WAPI-based Trusted Access for Smart Grounding Systems in Substations via Cyber-Physical Simulation

Zehui Liu[1], Zhihong Xiao[2], Haoyu Liu[2], Xinru Song[2], Yun Ju[2,*]
[1]Electric Power Research Institute of State Grid Shanxi Electric Power Company, Taiyuan 030001, China
[2]North China Electric Power University, Beijing, China
Corresponding author: Yun Ju (e-mail: 50501482@ncepu.edu.cn).

ABSTRACT As power grids become more digitalized, substation communication networks must offer high bandwidth, low latency, and strong security, which traditional wireless methods cannot provide at the same time. This paper proposes a trustworthy access scheme for power IoT terminals based on WAPI (WLAN Authentication and Privacy Infrastructure) and builds a cyber-physical simulation platform that jointly models the communication and power processes. We compare WAPI with Wi-Fi HaLow, LoRaWAN, and 6LoWPAN. In steady state WAPI keeps packet latency below 5 ms and a packet delivery ratio near 100% under typical load, and it reaches the highest effective throughput among the four. These results indicate that WAPI can support an independent and controllable access system for the power IoT.

INDEX TERMS WAPI, Power Internet of Things, Trusted Terminal Access, Cyber-physical Simulation

I. INTRODUCTION

As power grids undergo digital transformation and smart grids are built out, substations are deploying applications such as robotic inspection, mobile operations, and intelligent equipment monitoring. These applications raise the level of automation, but they also place heavier demands on the communication network in bandwidth, connection density, and mobility[1]. Robotic inspection transmits high-definition video, mobile operations rely on wireless terminals, and intelligent monitoring needs millisecond-level response. Conventional communication methods have trouble meeting all of these at once, so new terminal access solutions are needed.

Conventional communication solutions are not enough. Wired communication is stable but expensive and hard to scale. Public 4G and traditional Wi-Fi are flexible, yet they cover complex environments poorly, have complicated access procedures, and rely on one-way authentication with generic encryption. Three gaps remain in current substation access:

(1) they cannot provide strong security, such as bidirectional authentication and cryptographic protection, against evolving cyber threats;
(2) their real-time performance is limited for delay-sensitive operations such as intelligent grounding wire management; and
(3) they comply poorly with national standards for autonomy and controllability.

In short, there is no wireless protocol that balances security, low latency, and regulatory compliance, which mission-critical power applications require.

WAPI is a wireless security standard. It uses two-way authentication and the SM4 symmetric block cipher approved by the National Cryptography Administration. Compared with traditional Wi-Fi, it provides stronger identity verification and data protection. Applying WAPI to terminal access in the power IoT can improve communication security and help build an independent and controllable access system in line with digitalization and domestic cryptographic standards.

A key question is how applicable WAPI is in the power IoT. Because the requirements span communication efficiency, energy consumption, real-time performance, and reliability, no single indicator captures overall system performance. We therefore built a cyber-physical simulation platform that combines power physical processes with communication networks in one test environment. The platform evaluates throughput, delay, and delivery ratio under realistic operating conditions, which helps identify risks early and provides experimental evidence for engineering deployment.

We use intelligent ground wire management in substations as a representative application. This scenario needs real-time status and location data for ground wires during installation and removal, checked against a misoperation prevention system. Its demands for low latency and high reliability are hard for conventional wireless technologies to meet. We integrated WAPI into the simulation platform and compared it with Wi-Fi HaLow, LoRaWAN, and 6LoWPAN. WAPI gives better effective throughput, packet delay, and delivery

ratio, and its advantages in latency and reliability match what the power IoT needs.

This paper makes four contributions:

(1) it analyzes the communication requirements and security risks of terminal access in the power IoT;
(2) it proposes a WAPI-based trusted access scheme supported by a cyber-physical simulation platform;
(3) it validates WAPI's performance in intelligent ground wire management through comparative experiments with mainstream wireless technologies; and
(4) it shows WAPI's advantages and where it could be applied more broadly.

II. RELATED WORK

Currently, the primary simulation methods employed in power systems include physical simulation and digital simulation[2]. Physical simulation methods involve constructing experimental platforms or scaled-down physical models that are similar to the actual system, and conducting validation and experiments with the aid of sensors, controllers, and actuation units[3]. The fundamental principle of physical simulation is to use real hardware and physical components as the subjects of study, simulating the responses of power terminals under various operating conditions to obtain results that closely approximate actual operation. Physical simulation can intuitively reflect the interactions between devices, test the safety and reliability of the system, and identify potential risks in advance under laboratory conditions, thereby providing valuable references for practical engineering applications. However, physical simulation often requires high construction costs and lacks flexibility. Different physical systems need to be established for two different cases, and scalability is poor [4]. For example, Xie Fuhong et al. [5] proposed a network-based hardware-in-the-loop (HIL) simulation system that integrates OPAL-RT simulators from multiple institutions. Data interaction is achieved through VPN and shared files for large-scale power system simulation. The performance meets the standards, but improvements are needed in synchronous coupling and modeling of more nodes. Pham et al. [6] proposed a real-time cyber-physical power system (CPPS) test platform based on Typhoon HIL, which realizes the measurement of IEC 61850 GOOSE transmission time and meets the requirements of substations. However, there are still shortcomings in the transmission time that can be optimized and the need for in-depth research on communication delay factors. Hosseinzadeh et al. [7] proposed a hybrid cyber-physical test platform (CPT) with an automated level crossing as the physical process. Single-board computers are used to simulate ICS components to achieve OT network security teaching and research. The platform is low-cost and fully functional, but improvements are needed in defense mechanisms and more teaching tests are required. Digital simulation methods involve the use of computer software and mathematical modeling to virtually model and computationally deduce the operational characteristics of power systems [8]. The principle behind this method is to describe the dynamic processes of power equipment and networks using mathematical equations, and to conduct real-time or offline simulations via high-performance computing platforms. Moreover, digital simulation can also facilitate the dynamic study of large-scale power networks, thereby enhancing research efficiency. However, the accuracy and authenticity of digital simulation are heavily dependent on model assumptions. The parameters and precision within the model can significantly affect the simulation outcomes, thereby reducing the credibility of the simulation results[9]. For instance, Verdugo-Cedeño et al. [10] proposed a simulation-based digital twin (SDT) method to realize intelligent services for heavy mobile machinery under the Operator 5.0 framework. This method is divided into two categories: operator-centric and resilient services, which support decision-making and value co-creation. However, it suffers from sample limitations and does not delve into the issues of technical trustworthiness and multi-entity collaboration. Lv et al. [11] proposed a method to construct the metaverse using digital twins (DT), covering a wide range of scales from macro to micro, multiple physical states including solid, liquid, and gas, as well as social relationships, and integrating relevant theoretical support for modeling. However, this approach faces sensor technology bottlenecks, and the implementation of DT for certain physical states and social relationships is highly challenging. With the advancement of information technology, new possibilities have been provided for the development of network simulation systems, which have become mainstream simulation technology solutions[12]. Tang et al. [13] proposed the Mini-Savi satellite network simulation platform, which integrates Mininet, Savi, and Ryu to achieve integrated constellation orbit and network simulation. The platform was verified using the Iridium system, but it did not address the capability for multi-constellation adaptation and complex scenario simulation. Chen et al. [14] proposed a modeling method for power cyber-physical systems and built a simulation platform. They used the Analytic Hierarchy Process (AHP) to evaluate the impact of network attacks and found that the consequences of attacks are more severe under heavy loads. However, the simulation of multiple types of attacks was not covered. Gallegos Ramonet et al. [15] explored network simulation systems for the Internet of Things, based on ns-3, and pointed out the need to optimize the GUI and hardware simulation. However, they did not provide specific optimization implementation plans. Musa et al. [16] analyzed 23 discrete-event network simulation tools, categorically assessed their functions and performance, and concluded that tools such as NS3 and OMNET++ are extensible. However, they did not delve into the co-simulation capabilities between different tools.

