attackers manipulate multiple computers as the attack source by Client/Server techniques to strengthen the attack effect, including Synflood, Smurf, Land-based, etc. After a DDOS attack, the host has a large number of waiting connections and the network is flooded with massive useless packets, which results in network congestion. Consequently, the attack target cannot communicate with the outside.

The attack scheme of a DDOS is demonstrated in Figure 6a, and it consists of the 4 following parts: attacker, control puppet, attack puppet and target. The attackers obtain

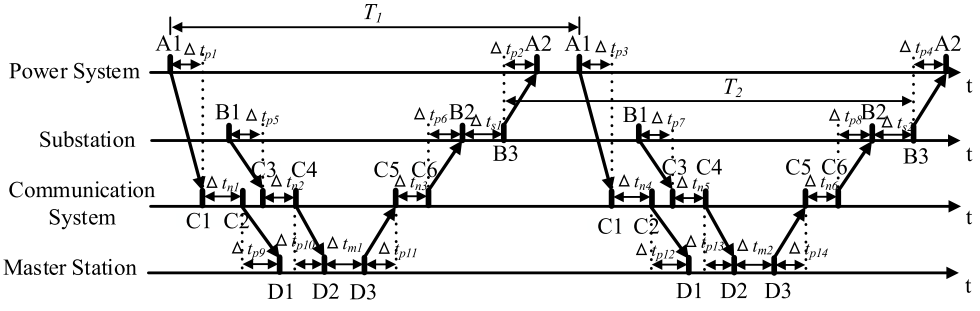

FIGURE 5. Time steps of cosimulation.

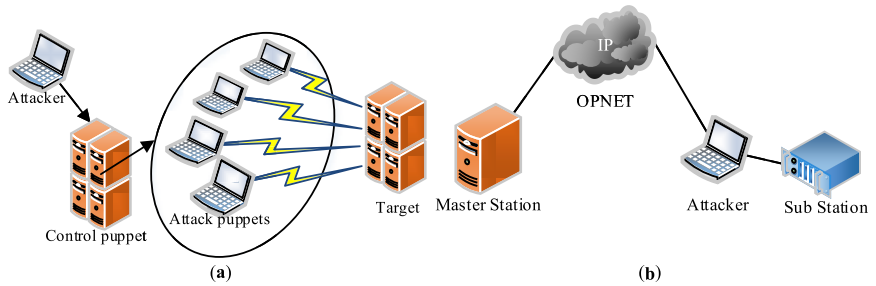

FIGURE 6. Cyber-attacks: (a) DDOS attack, (b) MITM attack.

control of the control puppet and attack puppet partly or fully. The control puppet sends the attack program to the attack puppet, the attacker sends a command to the attack puppet through the control puppet, and then the attack puppet sends the actual attack packets to the target.

In this paper, the attacker node is deployed in the OPNET simulation. The standard model library provided in OPNET is used to build the DDOS attack scenario. The steps are as follows.

Step 1: Build the communication network. Infected nodes, normal nodes, serves, attacker nodes and monitoring nodes are needed in the network. Routing table needs to be configured to supply the power services in terminals and servers.

Step 2: Configure the cyber effect scripts. Four basic operations are provided in OPNET, including infection, confirming infection, generating traffic flow, and scanning infected nodes. The required cyber effect scripts can be obtained by combining these four operations. The infection script defines the number of infected nodes and the duration. The confirmation script defines the moment when the infected nodes return the packets to attacker. The flooding script defines the start time and the traffic flow of the attack. The clear script defines the time that start scanning and the number of infected nodes cleared.

Step 3: Link the cyber-attack profiles. DDOS attack consists of 2 phases. In phase P1, the attacker randomly scans and attacks all terminals where the infected computers will send confirmations back to the attacker, therefore P1 is linked to the infection script and the confirmation script. In phase P2, the infected computers will send many meaningless packets to flood the network connected to the target, therefore P2 is linked to flooding script.

