Research on the Network Architecture of Secure Power Wireless Local Area Network Based on WAPI and SDN

Feiyang Li[1], Min Guo[1], Zehui Liu[1], 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 In smart-grid WLANs, a terminal is not fully secured once it has merely passed wireless access authentication. The more difficult part is how the authentication result is carried forward into service isolation, forwarding control, bandwidth allocation, and security operation. In many conventional WLAN deployments, these functions are configured in separate systems, so terminals for distribution automation, electricity information collection, inspection robots, and other power services may still depend on similar access and management policies. This separation also makes burst traffic and O&M fault tracing harder to handle. To deal with this coupling problem, this study designs a secure power WLAN architecture that combines Wireless Local Area Network Authentication and Privacy Infrastructure (WAPI) with Software-Defined Networking (SDN). WAPI provides public-key-based two-way authentication, while SDN supplies centralized control through control-forwarding separation. In the architecture, the SDN controller manages WAPI servers, AP rules, and network resources together. Security domains and service domains are isolated by VLANs, and OpenFlow-supported WAPI-APs are used in the data layer to keep authenticated access, encrypted transmission, and flexible forwarding under the same control logic. A security-resource linkage module maps WAPI authentication results to SDN resource policies, so trusted power terminals can obtain service-specific access permissions and bandwidth guarantees. For typical power scenarios, differentiated WAPI policies and a "detection-alarm-disposal" monitoring loop are also introduced. The experimental results show end-to-end latency below 5 ms, throughput above 93%, and packet loss below 7%; unauthorized access alarms are reduced by 94.8% after WAPI-based protection is enabled. These results suggest that using WAPI authentication semantics as an input to SDN policy control can improve both access security and operational manageability in power WLANs.

INDEX TERMS WAPI, SDN, WLAN, network architecture

I. INTRODUCTION

IN the "source-grid-load-storage" interaction model, field terminals are no longer simple reporting nodes connected to a dispatching center. They take part in local sensing, mobile inspection, metering collection, and control-related data exchange, often under changing load and movement conditions. For this reason, Wireless Local Area Networks (WLANs) [1] have been introduced into several power IoT links, such as distribution terminal communication, electricity information collection, inspection robot data transmission, and substation local monitoring. In other words, access security and network scheduling cannot be treated as two independent tasks. WAPI, as defined in the GB15629.11 series, provides public-key-based two-way authentication and dynamic key management, which are more suitable for trusted terminal access than traditional WEP/WPA-style mechanisms.

SDN addresses a different part of the same problem: by separating the control plane from the forwarding plane, it allows topology adjustment, path selection, and resource allocation to be handled by a centralized controller rather than by isolated AP configurations. Their integration is expected to break power WLANs' current security and management bottlenecks, becoming vital for building highly secure, reliable power wireless systems. Current power WLAN technical applications face three core issues limiting their use in key business scenarios [2]. First, security mechanisms poorly adapt to business needs: Traditional WLANs mostly use preshared key (PSK) authentication or standalone WAPI without linking to network management. Although WAPI can verify the identity of an accessing terminal, authentication alone does not determine how the terminal should be treated after access. In many deployments, passing authentication is only treated as an access result. It is not always used to decide which service domain the terminal should enter, what security level it should have, or what

operations it is allowed to perform. Because of this, a distribution automation terminal may still stay close to ordinary office terminals in terms of wireless channel use and management policy. For power services, this is a weak point: the boundary between high-security control traffic and general data traffic becomes unclear. The problem is even harder in distributed WLANs, where each AP is configured and checked more or less separately. If one AP is compromised, operators may not quickly know which domain is affected, where the abnormal flows are going, or how to isolate the risk in time [3]. The same separation also hurts real-time service control. Power traffic changes a lot in practice. Electricity information collection may rise by 3–5 times during peak periods, and inspection robots may move across different APs while transmitting data [4]. O&M faces a similar fragmentation problem. In many power companies, WAPI, firewalls, topology monitoring, and traffic statistics are deployed as separate tools [5]. A failed authentication event is therefore not naturally linked with AP configuration or link status. Operators often have to check certificates, AP settings, and wireless link conditions in different systems before they can locate the cause. This workflow is workable, but it is slow and not suitable for fast recovery in power communication services. The resulting mean time to repair may reach 4–6 h, which is difficult to reconcile with the rapid recovery requirement of power communication services [6]. Moreover, growing power IoT terminals (over 500 in some substations) raise traditional WLANs' AP management costs linearly, making unified security policy deployment hard and reducing O&M standardization.

To address these issues, this paper focuses on security-management coordinated optimization, researching WAPI-SDN-based secure power WLAN networking architectures to break traditional bottlenecks via tech integration. Research includes two parts: First, building a deeply integrated WAPI-SDN power WLAN architecture. The control layer deploys an SDN controller with security policy parsing, centrally managing WAPI servers, AP rules, and resources. The data layer uses OpenFlow-supported WAPI-APs for encrypted, flexible data transmission. The controller logically isolates security and business domains: the former handles authentication, key management, and attack detection; the latter uses virtual networks (VLANs) for different power services. A security-resource linkage module uses WAPI results for SDN resource allocation, WAPI-authenticated distribution terminals access high-priority domains with exclusive bandwidth, enabling architectural-level security-management coordination. Second, developing a WAPI-based power security solution. It designs differentiated WAPI policies for scenarios like distribution automation, information collection, and inspection robots, matching security mechanisms to each. Some scenarios link SDN to optimize network switching, ensuring data security and continuity. A WAPI security monitoring submodule collects real-time indicators (authentication success rate, abnormal access) and connects to the power dispatching system via SDN. Detected attacks trigger rapid protection, forming a "detection-alarm-disposal" closed-loop to support stable WLAN operation. Power WLAN in smart grid environments is not only a connectivity layer, but also a coupling point of authentication, service scheduling, and operational maintenance.

II. RELATED WORK

A. SDN DIFFERENTIATED ACCESS AND BANDWIDTH GUARANTEE TECHNOLOGY BASED ON WAPI AUTHENTICATION

For power WLANs, access security alone is not enough. After a terminal is admitted, the network still needs to decide where the terminal should be placed, how its traffic should be forwarded, and what service guarantee it should receive. This is why WAPI-SDN integration is discussed in recent work: WAPI helps with trusted access, while SDN gives the network a programmable way to control service assurance [7]. The problem is that many existing solutions still leave authentication, orchestration, and resource scheduling as separate steps, instead of making them one continuous control chain.