In parallel with simulation platform development, substantial progress has been made in the domain of wireless security protocols for power IoT. Alsharbaty and Ali [17]

proposed a smart electrical substation cybersecurity model integrating WPA3 Enterprise with a cooperative hybrid intrusion detection system (CHIDS), demonstrating that even the latest Wi-Fi security standards still rely on pre-shared key or 802.1X-based authentication, which lacks the certificate-based mutual authentication and national cryptographic compliance that WAPI inherently provides. Wang and Liu [18] further investigated the application of WAPI technology in power systems, confirming its suitability for substation wireless networks through its three-element peer-to-peer architecture (AS, AP, STA) and SM4 symmetric encryption. These recent advances highlight a growing consensus on the need for hardware-rooted trust and national-standard cryptographic protocols in critical power infrastructure, yet also underscore that WAPI remains the only solution that simultaneously satisfies bidirectional certificate authentication, low-latency communication, and compliance with China's cryptographic regulations.

III. SECURE ACCESS OF POWER IOT TERMINALS

A. WAPI AUTHENTICATION PROCESS

WAPI (WLAN Authentication and Privacy Infrastructure) technology, namely Wireless LAN Authentication and Privacy Infrastructure, is a wireless security standard proposed by China based on the 802.11 wireless protocol. It consists of two fundamental components: WLAN Authentication Infrastructure (WAI) and WLAN Privacy Infrastructure (WPI). In the context of power systems, ensuring the secure transmission of information between networks is of vital importance. Compared with the one-way authentication of WIFI, the WAPI protocol employs a more secure two-way authentication method, as illustrated in Figure 1.

B. COMPARISON OF WAPI TECHNOLOGY WITH OTHER COMMUNICATION TECHNOLOGIES

The WAPI protocol adopts a two-way authentication mechanism (as shown in Figure 1), which significantly enhances the security during the communication process. Meanwhile, the protocol utilizes cryptographic algorithms approved by the National Cryptography Administration, thereby providing stronger protection in terms of identity authentication and data protection. In contrast, Wi-Fi HaLow is a wireless communication technology launched by the Wi-Fi Alliance for IoT applications. Its strengths lie in supporting long-range and low-power connections, but it may fall short in terms of security compared with WAPI. LoRaWAN_SF7, as a configuration version of the LoRaWAN protocol, is mainly applied in low-power wide-area network (LPWAN) scenarios. It can support large-scale device access and long-range communication, but its security performance is also relatively limited. 6LoWPAN, on the other hand, is a low-power wireless personal area network protocol based on IPv6, suitable for various IoT terminal devices, but its security level is also not comparable to that of WAPI. The comparison between the WAPI protocol and Wi-Fi HaLow, LoRaWAN_SF7, and 6LoWPAN protocols is shown in Table I.

The WAPI authentication process is a rigorous mutual certificate-based authentication designed to ensure the mutual trustworthiness between the wireless terminal and the network. The detailed process is as follows:

1. *Authentication Initiation & Link Connection (Step 1):* The Mobile Terminal(MT) first establishes a basic wireless link connection with the Access Point (AP), preparing the channel for subsequent authentication exchanges.
2. *Certificate Authentication Request Phase (Steps 2&3):* The MT sends a Request to the AP. AP appends its own certificate and signs the entire message, forming an Authentication Request which is forwarded to the Authentication Server (AS).
3. *Certificate Authentication & Response Phase (Steps 4& 5):* The AS, upon receiving the request, first verifies the validity of the MT's certificate (e.g. issued by a trusted authority, within validity period) and also verifies the AP's signature. After successful verification, the AS generates a "Certificate Authentication Response" message, containing the AS's signature on the authentication result, the MT's certificate information, the AP's certificate information, and the access time, etc. This response is first sent back to the AP, which then encapsulates it into an "Access Authentication Response" and forwards it to the MT.
4. *Mutual Private Key Verification Phase (Steps 6–8):* Following successful certificate verification, to ensure that the certificate holders genuinely possess the corresponding private keys, a mutual private key verification is conducted between the MT and the AP. First, the AP generates a random number R1 and sends it to the MT (Private Key Verification Request). The MT signs R1 using its private key and returns the signature (Private Key Verification Response). Similarly, the MT generates a random number R2 and sends it to the AP (Private Key Verification Request), and the AP signs R2 using its private key and returns the signature (Private Key Verification Response). Only after both sides successfully verify the other's signature is the mutual authentication fully completed.
5. *Result Handling:* If all the above steps are successful, the MT is granted access to the network. If any verification fails, the connection is immediately terminated.

C. EVALUATION METRICS

This study aims to verify the applicability of WAPI technology in the scenario of intelligent ground wire management in substations and compare its performance in communication efficiency and security with other communication technologies (such as Wi-Fi HaLow). To this end, the following evaluation metrics are employed to conduct the