Step 4: Link the cyber remedy profile. The cyber remedy profile is linked to clear script. It scans and clears the infected nodes when the monitoring node detects the cyber-attack. If the defense is not considered in the simulation, the cyber remedy profile can be set to null.

B. MAN-IN-THE-MIDDLE ATTACK

MITM attack is an indirect approach to controlling the target. The attacker invades and controls a virtual computer by IP address spoofing and port spoofing and build a new communication channel between the original nodes. Packets in the new channel are be easily modified to make the target send a wrong decision. Careto, Cryptolocker, Dexter and FinFisher are typical MITM attack methods.

A computer with two NICs is used as the attacker in the research as in Figure 6b. Two NICs are connected to the OPNET and sub-station, and the IP address of the NIC connected to sub-station is set as the master station while the IP address of the NIC connected to the master station is set as the sub-station.

The two proposed MITM methods are detailed as follows:

Data interception, which the attacker intercepts the packet from the sub-station and master station and analyses the packet header to determine the function of the packet. If a time packet is detected, it will be copied to the buffer and sent to the sub-station. If a command packet is detected, it will be replaced by the time packet in the buffer. Under this attack, the sub-station cannot receive the command from the master station.

Data tampering, which attacker replace all packets to the modified command packets to make the sub-station execute load shedding and casting unreasonably, once a command packet is detected.

IV. CASE STUDY

A. TEST SYSTEM DESCRIPTION

To reflect the influence of the communication system and devices on the power system simulation and verify the correctness and necessity of the cosimulation platform applied for the power system analysis, a 7-bus system (shown in Figure 7a) is built in RT-Lab. This system consists of seven buses, two controllable loads, two generators, one ideal voltage source, four transformers and seventeen circuit breakers. The buses B1, B2 and B3 are monitored by the measuring units, and the controllable load and the generator are

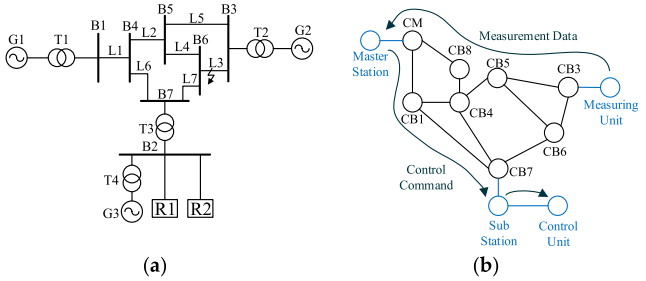

FIGURE 7. Structure of the 7-bus system: (a) power system, (b) communication system.

jointly controlled by the protection unit and control unit. The protection unit prohibits the control unit from operating the protected device after breaking it out. In this case, the reference AC voltage value is 230 kV, the frequency is 60 Hz, the simulation step h $= 2.5 \times 10^{-5}$s, and the parameters of each device are shown in Table 1.

TABLE 1. Parameters of devices.

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

The system protection and security control strategy of the three-phase short-circuit fault on transmission line L3 are as follows. The short-circuit protection unit cuts off L3 0.1 s after the fault occurs. The overcurrent protection unit cuts off L1 2 s after the fault occurs and cuts off L5 3.5 s after the fault occurs. The security and stability control device cut off R2 2 s after the short-circuit fault occurs.

The communication network built in OPNET is shown in Figure 7b, which contains 8 router nodes with a number of servers and terminals for simulating the data transmission generated by other services. The measuring unit, master station and sub-station are accessed by the communication network in OPNET through the SITL module, and the control unit is connected with the sub-station through the switch. The communication channel between the router nodes adopts a 100 Mbps optical fibre. CB1∼CB7 in communication network correspond to B1∼B7 in power grid. CB8 is a relay router, and CM is the router of master station.

The DDOS attack and MITM attack are performed after the three-phase short-circuit fault occurs on L3 to observe the impact of the cyber-attack on the power system.