Centralized wireless control has already shown its value in this direction. In power-oriented programmable wireless scenarios, the Odin-based prototype uses virtual access points to maintain uninterrupted access and support centralized orchestration [8]. In other words, Odin improves access continuity, but it does not yet make authentication identity directly drive resource policy.

Another group of studies examines the controller architecture itself. Enterprise-level programmable wireless systems usually emphasize logical centralization with physical distribution, and their discussions of controller security threats, mitigation strategies, and multi-controller coordination are important for building a reliable control plane. Such work, however, mainly establishes the control and security baseline of the controller system. It does not fully describe how identity attributes or trust states should be inserted into slices, forwarding rules, or queue configurations after a terminal is admitted.

A related direction concerns authentication infrastructure management. The SDN-based authentication solution using YANG and NETCONF provides unified orchestration of peer relationships, keys, and domain-based routing among authentication nodes [9]. Its active and passive configuration modes support dynamic routing and security-association management, and its scalability has been examined in both star and mesh topologies. This contribution is closer to the authentication layer than to the service-assurance layer: it improves the manageability of authentication nodes, but it does not convert access-layer authentication outcomes into data-plane scheduling decisions.

WAPI deployment studies further confirm that certificate-based wireless access is suitable for high-security industrial environments. In critical infrastructure and smart factory

scenarios, WAPI's mandatory two-way certificate authentication, support for local and offline certificate systems, and consistent access control across heterogeneous terminals have been shown to match industry security requirements better than generic public-facing wireless mechanisms [10]. This evidence supports the use of WAPI in power WLANs, but most comparisons still stop at protocol security or access control. They do not close the loop between WAPI certificate status and controller-side orchestration.

Taken together, prior studies have established several necessary foundations: resilient programmable wireless access, centralized controller and authentication-system orchestration, and engineering deployment paths for secure wireless protocols in industrial scenarios [11]. What remains insufficient is the mechanism that carries identity and trust information across these layers and turns it into executable resource policies. However, the field still lacks systematic technical methods for injecting WAPI certificate attributes and session states (including device categories, trust levels, threat detection results, etc.) into SDN controller policy engines. A fully closed-loop mechanism directly driven by identity trust to manage business domain segmentation, queue and bandwidth allocation, and dynamic rule deployment has yet to be established. To address this, this paper proposes an architectural solution centered on WAPI authentication semantics to drive the coordinated orchestration of VLANs and network slicing, queue scheduling, and OpenFlow rules. Through logical isolation between "security domains and service domains" and "security resource linkage" control policies, this approach translates identity and key status at the access layer into executable security assurance policies at the data plane. This bridges critical gaps in authentication, orchestration, and service assurance at the architectural level [12].

B. CURRENT STATUS OF WAPI IMPLEMENTATION

In recent years, research on wireless secure access for power IoT scenarios has primarily focused on three key directions: First, industry-specific deployment and engineering validation based on WAPI; second, achieving Wi-Fi network virtualization and slicing management through SDN/SDWN as the core, along with QoS control based on service requirements; third, establishing a closed-loop operational security assurance system by integrating identity authentication with network resource policies, and incorporating anomaly detection and intrusion detection mechanisms.

Existing WAPI studies first provide the engineering basis for secure wireless access in power-related environments. WAPI has already been tested in several high-security industrial and power communication settings. Existing work covers multi-terminal access, protected data transmission, deployment procedures, and security evaluation. For power devices with tighter communication conditions, such as distribution transformer terminals, reinforced WAPI mechanisms have also been studied, which gives more specific guidance for secure access design in power applications [13].

After terminals are admitted, the network still has to separate services, assign QoS, and adjust control policies when wireless links fluctuate. This is where SDN and SDWN studies become useful. By adding programmable control to Wi-Fi access networks, previous work has supported wireless slicing, slicing scheduling, and differentiated QoS for IoT and industrial Internet scenarios. Studies on SDWN controller performance also show that controller selection and control strategy should be adjusted when wireless links become unstable or service loads change [14]. Examples include cross-domain Federated AAA-SDN (FedAAA-SDN) designs and mechanisms for propagating and enforcing cross-layer, cross-domain security policies within slicing networks. These studies provide theoretical underpinnings for the proposed approach of "dynamically deploying VLAN/slicing and QoS policies driven by authentication outcomes." Furthermore, to achieve continuous communication for wireless terminals, existing standards and enterprise-level WLAN practices widely adopt mechanisms like 802.11r fast handover and OKC to reduce roaming delays. This also provides technical justification for the seamless roaming strategy based on pre-authentication and key caching proposed in this paper [15].

Regarding security monitoring and closed-loop handling, anomaly detection and intrusion detection technologies based on deep learning and machine learning have advanced rapidly in smart grid communications. Simultaneously, reviews of SDN-oriented intrusion detection systems and distributed collaborative IDS solutions provide feasible pathways for linking security monitoring alerts with controller policies [16].

III. METHOD

A. OVERVIEW OF THE METHOD

To address the pain points such as security-management misalignment, insufficient real-time performance, and low operation and maintenance efficiency in power WLAN (a crucial component for smart grid transformation), this paper proposes a WAPI-SDN based secure power WLAN networking architecture for security-management collaborative optimization, as illustrated in Figure 1. The architecture comprises three planes—Application Plane, Control Plane, and Data Plane—with secure channels facilitating WAPI-driven secure interactions among them. Specifically, the interaction between the application plane and the control plane is protected by HTTPS/gRPC over TLS, and mutual certificate authentication is used to verify the identity of management applications and SDN controllers. The interaction between the control plane and the data plane adopts OpenFlow over TLS to prevent flow rule tampering and controller spoofing. The communication between the SDN controller and the WAPI authentication server is protected through TLS or IPsec tunnels, and both sides are authenticated using locally issued certificates. Session keys are periodically updated, and device identities are bound

to certificate fingerprints and terminal white lists. In this way, WAPI authentication results, SDN control instructions, and monitoring data can be transmitted securely across different layers. For the isolation boundary between security domains and business domains, refined boundary access control policies are formulated based on VLAN division and ACL rules, which only allow authorized control signaling and standard service data to pass through the boundary. Meanwhile, a cross-domain attack detection and blocking mechanism is built. The SDN controller monitors cross-domain traffic in real time, identifies abnormal behaviors such as unauthorized cross-domain access and malicious data injection, and immediately issues OpenFlow flow table rules to block attack traffic, so as to maintain the stability and security of domain isolation.