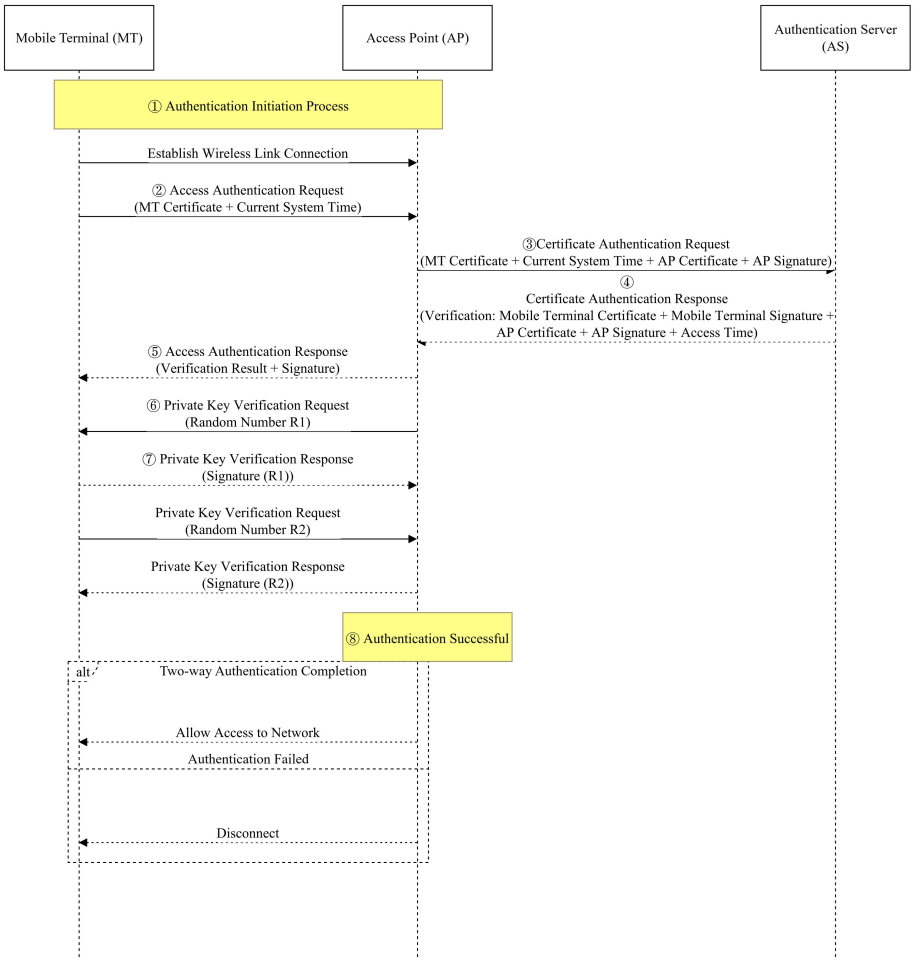

FIGURE 1. The two-way authentication process of the WAPI protocol

TABLE I. Comparison of WAPI protocol with Wi-Fi HaLow, LoRaWAN_SF7, and 6LoWPAN protocols

Feature	WAPI	Wi-Fi HaLow	LoRaWAN_SF7	6LoWPAN
Safety	High, two-way authentication	Medium, using the WPA3 protocol	Low, mainly used for LPWAN	Medium, based on IPv6
Transmission distance	15–50m in typical substation deployment	It can be as far as 1 kilometer	It can be as far as 10 kilometers	10–100m under typical IEEE 802.15.4-based deployment conditions
Power consumption	Medium	Low	Low	Low
Application scenarios	Sensitive fields such as government and finance	Home, office, etc	The Internet of Things, smart cities, etc	Internet of Things devices

performance assessment.

1) GOODPUT

Goodput indicates the amount of successfully received valid data within a unit of time, excluding the bit count of invalid payload such as retransmissions and protocol overhead. It can truly reflect the effective efficiency of network transmission, rather than just the physical layer rate. The calculation formula is shown in Equation (3.1):

$$\text{Goodput} = \frac{B_{\text{succ}}}{T_{\text{total}}}. \tag{3.1}$$

Here, B_{succ} represents the number of successfully received valid bits during the measurement period, in units of bits; T_{total} denotes the total duration of the measurement, in seconds (s).

2) BATTERY LIFETIME

Battery lifetime reflects the duration for which a node can operate under battery power. This metric is closely related to the energy consumption efficiency of the communication protocol and is particularly applicable for evaluating low-power IoT applications. The calculation formula is shown in Equation (3.2):

$$\text{Battery Lifetime (hours)} = \frac{C\ (\text{mAh})}{I_{\text{avg}}\ (\text{mA})}. \tag{3.2}$$

Here, C represents the rated capacity of the battery, in units of mAh; I_{avg} denotes the average current consumption of the device during the standby/communication cycle, in units of mA. The result obtained by dividing the two is in hours (neglecting losses such as discharge efficiency and self-discharge).

For presentation in Figure 4, the calculated battery lifetime is converted from hours to days by dividing by 24.

3) PACKET LATENCY

Packet latency describes the transmission delay of a data packet from the sender to the receiver and is an important metric for measuring communication real-time performance. In industrial scenarios such as substations, low latency is particularly critical for the safety and reliability of the system. The formula for calculating single-packet latency is shown in Equation (3.3), and the formula for sample average latency is shown in Equation (3.4):

$$\text{Packet Latency} = t_{\text{receive}} - t_{\text{send}}. \tag{3.3}$$

$$\overline{L} = \frac{1}{N}\sum_{i=1}^{N}\left(t_{\text{receive},i} - t_{\text{send},i}\right). \tag{3.4}$$

Here, t_{send} and t_{receive} represent the timestamps of packet transmission and reception, respectively, in seconds. $\overline{L}$ denotes the average latency over N packets, in seconds. Packet latency encompasses queuing delay, transmission delay, processing delay, and propagation delay, and is a key metric for assessing communication real-time performance.

The average packet delay $\overline{L}$ in Equation (3.4) refers to the steady-state data transmission delay after successful link establishment and WAPI certificate-based mutual authentication. It does not include the initial authentication handshake or setup time. This definition is adopted because the grounding line status and location packets are periodically transmitted after the terminal has completed network access authentication. The initial setup time is evaluated separately as the authentication delay, rather than being included in the per-packet steady-state transmission delay.

4) PACKET DELIVERY RATIO, PDR

Packet Delivery Ratio (PDR) indicates the proportion of data packets successfully delivered to the receiver among those transmitted, serving as a crucial metric for evaluating network reliability. A higher PDR signifies a more stable communication link. The calculation process is shown in Equation (3.5):

$$\text{PDR}(\%) = \frac{N_{\text{received}}}{N_{\text{sent}}} \times 100\%. \tag{3.5}$$

Here, N_{sent} represents the total number of packets transmitted by the sender during the measurement period(unitless), and N_{received} denotes the number of packets successfully received and verified by the receiver(unitless). And the calculation result is expressed as a percentage (%).

IV. INTRODUCTION TO THE SIMULATION PLATFORM SYSTEM

A. ARCHITECTURE OF THE INFORMATION-PHYSICAL CONVERGENCE SIMULATION PLATFORM

The Information-Physical Convergence Simulation Platform is positioned as a distribution Internet of Things simulation system based on the WAPI protocol for substation user side. It aims to achieve unified modeling and verification of the power physical process and communication network security process.

The overall structure of the platform consists of five core modules: First, the communication network simulation module is based on Mininet and has been modified to support flexible modeling of communication nodes and topologies. It can simulate substation networks, wireless access, and IoT gateway scenarios, thereby reproducing the performance of the distribution Internet of Things under complex communication conditions. Second, the physical information access module realizes the access of static power grid data (such as lines, switches, transformers) and dynamic operation data, providing the basis for the connection between the physical side and the information side. Third, the physical characteristics simulation module relies on GridLAB-D and can carry out power grid process simulations such as power flow, faults, and power quality on a continuous time scale, accurately depicting the physical mechanisms of electricity. Fourth, the information fusion simulation module, as a key hub, integrates data from the communication and physical sides, undertakes access control, interaction processing, and multi-module coordination, and achieves global consistency and real-time performance. Finally, the real-time simulator aggregates information from all modules, performs parallel high-precision calculations, and outputs the operating status and performance indicators of the distribution Internet of Things, providing computational support for experimental verification and application evaluation.