B. DDOS ATTACK

In this scenario, an attacker node was connected to node CB5 in OPNET, which sent malware to all terminals in the network and randomly infected 80% of them. The attacker controlled the infected terminals, which send twice as many packets as normal, and forced them to send meaningless requests to the server at 10s to clog up the network. The data traffic and CPU utilization of master station is shown in Figure 8 and the response delay is shown in Figure 9. Before the attack started, the data traffic from all terminals to master station was about 64.2Mb/s. The master station CPU utilization was 32% and the response delay was 0.58s due to the small amount of packet that needs to be processed. After the attack, the data traffic jumped to 110.5Mb/s and the CPU utilization was up to 86.4%. It caused the channel

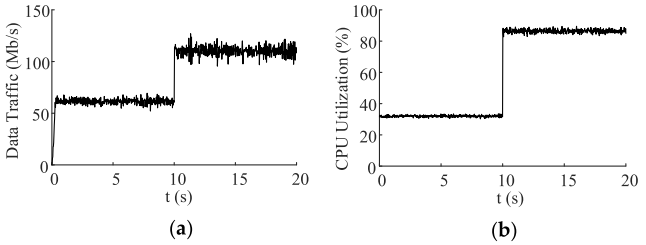

FIGURE 8. Operating data of master station: (a) data traffic, (b) CPU utilization.

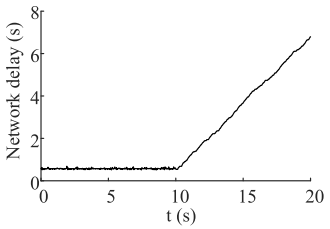

FIGURE 9. Response delay.

to be overloaded and more packets to be queued. Therefore, the response delay of the system continued to increase.

In power system, all the loads are connected to B2, and the output of G3 is not enough to supply the load. Therefore, the current of B2 can directly reflect the load action and stability of the system. A comparison of the currents of B2 in three scenarios is shown in Figure 10.

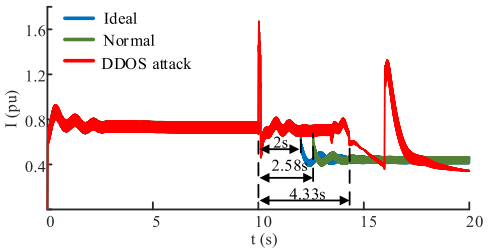

FIGURE 10. A comparison of the currents of B2.

Under the ideal environment, without considering the communication system and the actual device, the response delay of the security and stability control device was 0 ms. Therefore, the control unit cut off R2 after 2 s of the short-circuit fault, and the system remained stable.

Considering the communication system and the actual device, the channel was non-blocked and congestion-free under the normal circumstance. The sub-station cut R2 off in time; therefore, the current of L5 was reduced, which suppressed the spread of the fault.

During the DDOS attack, the response delay increased when a large number of meaningless packets blocked the channel. Although the sub-station responded to the command of the master station, the latency was too long, and the protection device further spread the fault and caused system instability.

For different attack intensities, the average response delay and the communication devices operation data is shown in Table 2. Under the weak DDOS attack with the infection

TABLE 2. The simulation results of communication system under different attack intensity.

Infection rate	Data traffic	Delay	Utilization (CPU)	Utilization (Channel)
0%	64.2Mb/s	0.58s	32%	57.9%
20%	73.7Mb/s	0.62s	38.4%	69.3%
40%	86.0Mb/s	0.66s	44.8%	80.7%
60%	98.2Mb/s	0.78s	61.4%	92.1%
80%	110.5Mb/s	2.33s	86.4%	103%
100%	122.8Mb/s	3.10s	100%	115%

rate lower than 60%, the communication system had the ability to carry the packets sent by the puppet machine, and the response delay changed little. As the number of infected terminals increased, the resources of the communication system were exhausted and the response delay increased significantly.