In the Application Plane, applications interact with lower layers through the WAPI core. The Control Plane deploys SDN controllers with security policy parsing capabilities to centrally manage WAPI servers, AP rules, and resources; these controllers logically isolate security domains (undertaking authentication, key management, and attack detection) and service domains (distinguishing different power services via VLANs), and integrate a security-resource linkage module that leverages WAPI authentication results for SDN resource allocation—distribution terminals passing WAPI authentication can access high-priority domains with exclusive bandwidth, realizing architecture-level security-management collaboration. The Data Plane employs WAPI-AP supporting OpenFlow to achieve encrypted and flexible data transmission. Moreover, the architecture incorporates a power-oriented WAPI security solution subcase: it designs differentiated WAPI strategies for scenarios including distribution automation, information collection, and inspection robots to accurately match security mechanisms with business scenarios, and in some scenarios, collaborates with SDN to optimize network handover for guaranteeing data security and business continuity; simultaneously, a WAPI security monitoring submodule collects indicators like authentication success rate and abnormal access in real time, connects to the power dispatching system via SDN, and triggers rapid protection upon attack detection to form a "detection-alarm-disposal" closed-loop, supporting the stable operation of WLAN.

B. SDN DIFFERENTIATED ACCESS AND BANDWIDTH GUARANTEE TECHNOLOGY BASED ON WAPI AUTHENTICATION

The "SDN Differentiated Access and Bandwidth Guarantee Technology Based on WAPI Authentication" proposed in this paper is developed along the line of "authentication - resources - path" as a unified entity. Its structure is shown in Figure 2. This technology is designed to overcome the engineering challenges in traditional access networks, such as the separation of authentication and resource management, scattered configuration of service slicing and forwarding tables, and uncontrollable latency and jitter caused by wireless link fluctuations. In the overall design, the control layer deploys a multi-instance SDN controller with the capability of security policy parsing and orchestration, which uniformly receives WAPI authentication and key service events. The controller instances synchronize key states such as authentication results, service-domain mapping, and flow-rule versions through a distributed state database. An active-standby mechanism is adopted so that a standby controller can take over rule delivery when the master controller fails. The data layer consists of WAPI-APs and aggregation switching devices that support OpenFlow 1.3, completing encrypted bearer, classification queuing, and flexible forwarding. OpenFlow 1.3 is selected because it supports flow tables, meter tables, group tables, and QoS control, which are suitable for VLAN isolation, bandwidth guarantee, and fast failover.

Terminals are mapped to differentiated service domains (VLAN, VRF, SSID) according to the type of power business. A typical VLAN planning scheme is further defined to make the service-domain isolation executable. VLAN 10 is used for WAPI authentication and security management traffic, VLAN 20 is used for distribution automation services, VLAN 30 is used for electricity information collection, VLAN 40 is used for inspection robot video and telemetry traffic, VLAN 50 is used for substation local monitoring and photovoltaic station monitoring, and VLAN 99 is reserved as the quarantine domain for suspicious or unauthenticated terminals. The SDN controller dynamically binds terminal identity, certificate attributes, SSID, and VLAN ID after WAPI authentication. Inter-VLAN access is denied by default. Distribution automation terminals in VLAN 20 are only allowed to communicate with authorized control servers; electricity information collection terminals in VLAN 30 can only access the metering master station; inspection robots in VLAN 40 are allowed to access video processing and inspection management servers but cannot directly access control service hosts. Terminals in VLAN 99 can only access the authentication server, patch server, and security remediation platform. All exceptions are implemented through SDN-issued ACLs and OpenFlow rules, ensuring that business isolation and access control remain consistent with authentication results.

The SDN controller policy engine divides policy issuance into three priority levels, security protection policies are the highest level, resource scheduling policies are the middle level and service configuration policies are the lowest level. When policy conflicts occur, the controller preferentially implements high-priority policies and adjusts low-priority policies according to WAPI authentication status and power service priority weights to eliminate conflicts and ensure stable policy execution.

During the access phase, after the terminal undergoes WAPI two-way authentication, the controller generates a southbound rule template based on "authentication result + risk score + business intent," and sends ACL, Meter, Queue, and forwarding table entries to the entry AP and

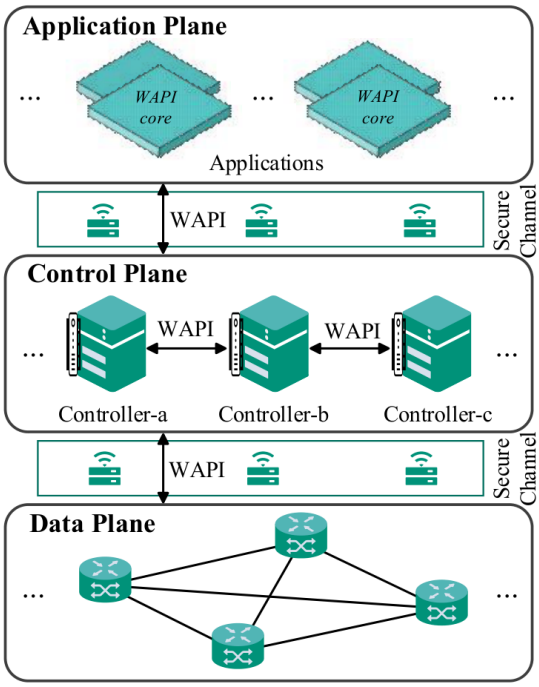


FIGURE 1. Overview of the Method

intermediate switching devices in one go, achieving "one-time policy orchestration and consistent effectiveness across the network." To achieve cross-layer collaboration, this paper quantifies the WAPI authentication result into a unified scheduling weight. The core is a two-step mapping and resource allocation, as shown in Equations (1) and (2):

$$\bar{\omega}_i = a_i \bar{\omega}_{c(i)} e^{-\gamma r_i} \tag{1}$$

$$B_i = \max\left(b_i^{\min}, \frac{\bar{\omega}_i}{\sum_{j\in F}\bar{\omega}_j} B^*\right), \qquad \sum_{i\in F} B_i \le B^* \tag{2}$$

Here, i represents the index of the accessing terminal, $a_i \in \{0,1\}$ indicates whether WAPI authentication is passed, $\bar{\omega}_{c(i)}$ is the priority weight of the service domain, $r_i \in [0,1]$ is the security risk score, γ is the risk suppression coefficient, $b_i^{\min}$ is the minimum guaranteed bandwidth for the flow, F is the set of active flows, and B^* is the allocable bandwidth within the domain. Equation (1) integrates "security trustworthiness - stable business importance - risk status" into a unified metric $\bar{\omega}_i$, and Equation (2) completes admission and bandwidth allocation for slices based on this, thereby directly converting the security conclusion of WAPI into measurable and executable resource outcomes.