WAPI is embedded in the platform at the WLAN access layer, where it provides mutual authentication and link-layer encryption for simulated terminal access. In a substation IoT setting with many dispersed terminals, this design helps restrict untrusted devices from joining the network and reduces the risk that status or location messages are altered in transit. The simulation data therefore remain traceable and consistent as they are generated, transmitted, and exchanged across modules. This setting allows the platform to evaluate communication performance together with the security conditions required for later deployment in a real system. The platform diagram is shown in Figure 2.

B. MODULE ANALYSIS OF THE INFORMATION-PHYSICAL FUSION SIMULATION PLATFORM

1) COMMUNICATION NETWORK SIMULATION MODULE

The communication network simulation module provides the cyber-side model of the information-physical convergence platform. With WAPI support, the module also rep-

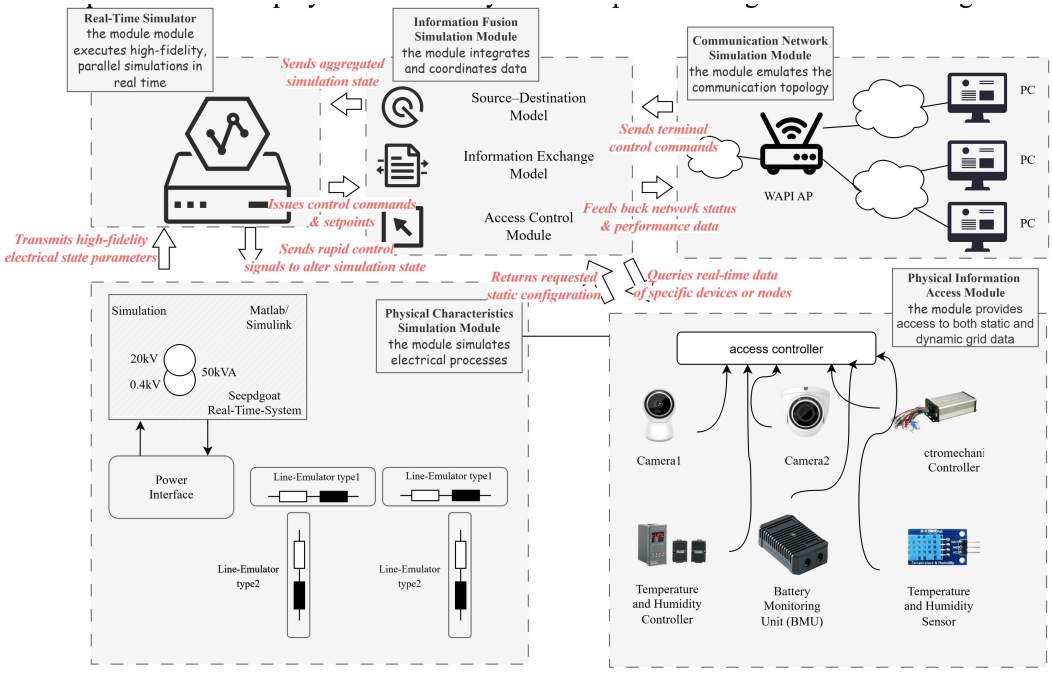

FIGURE 2. Architecture diagram of the cyber-physical fusion simulation platform

resents authentication and encryption during packet transmission, allowing communication performance and access security to be assessed under the same network scenario.

In the implementation, the communication network module extends the standard Mininet node and link configuration logic by adding configurable wireless access parameters, including access node type, terminal number, link bandwidth, packet loss rate, propagation delay, and traffic generation interval. The WAPI access process is abstracted into a trusted association procedure between STA, AP, and AS, and the corresponding authentication delay and key negotiation overhead are mapped into the link-layer access model. Traffic flows are generated according to the reporting behavior of intelligent grounding wire terminals, so that changes in node scale and packet transmission frequency can be reflected in throughput, delay, and packet delivery ratio.

2) PHYSICAL INFORMATION ACCESS MODULE

The physical information access module mainly focuses on the basic data management and access simulation of the power grid, which is a prerequisite for the interaction between the information layer and the physical layer. This module supports the integration of static and dynamic data, including the topological information of power grid equipment such as lines, transformers, and switches, as well as dynamic parameters that change over time, such as operating status and measurement data. Through virtual interfaces, the module can simulate the data acquisition and transmission process of real physical devices, enabling the simulation system to have data characteristics consistent with the actual distribution network. Additionally, it undertakes the tasks of data preprocessing and standardization to ensure that data from different sources can be uniformly invoked.

At this stage, the module acts as the interface between the power-side model and the communication-side model. Static records, including grounding-pile locations, equipment identities, and topology associations, are kept in structured configuration files. Dynamic records, including grounding wire hanging/removal states and terminal reporting events, are refreshed during each simulation iteration. The module then maps each physical event to a communication packet with fields for terminal ID, device location, event type, timestamp, and status value, so that the physical process can drive network traffic generation.

3) PHYSICAL PROPERTY SIMULATION MODULE

The physical characteristics simulation module is responsible for modeling the operating mechanisms and physical processes of the power grid, and it is the core of the platform for reproducing the dynamic characteristics of the power system. Based on the secondary development of GridLAB-D, this module can build simulation models that cover multiple aspects, including power flow calculation, short-circuit analysis, and power quality assessment. During operation, the module can perform real-time calculations of electrical quantities such as voltage, current, and power, and it can demonstrate the dynamic response characteristics of the power grid on a continuous time scale. By introducing external disturbances and changes in operating conditions, it can intuitively reflect the operating behavior of the distribution network under conditions such as faults, load fluctuations, or the integration of new energy sources.

Based on GridLAB-D, the physical property simulation

module mainly modifies the model configuration and data output interface rather than the internal power-flow solver. The grounding wire management process is represented by discrete state variables associated with corresponding substation equipment nodes. During each simulation step, the module updates the physical state of the target equipment and exports the resulting status data to the information fusion module through a unified data interface, providing the physical basis for subsequent communication and control evaluation.

4) INFORMATION FUSION SIMULATION MODULE

The information fusion simulation module is at the intersection of the communication and physical systems, responsible for the integration, transmission, and interaction of information from different sources. It is the core hub for the coordinated operation of multiple modules. This module can parse the power data generated by the physical information access module and simultaneously receive the network status information passed from the communication network simulation module. Based on this, it achieves bidirectional interaction and dynamic updating of data. Its functions are not limited to data transmission but also include access control and verification of security policies to ensure the integrity and consistency of cross-module information transmission. With the help of this module, the platform can coordinate the power grid status and communication status in a unified environment, thereby achieving the mapping of real-world scenarios.

In this platform, the interaction between GridLAB-D and the communication network simulation module is organized through step-based data exchange rather than continuous strong coupling. The information fusion module uses timestamps and temporary data buffers to align the physical-state updates generated by GridLAB-D with the communication-side message transmission results at each predefined exchange interval.