C. MITM ATTACK (DATA INTERCEPTION)

In an actual control system, although the master station and sub-station can be protected by a vertical encryption device, the transmission between the vertical encryption device and master station or sub-station is in clear text. If the attacker is inserted between them, the structure and meaning of the packet can be resolved via long-term learning. Therefore, to simplify the modelling, this paper ignores the impact of vertical encryption devices and assumes that the type of packet can be identified and the content can be modified by the attacker with a known packet definition.

In this scenario, the attacker intercepted the packet sent from master station to the sub-station, which made the sub-station unable to receive the command, thus causing a mis-tripping. Under the normal condition, the sub-station controlled the breaker to cut R2 off at 12.49 s. The overcurrent protection for L1 and L5 was not active because the operating conditions were not met. The bus current and generator speed under a MITM attack with data interception are shown in Figure 11. The attacker filtered the control command sent by the master to the sub-station, which caused the mis-tripping; therefore, the R2 was not cut off by the breaker. The overcurrent protection cut L5 off at 12.74 s and cut L1 off at 15.25 s. The generator G1 is cut off from the power grid, and the output drops to 0, so the generator speed recovers gradually. Generator G3 still supply power to the load, but the over-limit leads to G3 being out of step.

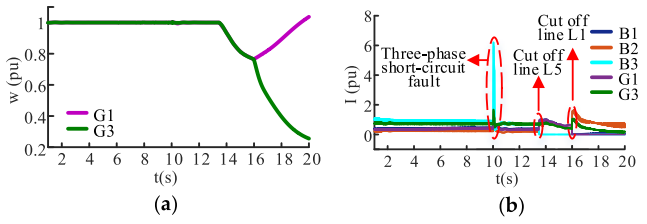

FIGURE 11. Power system status under a MITM attack with data interception: (a) speed of generator, (b) current of bus.

D. MITM ATTACK (DATA MODIFICATION)

In this scenario, the attacker listened to the packet sent by the master station. If the command packet was detected, the attacker subsequently intercepted all packets and sent switching load commands randomly to the sub-station. As shown in Figure 12(a) and (b), the current of B2 and the speed of G3 under a MITM attack are different from the normal condition. The sub-station cut R2 off in the normal condition; therefore, the current of B2 declined and stabilized gradually and the speed of G3 fluctuated only when load shedding. During the attack, the sub-station randomly switched the load, and the current of B2 and the speed of G3 continued to fluctuate sharply. Although the system was not destabilized in this example, disturbances were injected into the system continuously via sub-station malfunctioning, which reduced the stability of the system.

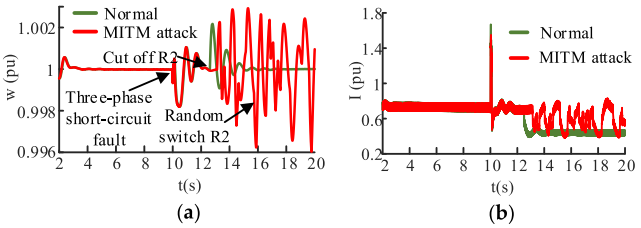

FIGURE 12. Comparison of the power system status under normal conditions and a MITM attack: (a) speed comparison of G3, (b) current comparison of B2.

V. CONCLUSION

In this paper, we have proposed a framework for a cosimulation platform, described the different latencies that affect the system, and discussed the method of modelling the power system, communication system and control device. Compared with a traditional power grid, simulating a CPPS introduces a variety of hardware devices, software programs and communication protocols. The cosimulation platform presented in this paper considers the communication system and the actual device and can analyze the impact of latency, data loss and bit errors in the communication system on the power system and evaluates the response delay, rejecting act and fault operations of the actual device. By allowing the security and stability control system access to cosimulation, this system is able to simulate the generation of cyber-attack and the process of failure propagation.

A cyber physical power system is built with the aforementioned technologies to verify the influence of the communication system. The model contains the typical units in a smart grid, including controllable loads, circuit breakers, generators, protective relays, security and stability control device and comprehensive communication network. Simulations of a DDOS attack and MITM attack were conducted, and the results showed that the system is capable of simulating detailed models with cyber-attacks. The simulation results illustrate that the communication system, actual device and cyber-attack should be considered when performing power system simulations.