The security risk score is calculated by a linear weighted quantitative model consisting of four core indicators, namely terminal certificate validity, abnormal access frequency, illegal access attempts and data encryption integrity. The weight of each indicator is determined by the analytic hierarchy process, with 0.3 for certificate validity, 0.25 for abnormal access frequency, 0.25 for illegal access attempts and 0.2 for data encryption integrity. The specific calculation formula is $S = 0.3C + 0.25F + 0.25A + 0.2E$, where S represents the security risk score, C represents the certificate validity score, F represents the abnormal access frequency score, A represents the illegal access attempt score, and E represents the data encryption integrity score.

To avoid the strong coupling and tuning overhead caused by the superposition of multiple ACLs, QoS, and slicing policies, this paper embeds the communication and control logic into the packet and label layers: after the entry AP completes WAPI encryption and encapsulation, it classifies based on VLAN/DSCP/service labels and aligns with the Queue/Meter mapping table issued by the controller, allowing paths, queues, and rates to be uniformly inferred within the same intent space. For latency-sensitive services (such as distribution automation), priority is given to primary/backup dual paths and low-latency queues, while for throughput-oriented services (such as video inspection), bandwidth guarantee and jitter control are used. Path selection aims at a composite cost of "congestion - latency," with the controller solving for the minimum cost path on the feasible path set, as shown in Equation (3):

$$p_i^* = \arg\min_{p\in P_i} \sum_{e\in p} \left[\alpha \frac{U_e}{C_e} + (1-\alpha) d_e\right] \tag{3}$$

Here, U_e/C_e is the relative link occupancy, d_e is the link latency, and $\alpha \in [0,1]$ is configured according to the scenario (taking a smaller value when latency is prioritized). During the operation phase, the data layer periodically reports Telemetry (throughput, packet loss, retransmission, roaming, and RSSI), and the control layer constructs a two-

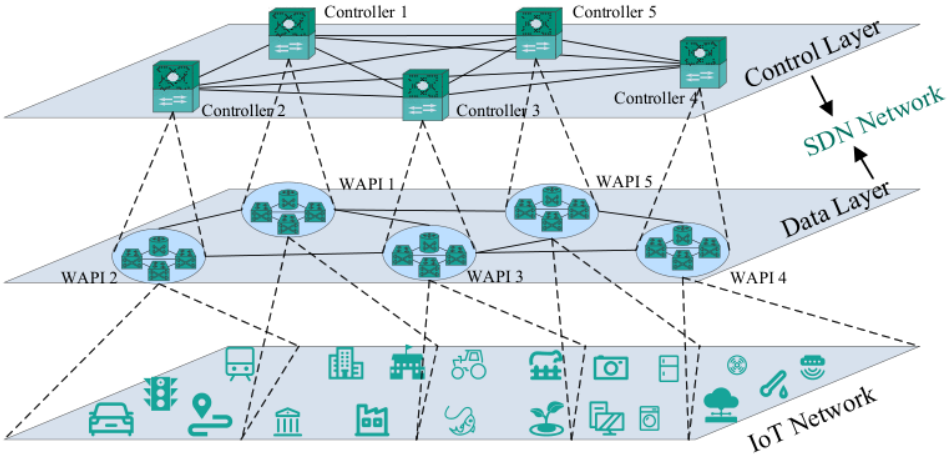


FIGURE 2. WAPI-Aware SDN Architecture for Secure Utility WLANs

level closed loop of "fast - slow": the fast loop (100–500 ms) adjusts Queue/Meter based on $\bar{\omega}_i$ and real-time indicators, while the slow loop (≥ 5 s) triggers lossless rerouting and slice reallocation when the cost in Equation (3) changes significantly. When abnormal authentication or signs of intrusion are detected, the system increases r_i to reduce $\bar{\omega}_i$, and migrates suspicious flows to the isolation domain or only allows control-plane traffic, forming an automatic collaboration of "authentication - resources - path." The fast closed loop sets the Telemetry data reporting frequency to 500 milliseconds and the slow closed loop to 5 seconds, and the single reporting data volume threshold is limited to 128 KB to prevent excessive occupation of network and controller resources. The reporting strategy is dynamically adjusted with power service priorities, latency-sensitive services use a higher reporting frequency to guarantee real-time scheduling, and conventional services adopt standard frequency to keep the overall system load stable.

To enhance system reliability and end-to-end verifiability, this paper sets up a lightweight consistency check and rollback mechanism at the boundary between the controller and the data plane. The shadow-table based consistency check is implemented as a lightweight two-phase rule verification mechanism. In the first phase, the controller writes newly generated flow rules into a shadow table rather than directly activating them in the data plane. The shadow table is updated periodically every 500 ms for fast QoS adjustments and every 5 s for slice-level or path-level reconfiguration. In addition, event-driven updates are triggered immediately when WAPI authentication failure, abnormal roaming, packet loss surge, or link utilization exceeding 80% is detected. In the second phase, the controller verifies the shadow rules before activation. Path reachability verification confirms that the selected forwarding path is available from the ingress WAPI-AP to the target service domain. Resource constraint validation checks whether the bandwidth allocation satisfies $\sum B_i \leq B^*$. Only after all checks are passed are the shadow rules atomically switched into the active table. If telemetry data show abnormal delay, packet loss, or session interruption after switching, the controller rolls back to the previous rule version and maintains the WAPI session state to avoid service interruption.

In summary, this paper replaces distributed manual configuration with "multi-controller fault tolerance + unified policy DSL," weakening single-point bottlenecks at the architectural level; it replaces fragmented maintenance with a three-step method of "authentication quantification - resource slicing - path orchestration," converging parameter coupling and tuning paths at the statistical and control levels; and it unifies the three equations to characterize the measurable trade-offs between security, bandwidth, and latency, achieving low-latency, manageable, controllable, and auditable power wireless local area networking under the conditions of wireless channel fluctuations and concurrent multiple services.

C. WAPI WIRELESS SECURITY APPLICATION FRAMEWORK FOR POWER TERMINALS

Based on the WAPI standard, we designed and implemented a wireless secure access framework for power terminal devices, as shown in Figure 3, to address security and continuity challenges across diverse operational scenarios in power systems.

Its core lies in integrating power-specific characteristics through scenario-based security policy design, SDN technology coordination, and real-time monitoring mechanisms to establish a closed-loop protection system. The framework is implemented around three connected operations: scenario-specific access policy selection, SDN-assisted resource allocation, and security-state feedback.