5) REAL-TIME SIMULATOR

The real-time simulator is the core execution environment of the entire information-physical convergence platform, undertaking the tasks of multi-module data aggregation and real-time computation. By interfacing with the physical information, physical characteristics, and communication network simulation modules, it integrates input data from different dimensions into the simulation computation framework. During operation, the real-time simulator can process large-scale computation tasks in parallel, ensuring that the system achieves response on a millisecond or even shorter time scale to meet the strict real-time requirements for Power IoT research. Its output results not only include the operating status parameters of the distribution network but also communication performance indicators and security validation results, providing researchers with comprehensive references.

The real-time simulator controls the execution order of different modules by using an iteration-based scheduling mechanism. In each iteration, the physical module first updates the equipment state, the information access module then generates corresponding terminal reporting events, the communication module simulates packet transmission, and the information fusion module finally records the interaction results. This scheduling logic ensures that the cyber-side communication process and the physical-side state evolution are evaluated under the same simulation scenario.

C. SIMULATION SETUP AND PARAMETER CONFIGURATION

The simulations ran on a server with an Intel Xeon Gold 6248 processor (24 cores, 2.5 GHz), 128 GB DDR4 memory, and 1 TB SSD storage. The test scene was a typical 220 kV outdoor substation. The communication area covered the main equipment zone. Thirty intelligent grounding wire modules (STAs) were placed at grounding piles in the 10 kV switch room, main transformer area, and outdoor capacitor grounding transformer area. Each module reported grounding wire status and location every 5 s. Eight WAPI APs were placed based on equipment density. The data sampling interval was 1 ms.

The simulation was repeated 10 times. Each run represented 2 h of simulated system operation. In each run, the terminals uploaded status and location data at the set reporting interval. For each metric, the mean value, standard deviation, and 95% confidence interval were calculated from the repeated simulation results. Statistical significance among different communication technologies was examined using one-way ANOVA when the assumptions of normality and homogeneity of variance were satisfied; otherwise, the Kruskal-Wallis non-parametric test was adopted. The significance level was set to $p < 0.05$. This procedure was used to quantify result uncertainty and improve the reliability of the comparative analysis.

Background noise in the station was set to -85 dBm, the preset packet loss rate was 0.1% to 0.5%, and terminal mobility was not considered at this stage. WAPI was configured according to GB 15629.11-2022 with national cryptographic SM4 encryption enabled; Wi-Fi HaLow followed IEEE 802.11ah with WPA3 encryption; LoRaWAN-SF7 followed LoRa Alliance v1.0.3 with spreading factor 7; and 6LoWPAN followed RFC 4944 with IPsec encryption. The channel bandwidth was set to 2 MHz for all four technologies to support a consistent comparison.

V. APPLICATION SCENARIO DEMONSTRATION

A. APPLICATION AND TESTING

To meet the strict requirements of the power industry for the security, real-time performance, and reliability of wireless networks, especially in the scenario of state collection and error-prevention control for intelligent grounding wire management in substations, a power wireless network system based on the WAPI ternary security architecture design, as

shown in Figure 3, has been constructed on the information-physical convergence simulation platform. By deploying core equipment in a hierarchical and distributed manner, a secure communication network covering three levels—Shanxi Province, cities, and substations—has been built, enabling trusted access of wireless terminals to the network and secure data transmission. This networking architecture takes the authentication server, access controller, wireless access point, and intelligent grounding wire module as its core components. The devices at each level work together to support core services such as real-time collection of grounding wire status and error-prevention verification.

AS acting as the security trust root of the entire networking architecture, is deployed uniformly at the provincial company level in Shanxi. It is configured with primary and secondary devices to ensure system redundancy and prevent security authentication interruptions caused by single-point failures. Based on a bidirectional authentication mechanism and public-key cryptography, the AS is responsible for the full-life-cycle management of digital certificates, including issuance, validity verification, and revocation. All wireless communication terminals and Wireless Access Points (APs) must be pre-configured with unique public-key certificates issued by the AS as their digital identity credentials. When a STA attempts to connect to an AP, it must first trigger a bidirectional identity verification of both by the AS. After receiving the access authentication request from the STA, the AP attaches its own certificate and submits it to the AS. The AS checks the validity of both certificates and then provides feedback. Only when both pass the authentication can they proceed to the subsequent communication process, fundamentally eliminating the risk of unauthorized device access.

The AC, as the core node for network access control and data aggregation, adopts a tiered deployment strategy to meet the needs of different power scenarios: for ultra-high-voltage and extra-high-voltage substations, one set of AC is independently deployed per station; for municipal companies, one set of AC is deployed per centralized control station, with a single AC capable of managing up to 2,048 APs, thus meeting the needs of large-scale networking.

The AP is the key access device for achieving full wireless signal coverage within substations. It is installed on walls or poles in areas where grounding stakes are located, including equipment areas of various voltage levels, 10kV switch rooms, main transformer areas, and outdoor capacitor grounding transformer areas. The signal coverage radius of a single AP is 15–20m. Multiple APs are deployed in coordination to ensure that all grounding stakes that need to be monitored within the station are within the signal coverage area. The AP is connected to a POE switch, which not only supplies power to it through POE technology but also enables wired data transmission with the AC. Its main function is to provide a wireless access interface for the intelligent grounding wire module, receive data such as the status and location information of the grounding wire from the module, and send upper-layer instructions (such as unlock commands) to the terminal. It also encrypts the transmitted data based on the WAPI protocol to ensure the security of over-the-air communication.

The intelligent grounding wire module, acting as the terminal STA, is the direct connection unit between the networking architecture and the grounding wire management business. It consists of a detachable grounding head module and a grounding pile module: The grounding head module is installed on the temporary grounding wire itself, responsible for defining the unique identity code of the grounding wire, collecting the status of the grounding wire's hanging and removal, and communicating with the AP through the WAPI network. The grounding pile module is installed on the on-site grounding pile, defining the identity code of the grounding pile, confirming the location of the grounding wire connection point, and featuring grounding end status detection.

The data uploaded by the module is aggregated by the AP to the AC, then crosses the reverse physical isolation device through the front-end server using the UDP (User Datagram Protocol) and CIM/E (Common Information Model / Efficient, an IEC 61970-based power system data exchange format) to interact with the intelligent error-prevention host in Zone I of the production control area, which complies with IEC 61850 (International Electrotechnical Commission 61850, Communication networks and systems for power utility automation) in Zone I of the production control area. This process realizes the conversion of the grounding wire status from virtual telemetry to real telemetry, providing real-time data support for error-prevention operation verification.