The cosimulation platform proposed in this paper is in the early stage of research. The next steps and future directions for this research include the following.

(1) Studying the interface technology and synchronization technology of the cosimulation platform to reduce or even eliminate the inherent latency of the simulation platform to increase the accuracy of the simulation results. (2) Establishing a model to quantify the communication latency. (3) Further applying the cosimulation platform to analyze the generation of a cyber-attack and the process of failure propagation under a CPPS.

REFERENCES

[1] M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, "A survey on smart grid cyber-physical system testbeds," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 446–464, 1st Quart., 2017.

[2] M. Garau, G. Celli, E. Ghiani, F. Pilo, and S. Corti, "Evaluation of smart grid communication technologies with a co-simulation platform," *IEEE Wireless Commun.*, vol. 24, no. 2, pp. 42–49, Apr. 2017.

[3] M. Kuzlu, M. Pipattanasomporn, and S. Rahman, "Communication network requirements for major smart grid applications in HAN, NAN and WAN," *Comput. Netw.*, vol. 67, pp. 74–88, Jul. 2014.

[4] X. Yin, Z. Zhang, Z. Li, X. Qi, W. Cao, and Q. Guo, "The research and the development of the wide area relaying protection based on fault element identification," *Protection Control Mod. Power Syst.*, vol. 1, no. 1, p. 12, Dec. 2016.

[5] D. Wei, Y. Lu, M. Jafari, P. M. Skare, and K. Rohde, "Protecting smart grid automation systems against cyberattacks," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 782–795, Dec. 2011.

[6] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Comput. Netw.*, vol. 57, no. 5, pp. 1344–1371, Apr. 2013.

[7] C.-W. Ten, C.-C. Liu, and M. Govindarasu, "Vulnerability assessment of cybersecurity for SCADA systems using attack trees," in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, Jun. 2007, pp. 1–8.

[8] D. U. Case and A. Center, "Analysis of the cyber attack on the Ukrainian power grid," in *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, 2016.

[9] P. Derler, E. A. Lee, and A. S. Vincentelli, "Modeling cyber–physical systems," *Proc. IEEE*, vol. 100, no. 1, pp. 13–28, Aug. 2011.

[10] Q. Wang, S. Rahman, Y. Tang, Y. Li, M. Pipattanasomporn, and M. Kuzlu, "Framework for vulnerability assessment of communication systems for electric power grids," *IET Gener., Transmiss. Distrib.*, vol. 10, no. 2, pp. 477–486, Feb. 2016.

[11] Y. Tang, Q. Wang, M. Ni, and Y. Xue, "Review on the hybrid simulation methods for power and communication system," *Autom. Electric Power Syst.*, vol. 39, no. 23, pp. 33–42, 2015.

[12] M. S. Hasan, H. Yu, A. Carrington, and T. C. Yang, "Co-simulation of wireless networked control systems over mobile ad hoc network using SIMULINK and OPNET," *IET Commun.*, vol. 3, no. 8, pp. 1297–1310, Aug. 2009.

[13] H. Lin, S. Sambamoorthy, S. Shukla, J. Thorp, and L. Mili, "Power system and communication network co-simulation for smart grid applications," in *Proc. ISGT*, Jan. 2011, pp. 1–6.

[14] V. Liberatore and A. Al-Hammouri, "Smart grid communication and co-simulation," in *Proc. IEEE EnergyTech*, May 2011, pp. 1–5.

[15] K. Mets, J. A. Ojea, and C. Develder, "Combining power and communication network simulation for cost-effective smart grid analysis," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1771–1796, 3rd Quart., 2014.

[16] A. T. Al-Hammouri, M. S. Branicky, and V. Liberatore, "Co-simulation tools for networked control systems," in *Proc. Int. Workshop Hybrid Syst., Comput. Control*, vol. 4981, 2008, pp. 16–29.