The starting point is not a uniform access procedure, but the different operating conditions of power terminals. Distribution automation, electricity information collection, inspection robots, and photovoltaic power station moni-

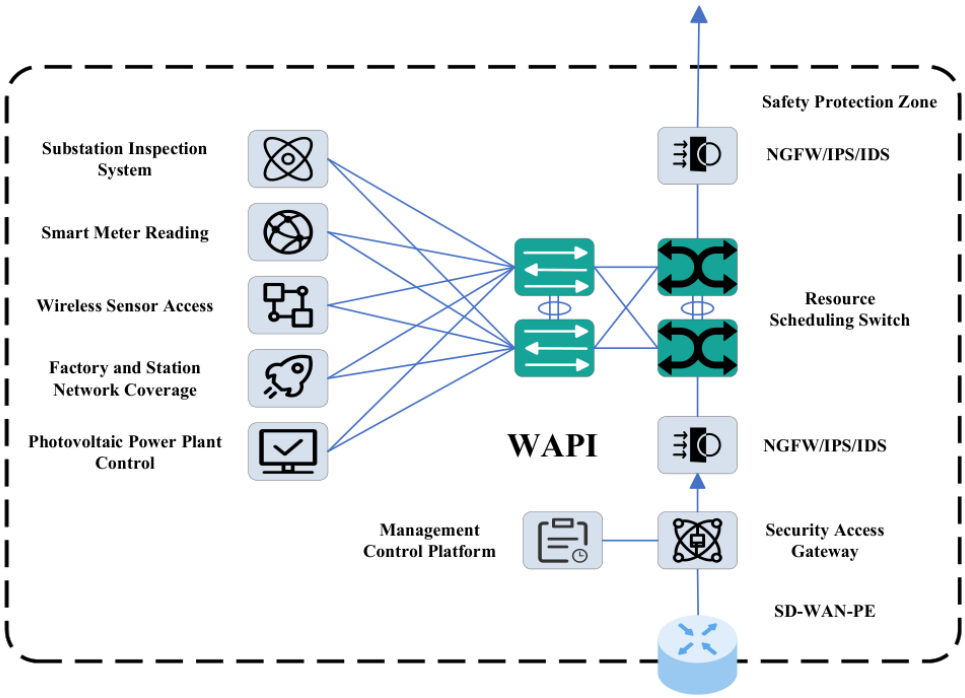


FIGURE 3. WAPI-Based Secure Access Framework for Power Terminal Devices

toring impose different constraints on delay, bandwidth, and security strength. Distribution automation is mainly constrained by low-latency and reliable control, whereas electricity information collection emphasizes data integrity and stable batch transmission. For this reason, WAPI is used as the common trusted-access mechanism, but its policy parameters are adjusted by scenario. In high-real-time services, pre-authentication and session key caching are introduced to reduce repeated certificate verification during roaming while retaining mutual authentication and dynamic key update. For large-volume transmission, stronger encryption and session persistence are maintained so that security protection does not interrupt continuous data delivery. The trade-off between security strength, authentication delay, and load overhead is described by the following utility function:

$$U = \alpha \cdot \frac{1}{T} + \beta \cdot S - \gamma \cdot L \tag{4}$$

In Equation (4), U denotes the effectiveness of the selected access strategy. T is the authentication delay, S represents the security strength, and L denotes the load overhead introduced by authentication, encryption, and session maintenance. The coefficients α, β, and γ are scenario weights rather than fixed constants; they indicate how much the strategy should emphasize delay reduction, security protection, and load control under a given power-service requirement.

For deployment, the three coefficients are normalized as $\alpha + \beta + \gamma = 1$. Their values are selected according to the dominant service constraint. In distribution automation, real-time control and reliability are given priority, so the delay-related weight is set higher, with $\alpha = 0.50$, $\beta = 0.35$, and $\gamma = 0.15$. In electricity information collection, data integrity and secure batch transmission are more important than millisecond-level latency, and the corresponding setting is $\alpha = 0.25$, $\beta = 0.50$, and $\gamma = 0.25$. For inspection robots, the policy must balance roaming continuity with video/data transmission overhead; therefore, $\alpha = 0.35$, $\beta = 0.30$, and $\gamma = 0.35$ are used. The allocation model is expressed as follows:

$$B_i = B_{\text{total}} \times \frac{(1-\lambda_i)w_i}{\sum_{j=1}^{n}(1-\lambda_j)w_j} \tag{5}$$

In Equation (5), B_i is the allocated effective bandwidth of service type i, B_{total} is the total available bandwidth, w_i is the priority weight of the service, and n is the number of service types. The coefficient λ_i represents the bandwidth loss of service type i caused by packet loss, retransmission, wireless attenuation, and protocol overhead, with its value ranging from 0 to 1. In this study, λ_i is estimated by combining periodic telemetry with active measurement. The AP and aggregation switch collect the physical link rate, retransmission ratio, packet loss rate, and effective throughput, while Iperf-based probing is performed during low-load periods. The coefficient is calculated as $\lambda_i = 1 - R_{i,\text{eff}}/R_{i,\text{phy}}$, where $R_{i,\text{eff}}$ is the measured effective throughput and $R_{i,\text{phy}}$ is the nominal or negotiated physical-layer rate. A sliding average window is used so that short-term wireless fluctuations do not cause frequent bandwidth oscillation.

The controller then applies different resource behaviors according to service criticality. Critical control operations

TABLE I. Emulation Scenarios

Scenarios	Number of Users	Number of Sensor Nodes
S1	4	4
S2	4	8
S3	4	12
S4	4	16
S5	4	20

receive bandwidth priority, while non-critical access can be restricted when resources are insufficient. Routine data collection uses elastic allocation so that channel resources are not occupied unnecessarily. The same centralized control logic is also used during mobility. When cross-region movement is detected, the controller can trigger path switching in advance to reduce roaming delay and keep the service session continuous. Security-state feedback is handled by a dedicated WAPI monitoring submodule deployed in access gateways or SD-WAN-PE nodes. The submodule collects WAPI authentication records, AP association information, SDN flow statistics, gateway security alarms, and terminal traffic behavior, and reports them to the central management platform through lightweight protocols.

IV. EXPERIMENT AND ANALYSIS

A. EXPERIMENT AND ANALYSIS OF WLAN OPERATION COMBINING WAPI AND SDN

In the emulation, the scale of the network was changed, but the communication relation inside each session was kept fixed. The user-sensor pairs listed in Table 1 were chosen from 50 pre-calibrated user devices and 20 sensor nodes. Once a user was paired with a dedicated sensor node, the pair was not changed during the run. This setting reduces the interference caused by session switching, so the changes in delay, throughput, and packet loss mainly reflect the increase in sensor-node scale.