To evaluate the performance of different communication technologies, this paper analyzes four key metrics: Goodput, Battery lifetime, Packet latency, and Packet delivery ratio. The rated battery capacity C in Equation (3.2) was set to 2000mAh for each terminal node. The same battery capacity was used for WAPI, Wi-Fi HaLow, LoRaWAN-SF7, and 6LoWPAN to ensure a fair comparison. The results are shown in Figure 4. In terms of goodput, the proposed method achieved the highest value, with Wi-Fi HaLow being close. The throughput of LoRaWAN-SF7 was at a medium level. This indicates that the proposed method can maintain a competitive goodput with mainstream communication methods such as Wi-Fi HaLow and 6LoWPAN. Regarding packet latency, the proposed method in this paper leads other technologies with extremely low latency, while LoRaWAN-SF7 has much higher latency. 6LoWPAN maintains a low latency (about 10 ms) similar to the proposed method. This shows that, compared with LoRaWAN-SF7 and Wi-Fi HaLow, the proposed method is more suitable for delay-sensitive application scenarios. Although 6LoWPAN also shows low latency, it does not provide the same integrated trusted-access capability as WAPI. Moreover, in terms of packet delivery ratio, the delivery ratio of the proposed method is close to 100%, while that of LoRaWAN-SF7

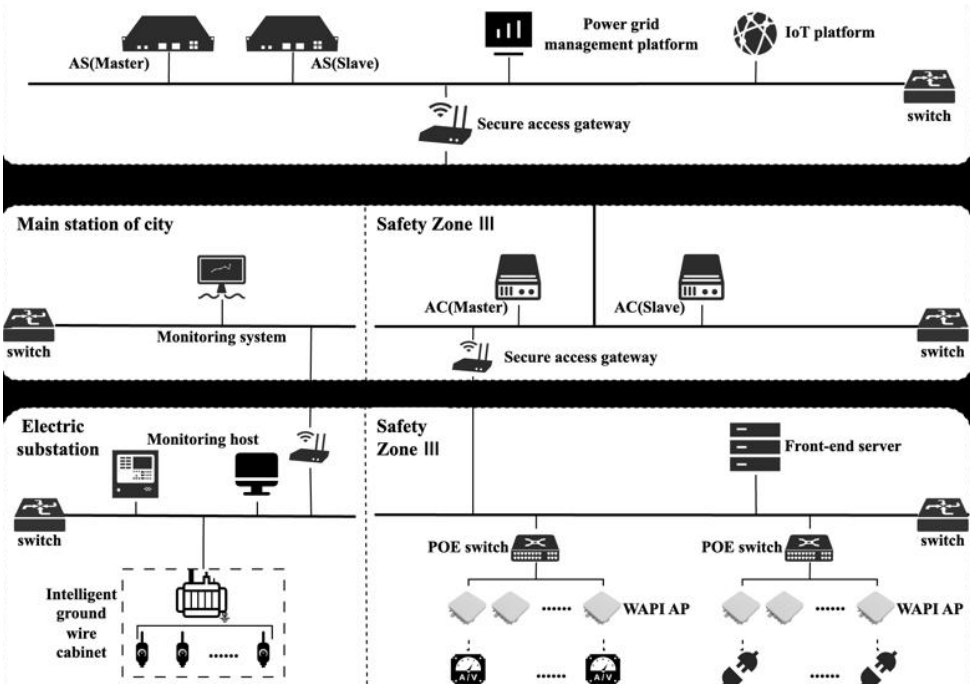

FIGURE 3. System architecture

is relatively low. In summary, the proposed technology has achieved a good balance in goodput, packet latency, and packet delivery ratio, and can effectively meet the requirements of low latency and high delivery ratio for the Power IoT.

To explore the impact of the number of sensors on communication performance, two key metrics, packet delivery ratio and packet latency, were analyzed. The results are shown in Figure 5. In terms of packet delivery ratio, 6LoWPAN demonstrated extremely strong stability. Its delivery ratio remained almost at 100% with little attenuation as the number of sensors increased from 200 to 600. The delivery ratio of the proposed method, though showing a downward trend, still maintained a high level, slowly decreasing from about 97% to about 88%. This decrease is mainly caused by the increased channel contention and packet collision probability under high-density sensor access. Although WAPI introduces additional authentication and encryption overhead, the packet delivery ratio remains at an acceptable level, indicating that the proposed method still maintains relatively stable reliability under heavy-load access conditions. The delivery ratios of Wi-Fi HaLow and LoRaWAN-SF7 decreased more significantly, with their reliability in multi-sensor scenarios decreasing markedly as the number of nodes increased. Regarding packet latency, the proposed method maintained a latency below 5 ms throughout the test, showing excellent low-latency characteristics. The latency of 6LoWPAN slowly increased from about 5 ms to about 20 ms, with a gentle increase. The latency performance of Wi-Fi HaLow showed a phased characteristic. When the number of sensors was less than 400, the latency was stable at about 40 ms. After the number of sensors exceeded 400, the latency increased rapidly, eventually reaching about 125 ms. The latency of LoRaWAN-SF7 was always at the highest level, indicating that it has inherent limitations in latency control. In summary, although 6LoWPAN showed the best stability in packet delivery ratio, the proposed method achieved a good balance between low latency and high delivery ratio.

B. SECURITY ANALYSIS AND EVALUATION

This section evaluates the security of WAPI-based terminal access in the Power IoT scenario. The analysis starts from the threats faced by intelligent grounding wire communication, then relates these threats to the authentication and encryption mechanisms of WAPI. Quantitative indicators are also introduced to support the discussion of secure and trusted access.

WAPI deals with these risks through certificate-based mutual authentication and link-layer encryption. In this access procedure, the first security boundary is placed before service data transmission rather than after a wireless link is trusted. As illustrated in Figure 1, both the Mobile Terminal (MT) and the Access Point (AP) present digital certificates issued by the Authentication Server (AS), so access decisions rely on verifiable device identities instead of mere link availability. The timestamp carried in the authentication exchange ensures request freshness; an outdated or replayed authentication message can therefore be discarded before establishing access. For the grounding-wire scenario, this