[17] W. Li, A. Monti, M. Luo, and R. A. Dougal, "VPNET: A co-simulation framework for analyzing communication channel effects on power systems," in *Proc. IEEE Electr. Ship Technol. Symp.*, Apr. 2011, pp. 143–149.

[18] H. Lin, S. S. Veda, S. S. Shukla, L. Mili, and J. Thorp, "GECO: Global event-driven co-simulation framework for interconnected power system and communication network," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1444–1456, Sep. 2012.

[19] W. Ye, R. T. Vaughan, G. S. Sukhatme, J. Heidemann, D. Estrin, and M. J. Mataric, "Evaluating control strategies for wireless-networked robots using an integrated robot and network simulation," in *Proc. IEEE Int. Conf. Robot. Autom. (ICRA)*, vol. 3, May 2001, pp. 2941–2947.

[20] K. Hopkinson, X. Wang, R. Giovanini, J. Thorp, K. Birman, and D. Coury, "EPOCHS: A platform for agent-based electric power and communication simulation built from commercial Off-the-Shelf components," *IEEE Trans. Power Syst.*, vol. 21, no. 2, pp. 548–558, May 2006.

[21] H. Georg, S. C. Muller, N. Dorsch, C. Rehtanz, and C. Wietfeld, "INSPIRE: Integrated co-simulation of power and ICT systems for real-time evaluation," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Oct. 2013, pp. 576–581.

[22] Y. Tang, Q. Wang, W. Tai, B. Chen, and M. Ni, "Real-time simulation of cyber-physical power system based on OPAL-RT and OPNET," *Autom. Electr. Power Syst.*, vol. 40, no. 23, pp. 15–21, 2016.

[23] B. Chen, K. L. Butler-Purry, A. Goulart, and D. Kundur, "Implementing a real-time cyber-physical system test bed in RTDS and OPNET," in *Proc. North Amer. Power Symp. (NAPS)*, Sep. 2014, pp. 1–6.

[24] Y. Chen, J. Hong, and C.-C. Liu, "Modeling of intrusion and defense for assessment of cyber security at power substations," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2541–2552, Jul. 2018.

[25] Y. Zhang, S. Eisele, A. Dubey, A. Laszka, and A. K. Srivastava, "Cyber-physical simulation platform for security assessment of transactive energy systems," 2019, *arXiv:1903.01520*. [Online]. Available: http://arxiv.org/abs/1903.01520

[26] T. M. Chen, J. C. Sanchez-Aarnoutse, and J. Buford, "Petri net modeling of cyber-physical attacks on smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 741–749, Dec. 2011.

[27] N. Liu, J. Zhang, H. Zhang, and W. Liu, "Security assessment for communication networks of power control systems using attack graph and MCDM," *IEEE Trans. Power Del.*, vol. 25, no. 3, pp. 1492–1500, Jul. 2010.

ZENGJI LIU (Member, IEEE) received the B.E. and M.E. degrees from Southeast University, China, in 2016 and 2019, respectively, where he is currently pursuing the Ph.D. degree. His research interests include cyber-physical power system cosimulation and cyber-attack.

QI WANG (Member, IEEE) received the B.E., M.E., and Ph.D. degrees from Southeast University, China, in 2011, 2013, and 2017, respectively, all in electrical engineering. He conducted research with the Virginia Polytechnic Institute and State University, as a Joint-Training Doctor, in 2014 and 2015, respectively. He joined Southeast University. His research interests include power system stability analysis, and control, and cyber physical power systems.

YI TANG (Senior Member, IEEE) received the B.E., M.E., and Ph.D. degrees from the Harbin Institute of Technology, China, in 2000, 2002, and 2006, respectively. Since 2006, he has been working with the School of Electrical Engineering, Southeast University. He is currently the Director of the Power System Automation Research Institute. His research interests include smart grid, power system security, power system stability analysis, renewable energy systems, and cyber physical systems.