Each scenario ran for 1000 s. The baseline traffic used a 1 KB payload every 1 s, which is close to periodic monitoring and routine sensor reporting in power WLAN services. Other payload sizes were added to represent different service loads: 128 B for control commands and protection instructions, 512 B for status and alarm messages, 4 KB for batch collection, and 16 KB for inspection image or video fragments. TCP flows were generated by Iperf for each user-sensor pair. Transmission delay, throughput, and packet loss were then used as the main KPIs.

Figure 4 gives the scalability results when the number of sensor nodes increases from 4 to 20. This small change suggests that the SDN-side forwarding adjustment and resource allocation absorbed part of the extra traffic pressure instead of letting node expansion directly cause a large throughput drop. In Figure 4(c), packet loss is also kept below 7%, which corresponds to a packet delivery rate of about 93% or higher. The highest loss rate is 6.94% with 16 sensor nodes, and the lowest is 4.29% with 8 sensor nodes. Since the loss rate does not increase monotonically with the node number, the result is more likely related to temporary wireless contention and traffic aggregation than to a simple scale effect.

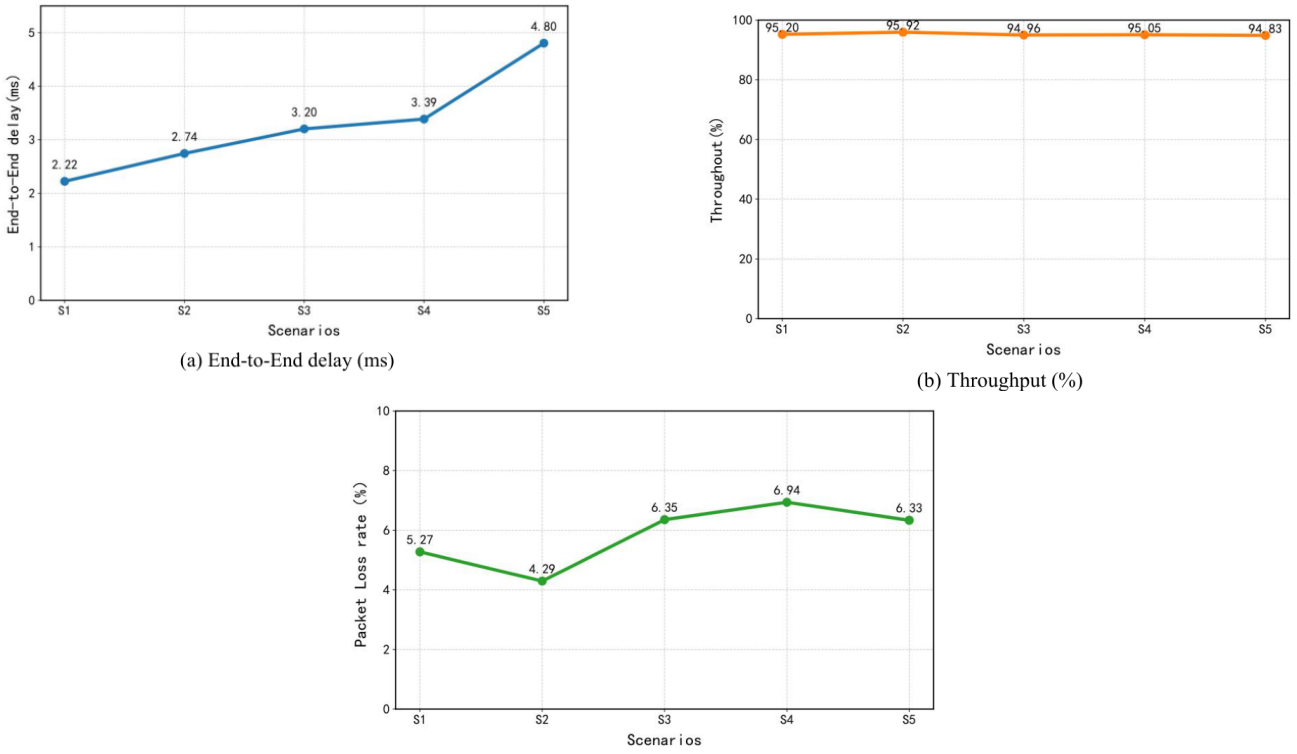
Burst-load tests were added because power WLAN traffic is not always periodic. Faults, alarms, and emergency reporting may create short periods of high-frequency transmission. When the packet interval was shortened to 0.1 s and 0.5 s, the end-to-end delay stayed within 8 ms, throughput remained above 88%, and packet loss was below 10%. These results do not mean that the network has unlimited capacity; rather, they show that the WAPI-SDN architecture still keeps usable transmission capacity under temporary traffic bursts, not only under the 1 s baseline reporting condition.

Figure 4 shows a clear difference among the three service cases, so a single traffic policy would be too rough for this network. Distribution automation is mainly limited by delay, and its end-to-end latency stays within 3 ms. Inspection robot traffic behaves differently: it keeps throughput above 95%, which is more relevant for image, video, and telemetry transmission. Photovoltaic power station monitoring is more sensitive to packet loss, and the loss rate is kept below 5%. These results fit the use of differentiated WAPI strategies and SDN slicing policies for different service types.

The payload-size test points to the same issue from another angle. Small packets, such as control commands and protection instructions, need low-latency queues and priority forwarding. Larger inspection payloads depend more on bandwidth guarantee and Meter-based rate control. So, in this WAPI-SDN architecture, resource scheduling should not be decided only by packet length. Service identity, risk score, and link status should also be included, since they tell the controller what the packet means and how urgent or risky the flow is. In deployment, this means control commands and protection instructions can be placed into latency-sensitive slices, while image and video fragments can use throughput-oriented slices with elastic bandwidth. This service-aware allocation is consistent with the low delay, limited throughput reduction, and controlled packet loss shown in Figure 4.

The inspection robot case also needs a mobility check, because its traffic is not only large but also moving across AP coverage. For this reason, a roaming experiment was added. Two adjacent WAPI-APs were deployed with partially overlapping coverage, and the robot repeatedly moved between them at about 1 m/s. The test compared pre-authentication with key caching against the conventional re-authentication mode.