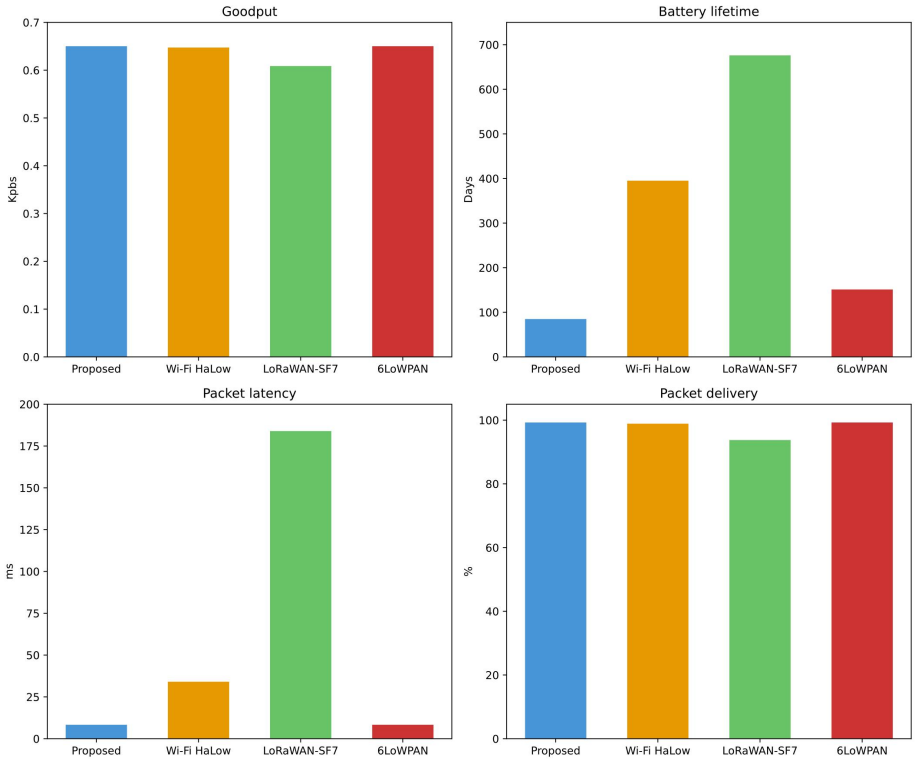

FIGURE 4. Comparison of simulation results

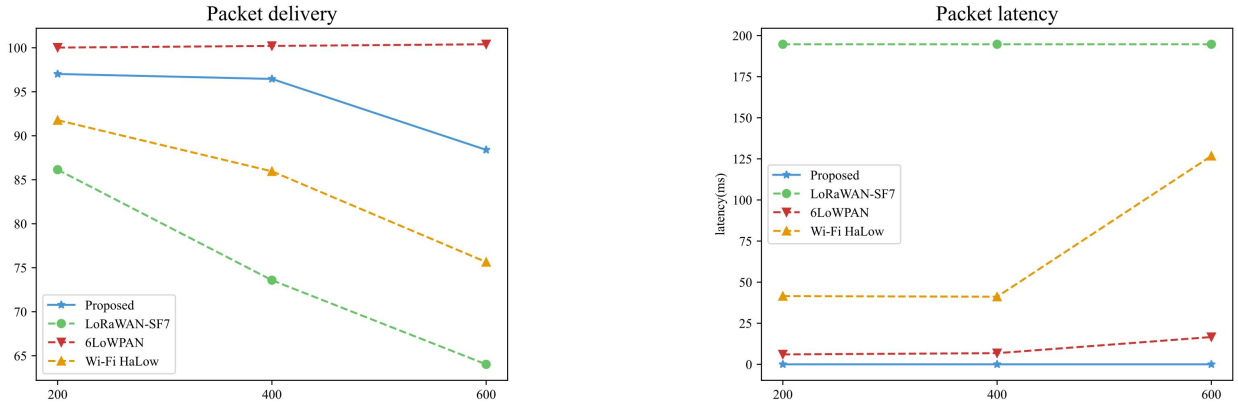

FIGURE 5. Simulation results under different numbers of sensors

TABLE II. Comparison of Quantitative Security Metrics

Security Metric	WAPI	WPA2-Enterprise
Auth. Latency (Initial)	45.2 ± 3.1 ms	38.5 ± 2.8 ms
Key Renewal Frequency	Per session / 30 min (Mandatory)	Implementation-dependent (Usually longer)
Authentication Basis	Digital Certificate (Asymmetric Crypto)	Pre-shared Key (PSK) or 802.1X
Encryption Mandatory	Mandatory End-to-End (SM4)	Optional (Mandatory in WPA3)

means status and location packets are not accepted as ordinary telemetry until the terminal and the access network pass mutual identity verification.

After mutual authentication, focus shifts from identity

TABLE III. Quantified security capability coverage

Security capability	WAPI	Wi-Fi HaLow	LoRaWAN	6LoWPAN
Mutual authentication	1	1	1	1
Link-layer encryption	1	1	1	1
Dynamic key negotiation	1	1	1	1
Centralized authentication management	1	1	1	0.5
Replay protection	1	0.5	1	1
Identity spoofing resistance	1	0.5	0.5	1
Integrated trusted access control	1	0.5	0.5	1
Coverage ratio	100%	78.6%	85.7%	92.8%

admission to protecting packets on the wireless link. In the grounding-wire application, these packets carry status and location data for the misoperation-prevention system. Thus, a valid terminal identity is insufficient if subsequent messages remain vulnerable to interception or modification. WAPI handles this stage via its WPI. This design restricts three local attack paths: passive interception of grounding-wire telemetry, modification of status or location fields, and post-access man-in-the-middle attacks. However, this protection incurs costs. Certificate processing, key negotiation, and SM4 encryption add processing and communication overheads, which must be included in the trusted-access budget during performance evaluation. Therefore, the following tests separate access protection costs from steady-state packet transmissions. At the system level, primary and backup centralized ASs reduce authentication interruptions when access requests surge or a single AS fails.

To test the security cost of WAPI, key authentication and protection metrics were measured on the simulation platform described in Section 4. The results were compared with WPA2-Enterprise. In this test, 100 terminals accessed the network at the same time. The results are shown in Table II.

The authentication latency in Table II represents a simulation-based access delay rather than a hardware benchmark. Although the cyber-physical platform in Section 4.3 ran on an Intel Xeon Gold 6248 server, this server merely provided the simulation environment and does not reflect an STA's computing capability. The access model treats each STA as an embedded wireless terminal, using terminal-side processing-delay parameters to represent the time needed for WAPI certificate parsing, signature verification, and key negotiation.

Consequently, the comparison with WPA2-Enterprise mainly reflects the initial access security cost. WAPI shows a longer authentication delay because it requires certificate-based identity verification and mandatory key negotiation before data transmission. This extra delay differs from the steady-state packet latency in Section 3.3.3. It is an upfront cost paid before periodically uploading grounding-wire status packets. For intelligent grounding wire management, this cost is acceptable since it blocks unauthenticated terminals from the substation wireless network and secures subsequent status and location messages via SM4-based link encryption. Ultimately, WAPI's security value is less about reducing initial access delay and more about establishing a controllable trust boundary for Power IoT terminals under the tested 100-terminal access condition.

To align the security evaluation with the communication technologies examined in this paper, the security mechanisms of WAPI, Wi-Fi HaLow, LoRaWAN, and 6LoWPAN are compared in terms of mutual authentication, link-layer encryption, dynamic key negotiation, centralized authentication management, replay protection, identity spoofing resistance, and trusted access control. A value of 1 indicates that the capability is natively supported by the protocol or the corresponding standard security architecture. A value of 0.5 indicates that the capability is achievable but depends on specific deployment configurations or auxiliary mechanisms. A value of 0 indicates that the capability is not defined by the protocol itself and relies on upper-layer or external security mechanisms.

As shown in Table III, WAPI provides complete coverage of the selected security capabilities because its security framework integrates certificate-based mutual authentication, dynamic key management, mandatory link-layer encryption, and centralized authentication server support. LoRaWAN also provides a relatively complete security architecture, especially in terms of session key generation, frame-counter-based replay protection, and network access control. However, its security design is mainly oriented toward low-power wide-area communication and does not provide the same type of link-layer trusted access control for local power IoT access networks as WAPI. Wi-Fi HaLow can achieve strong security when enterprise-level authentication mechanisms are deployed, but its actual protection level is dependent on the selected WPA security mode and deployment configuration. 6LoWPAN, by contrast, mainly provides IPv6 adaptation for low-power wireless networks, and its security protection generally depends on IEEE 802.15.4 security, DTLS, IPsec, or other upper-layer mechanisms. Therefore, WAPI shows stronger integrated security support for trusted terminal access and centralized authentication in power IoT scenarios.