The results show that the proposed pre-authentication and key caching strategy reduced the average authentication delay from 112.7 ms to 18.6 ms, and reduced the average service interruption time from 146.3 ms to 24.8 ms. The packet loss rate during roaming decreased from 3.9% to 0.8%. These results indicate that the proposed roaming optimization mechanism can maintain communication continuity for mobile power terminals such as inspection robots.



(a) End-to-End delay (ms)

(b) Throughput (%)

(c) Packet loss rate (%)

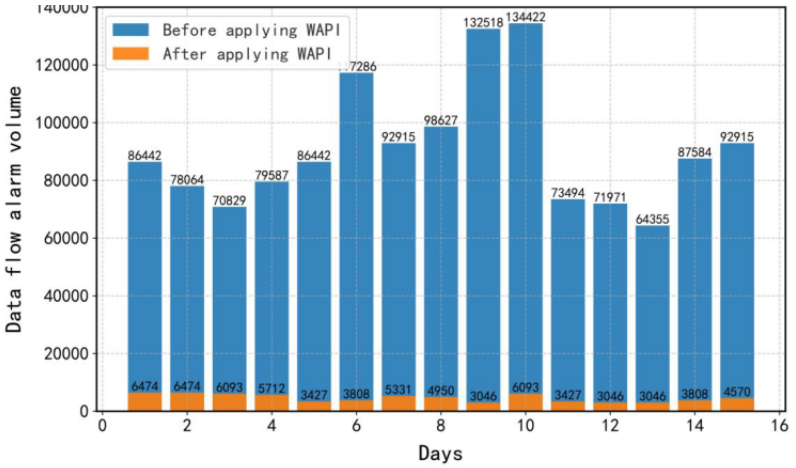
FIGURE 4. Emulation Results

B. EXPERIMENT AND ANALYSIS OF SECURE POWER WIRELESS LOCAL AREA NETWORK

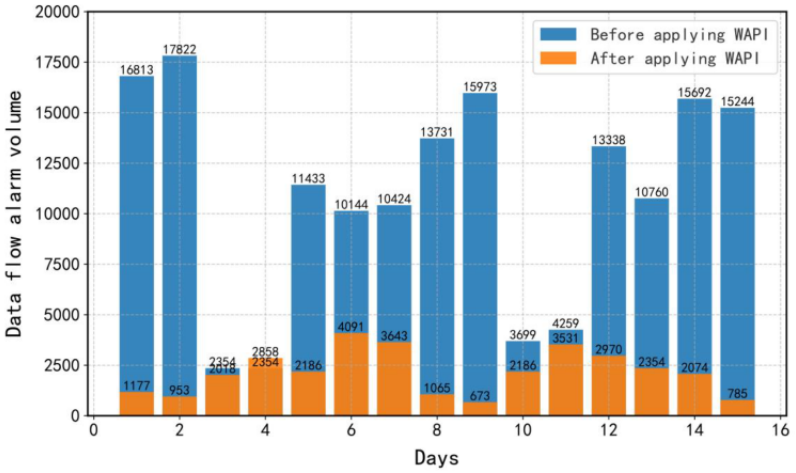
The purpose of the design verification phase is to investigate whether this wireless access method based on WAPI can centrally manage and uniformly schedule the wireless access traffic in the pilot area, and whether it can enhance the wireless network security capabilities of the pilot area (including core security capabilities such as identity authentication, data encryption, and anti-spoofing). The data collection process is divided into two stages: The first stage completes the wireless local area network networking of the pilot area. After the wireless traffic is accessed, the identity authentication and encryption mechanisms of WAPI are not enabled. Instead, it directly bypasses the security protection zone to access the target business. This stage lasts for 15 days. The second stage completes the deployment of WAPI security functions in the pilot area, enabling WAPI identity authentication, data encryption, and access control policies, and issuing appropriate wireless security scheduling rules to make WAPI security services available. This stage also lasts for 15 days.

In order to make a more objective evaluation of the solution, in the first stage, the full-flow probe of the security protection zone, the security analysis platform, and the log audit system are deployed on the untrusted side of the pilot area's wireless access gateway. In the second stage, the equipment remains in the same position, and the various types of wireless traffic data and alarm data collected in the two stages are compared and summarized. During the experiment, it was found that the access control and security scheduling policies of WAPI can take effect on the wireless terminal traffic in the pilot area, and traffic logs with source addresses from the wireless terminals in the pilot area and destination addresses of the business servers can be continuously monitored on the log audit system. The change curve of alarm quantities in the wireless access scenario collected from the security analysis platform is shown in Figure 5. It can be clearly seen from the figure that within 15 days after the WAPI security protection mechanism is enabled, the alarm quantities of north-south traffic in the wireless access scenario are significantly reduced, and the average alarm quantity of unauthorized wireless terminals accessing internal business servers from the outside was reduced by 94.8%.

The false positive rate of the unauthorized access alarm system is 1.2% and the false negative rate is 0.8%, both of which are far lower than the acceptable threshold of power system security monitoring. The low false positive and false negative rates prove that the WAPI-based security monitoring module has high accuracy and reliability, and can effectively identify real security threats without generating a large number of invalid alarms. By observing the protection logs, it was confirmed that the protection components filtered out a large amount of attack traffic from the outside, such as unauthorized wireless access, fake AP spoofing, malicious scanning, and command injec-



(a) Comparison of alarm volume change curves for branch nodes in stage one



(b) Comparison of alarm volume change curves for branch nodes in stage two

FIGURE 5. Comparison of Alarm Volume Change Curves for Branch Nodes in Stage One and Stage Two

tion, according to the WAPI security rule matching model. The remaining alarm types from the outside to the inside are mainly wireless terminal path traversal, configuration information leakage, weak password login, and access to illegal URLs. The alarms filtered out from the inside are mainly abnormal communications between internal wireless terminals and malicious IP addresses/domains, which are caused by suspected virus or Trojan infections in the pilot area's wireless terminals initiating C2 callbacks or mining activities. The remaining alarm types from the inside to the outside are mainly weak password login of wireless terminals and target application errors.

Balance tests between WAPI encryption strength and transmission performance are carried out for large data volume power scenarios. When the encryption strength is upgraded to the high-security level, the end-to-end delay only increases by 1.2 milliseconds and the throughput decreases by 4.1%, both within the acceptable range of power service requirements. The test data proves that the encryption enhancement measures can achieve a stable balance between security protection and transmission performance.

In addition, a simple quantitative comparison of AP management workload was conducted between the traditional WLAN management mode and the proposed WAPI-SDN architecture. In the traditional mode, AP configuration, security policy adjustment, and fault location mainly depend on distributed device configuration and manual cross-system checking. In contrast, the proposed architecture uses the SDN controller to centrally issue AP rules, VLAN policies, ACLs, and WAPI-related security service chains. In a pilot network containing 50 APs, the average time required for unified policy deployment decreased from 4.0 h to 0.8 h, and the average time for adding or replacing a single AP decreased from 18 min to 5 min.

Based on the experimental results, the management end of the WAPI pilot area can achieve unified deployment of the wireless access network in the pilot area and customization of the WAPI security service chain. It can also conduct unified auditing and management of the data streams of wireless terminals in the pilot area. Moreover, the WAPI security protection mechanism can effectively reinforce the security of north-south traffic in the wireless access scenario.

It is very effective in helping enterprises defend against unauthorized wireless access attacks, fake AP spoofing threats, and threat hunting and traceability of wireless traffic.

Although the experiment was conducted in a single pilot area, the proposed architecture can be extended to typical power scenarios such as substations, distribution station areas, and photovoltaic power stations. For substations, it supports low-latency and highly isolated control services; for distribution station areas, it supports access management of heterogeneous terminals; and for photovoltaic power stations, it supports elastic bandwidth allocation for monitoring and inspection data.

Considering that offline certificates are important for power scenarios where external network connectivity may be restricted, the efficiency of offline certificate verification and certificate update was also tested. The test used 100 power terminals and a local WAPI certificate server deployed in the pilot area.

V. CONCLUSION

This study examined power WLAN deployment from the perspective of coordination among security control, network scheduling, and operation and maintenance. The problems observed in conventional WLAN-based power communication are not limited to weak access protection. A more fundamental limitation is that terminal authentication, service-domain isolation, resource allocation, and fault diagnosis are often handled by separate mechanisms. Under this separation, high-security services may share policies with ordinary traffic, high-priority tasks such as distribution automation may suffer additional latency during congestion, and operators may need to correlate security events and network states across disconnected systems.

To reduce this separation, the study designed a secure power WLAN architecture that combines WAPI and SDN. In the architecture, WAPI provides public-key-based two-way authentication, dynamic key management, and encrypted wireless access, while SDN supplies centralized control and programmable resource scheduling. The control layer uses the SDN controller to manage WAPI servers, separate security and service domains through VLANs, and apply a security-resource linkage module that converts WAPI authentication results into SDN-side decisions.

ACKNOWLEDGMENT

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

REFERENCES

[1] T. Zang, S. Wang, Z. Wang, C. Li, Y. Liu, Y. Xiao, *et al.*, "Integrated planning and operation dispatching of source-grid-load-storage in a new power system: A coupled socio-cyber-physical perspective," *Energies*, vol. 17, no. 12, Art. no. 3013, 2024.

[2] S. A. H. Mohsan and H. Amjad, "A comprehensive survey on hybrid wireless networks: Practical considerations, challenges, applications and research directions," *Opt. Quantum Electron.*, vol. 53, no. 9, Art. no. 523, 2021.

[3] U. A. Bukar and M. Othman, "Architectural design, improvement, and challenges of distributed software-defined wireless sensor networks," *Wireless Pers. Commun.*, vol. 122, no. 3, pp. 2395–2439, 2022.

[4] S. Yang, K.-W. Lao, H. Hui, and Y. Chen, "A robustness-enhanced frequency regulation scheme for power system against multiple cyber and physical emergency events," *Appl. Energy*, vol. 350, Art. no. 121725, 2023.

[5] J. Zhou, B. Xu, Z. Fang, X. Zheng, R. Tang, and H. Haroglu, "Operations and maintenance digital built asset management," in *Digital Built Asset Management*, ch. 7. Cheltenham, U.K.: Edward Elgar Publishing, 2024, pp. 161–189.

[6] A. Karanveer, *Reliability Engineering in Cloud Computing: Strategies, Metrics, and Performance Assessment*. 2023.

[7] N. S. Shaji and R. Muthalagu, "Survey on security aspects of distributed software-defined networking controllers in an enterprise SD-WLAN," *Digital Commun. Netw.*, vol. 10, no. 6, pp. 1716–1731, 2024.

[8] Y. Andgelie, "The SDN based WLAN resilience enhancement for smart grid," *J. ICT Syst.*, vol. 3, no. 1, pp. 1–11, 2025.

[9] F. Lopez-Gomez, R. Marin-Lopez, O. Canovas, G. Lopez-Millan, and F. Pereniguez-Garcia, "SDN-AAA: Towards the standard management of AAA infrastructures," *J. Netw. Comput. Appl.*, vol. 236, Art. no. 104114, 2025.

[10] G. Hollósi, D. Ficzere, D. Varga, and P. Havinga, Eds., "Generative AI for low-level NETCONF configuration in network management based on YANG models," in *Proc. 20th Int. Conf. Netw. Service Manage. (CNSM)*, 2024.

[11] A. Amllou, A. Abane, M. Merzouki, L. Ait Ouchegou, Z. Maasqoui, and A. Battou, Eds., "Automated network programmability using OpenConfig YANG models and NETCONF protocol," in *Proc. 20th ACS/IEEE Int. Conf. Comput. Syst. Appl. (AICCSA)*, 2023.

[12] E. Batista, B. Alencar, E. Silva, J. Canário, R. A. Rios, S. Dustdar, *et al.*, "A new intelligent scheduler to improve reactive OpenFlow communication in SDN-based IoT data streams," *Discover Internet Things*, vol. 4, no. 1, Art. no. 15, 2024.

[13] P. Zhang, Y. Yang, Y. Zheng, and Y. Sun, "Multiplexed Internet of Things data transmission and visualization utilizing Wireless LAN Authentication and Privacy Infrastructure protocol in smart factories," *Sensors*, vol. 25, no. 10, Art. no. 3134, 2025.

[14] D. Kulikowski, K. Zia, O. Chiumento, and P. Havinga, Eds., "Towards robust slice control in SDN enabled WiFi based IoT networks," in *Proc. 20th Int. Conf. Design Reliable Commun. Netw. (DRCN)*, 2024.

[15] B. Sousa and C. Gonçalves, "FedAAA-SDN: Federated authentication, authorization and accounting in SDN controllers," *Comput. Netw.*, vol. 239, Art. no. 110130, 2024.

[16] M. F. Guato Burgos, J. Morato, and F. P. Vizcaino Imacaña, "A review of smart grid anomaly detection approaches pertaining to artificial intelligence," *Appl. Sci.*, vol. 14, no. 3, Art. no. 1194, 2024.