VI. CONCLUSION

This paper examined WAPI-based trusted access for Power IoT terminals, with intelligent grounding wire management in substations used as the representative scenario. To reflect the coupled requirements of secure access, low latency,

and reliable status reporting, a cyber-physical simulation platform was built to link the communication process with the power-side operating process. The comparative results show that WAPI achieved better effective throughput, packet delivery ratio, and transmission delay than Wi-Fi HaLow and LoRaWAN under the tested conditions. Together with its certificate-based authentication and SM4-enabled link protection, these results indicate that WAPI can support the combined security and performance requirements of substation terminal access. The proposed scheme therefore provides a practical basis for constructing an independent and controllable wireless access system for Power IoT applications.

However, when in high-mobility tasks, such as robotic inspection, WAPI's certificate-based re-authentication may add latency during AP transitions. Pre-authentication and fast-roaming extensions should be evaluated to maintain secure session continuity under terminal mobility. For resource-constrained field sensors, the computational cost of SM2/SM4 operations also needs further optimization, for example through lightweight hardware acceleration or pre-computation. In addition, long-distance coverage may require a tiered hybrid architecture in which WAPI provides secure last-hop access inside the substation, while LoRaWAN or 4G/5G backhaul supports wide-area interconnection. These directions would extend the present simulation work from protocol-level feasibility toward deployment-oriented validation.

ACKNOWLEDGEMENTS

Financial support from the State Grid Corporation of China Science and Technology Project (No. SGSXDK00HLJS2500142) is gratefully acknowledged.

REFERENCES

[1] J. Y. Wen, G. D. Xu, B. Z. Qi, et al., "Implementation and application of intelligent operation and maintenance scenarios in substations based on WAPI networks," *Electric Power Information and Communication Technology*, vol. 22, no. 12, pp. 83–89, 2024.

[2] H. Fan, H. Wang, S. Xia, X. Li, P. Xu, and Y. Gao, "Review of Modeling and Simulation Methods for Cyber Physical Power System," *Frontiers in Energy Research*, vol. 9, 2021.

[3] H. Fagcang, R. Stobart, and T. Steffen, "A review of component-in-the-loop: Cyber-physical experiments for rapid system development and integration," *Advances in Mechanical Engineering*, vol. 14, no. 8, Art. no. 16878132221109969, 2022.

[4] R. Almutairi, G. Bergami, and G. Morgan, "Advancements and Challenges in IoT Simulators: A Comprehensive Review," *Sensors*, vol. 24, no. 5, Art. no. 1511, 2024.

[5] F. Xie, C. McEntee, M. Zhang, N. Lu, X. Ke, M. R. Vallem, et al., Eds., "Networked HIL Simulation System for Modeling Large-scale Power Systems," in *2020 52nd North American Power Symposium (NAPS)*, Apr. 11–13, 2021.

[6] L. N. H. Pham, V. Rosero-Morillo, A. Shukla, F. Gonzalez-Longatt, and V. Meza-G, "Real-Time Cyber–Physical Power System Testbed for International Electrotechnical Commission 61850 Generic Object-Oriented Substation Event Transfer Time Measurements," *Engineering Proceedings*, vol. 77, no. 1, Art. no. 17, 2024.

[7] S. Hosseinzadeh, D. Voutos, D. Barrie, N. Owoh, M. Ashawa, and A. Shahrabi, "Design and Development Considerations of a Cyber Physical Testbed for Operational Technology Research and Education," *Sensors*, vol. 24, no. 12, Art. no. 3923, 2024.

[8] B. Barać, M. Krpan, T. Capuder, and I. Kuzle, "Modeling and Initialization of a Virtual Synchronous Machine for Power System Fundamental Frequency Simulations," *IEEE Access*, vol. 9, pp. 160116–160134, 2021.

[9] F. S. Prol, M. Z. H. Bhuiyan, S. Kaasalainen, E. S. Lohan, J. Praks, K. Çelikbilek, et al., "Simulations of Dedicated LEO-PNT Systems for Precise Point Positioning: Methodology, Parameter Analysis, and Accuracy Evaluation," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 60, no. 5, pp. 6499–6516, 2024.

[10] M. Verdugo-Cedeño, S. Jaiswal, V. Ojanen, L. Hannola, and A. Mikkola, "Simulation-Based Digital Twins Enabling Smart Services for Machine Operations: An Industry 5.0 Approach," *International Journal of Human–Computer Interaction*, vol. 40, no. 20, pp. 6327–6343, 2024.

[11] Z. Lv, S. Xie, Y. Li, M. S. Hossain, and A. El Saddik, "Building the metaverse using digital twins at all scales, states, and relations," *Virtual Reality & Intelligent Hardware*, vol. 4, no. 6, pp. 459–470, 2022.

[12] C. Huang, S. Fang, H. Wu, Y. Wang, and Y. Yang, "Low-altitude intelligent transportation: System architecture, infrastructure, and key technologies," *Journal of Industrial Information Integration*, vol. 42, Art. no. 100694, 2024.

[13] Z. Tang, J. Zhao, H. Li, T. Guo, Q. Wang, H. Chen, et al., Eds., "MiniSavi: Realistic Satellite Network Simulation Platform Based on Open-Source Tools," in *2023 Fourth International Conference on Frontiers of Computers and Communication Engineering (FCCE)*, Jan. 7–9, 2023.

[14] C. Chen, K. Shi, Y. Xiao, F. Tang, and L. Gong, "Power Network Vulnerability Assessment Based on Electric Power System Cyber Security Simulation Platform," *Journal of Physics: Conference Series*, vol. 2785, no. 1, Art. no. 012094, 2024.

[15] A. Gallegos Ramonet, T. Pecorella, B. Picano, and K. Kinoshita, "Perspectives on IoT-oriented network simulation systems," *Computer Networks*, vol. 253, Art. no. 110749, 2024.

[16] A. Musa and I. Awan, "Functional and Performance Analysis of Discrete Event Network Simulation Tools," *Simulation Modelling Practice and Theory*, vol. 116, Art. no. 102470, 2022.

[17] F. S. Alsharbaty and Q. I. Ali, "Smart Electrical Substation Cybersecurity Model Based on WPA3 and Cooperative Hybrid Intrusion Detection System (CHIDS)," *Smart Grids and Sustainable Energy*, vol. 9, no. 1, Art. no. 11, 2024.

[18] X. Wang and R. Liu, "Research and Application of WAPI Technology Based on Power Systems," in *Proceedings of the 2024 International Conference on Power Electronics and Artificial Intelligence*, Xiamen, China: Association for Computing Machinery, 2024, pp. 224–229.