Lightweight Multi-Channel BiLSTM-Attention with Coordinated Defense for Intrusion Detection in Distributed Photovoltaic Communication Networks

Danni Liu[1*],Shengda Wang[1],Chunhui Shi[2],Jia Li[2], Xiuhong Jiang[1]
[1]JiLin Information & Telecommunication Company, State Grid Jilin Electric Power Corporation Ltd., Changchun 130000,China
[2]Jilin Jineng Electric Power Communication Co., Ltd. Changchun 130000,China;
E-mail: liudanni1212@163.com
[*]Corresponding author

Keywords: Distributed PV communication, intrusion detection, BiLSTM-attention, security defense

Received: Januar 9, 2026

To address intrusion and data tampering threats in distributed photovoltaic (PV) communication networks, this paper proposes a lightweight multi-channel BiLSTM-Attention–based intrusion detection and coordinated defense framework. An attack-oriented, risk-aware feature modeling method constructs multi-dimensional temporal inputs by combining protocol semantics, operational interaction behaviors, and deviation-based risk indicators, which are processed by a BiLSTM backbone with time-step attention and channel-level attention fusion. Model pruning and attention sparsification are adopted to obtain a compact architecture suitable for edge deployment, while a dual-threshold, detection-driven defense coordination mechanism links anomaly scores to graded response policies and closed-loop control. Experiments on a hybrid dataset composed of real PV communication logs and PV-adapted UNSW-NB15 and CIC-IDS2018 traffic show that the proposed model achieves 94.8% accuracy, 94.2% recall, and a 95.6% F1-score with an average inference time of 16.2 ms and a false positive rate below 3.6%. Compared with a vanilla BiLSTM-Attention baseline, the proposed framework improves F1-score by 3.2 percentage points and reduces inference latency by about 11%, while maintaining higher robustness under noisy and imbalanced conditions. These results indicate that the framework can provide accurate, real-time intrusion detection and coordinated security defense for distributed photovoltaic communication networks in resource-constrained deployment scenarios.

Povzetek:An improved lightweight multi-channel BiLSTM-Attention framework enhances intrusion detection and coordinated security defense in distributed photovoltaic communication networks through risk-aware temporal modeling, multi-channel attention fusion, and model pruning for edge deployment.

Povzetek: Študija predlaga lahkoten model za zaznavanje vdorov v komunikacijskih omrežjih fotovoltaičnih sistemov, ki z uporabo pozornosti in optimizacije omogoča hitro, natančno in robustno varnostno zaščito v realnem času.

1 Introduction

In recent years, the large-scale deployment of distributed photovoltaic (PV) systems has become a critical component of modern energy infrastructures. To support real-time monitoring, remote control, and grid coordination, PV systems rely on communication networks that interconnect inverters, monitoring terminals, smart meters, and dispatch centers. These communication networks operate at high frequency and are increasingly integrated with edge computing devices, forming a typical Energy Internet of Things (Energy IoT) architecture. However, due to the widespread use of lightweight protocols, heterogeneous access mechanisms, and resource-constrained edge nodes, distributed PV communication networks are inherently exposed to multiple cybersecurity risks.

Unlike traditional enterprise networks, PV communication environments exhibit strong coupling between cyber behavior and physical power processes. Network intrusions, data tampering, or denial-of-service attacks may not only disrupt communication availability but also distort control commands and power feedback signals, potentially leading to inverter misoperation, regional energy imbalance, or cascading grid instability. Recent reports indicate a continuous increase in cyberattacks targeting Energy IoT and cyber–physical energy systems . Attackers often exploit protocol vulnerabilities or authentication weaknesses through

DNS redirection, man-in-the-middle attacks, and malicious script injection to achieve stealthy control or data manipulation in PV communication nodes .

Conventional intrusion detection systems (IDS), such as rule-based or signature-driven approaches (e.g., Snort, Bro), are insufficient for such scenarios. These methods typically rely on static feature matching and predefined attack patterns, resulting in high false-positive rates, limited recall, and delayed responses when facing low-frequency, multi-stage, or evolving attack behaviors . In particular, when attackers embed malicious actions within legitimate communication flows, static detection strategies become ineffective, highlighting the need for detection models capable of capturing temporal dependencies and behavioral deviations in PV communication data.

Deep learning techniques have shown promising potential in addressing complex intrusion detection tasks. Recurrent neural networks, especially Long Short-Term Memory (LSTM) and Bidirectional LSTM (BiLSTM), have demonstrated strong capability in modeling sequential data and capturing long-range temporal dependencies . Attention mechanisms further enhance such models by dynamically focusing on salient features while suppressing redundant or noisy information, thereby improving discrimination performance in time-series classification tasks . These advantages make deep temporal models particularly suitable for intrusion detection in PV communication environments.

Nevertheless, directly applying deep learning models to distributed PV systems remains challenging. PV communication data are often non-stationary, highly imbalanced, and generated under strict resource constraints at edge nodes. Many existing deep IDS solutions suffer from excessive model complexity, high inference latency, and limited adaptability to edge deployment. Moreover, most studies focus solely on detection accuracy, while neglecting the integration of detection results with coordinated defense and response mechanisms, resulting in fragmented security solutions.

To address these limitations, this paper proposes an improved BiLSTM-Attention–based intrusion detection and security defense framework for distributed PV communication networks, with an emphasis on lightweight deployment, high detection accuracy, and robust response capability. The proposed framework aims to answer the following research questions:

• Can temporal modeling combined with attention mechanisms significantly improve the identification of covert and multi-stage attack behaviors in PV communication data?

• How can channel-level attention fusion and model pruning strategies achieve an effective trade-off between detection performance and computational efficiency in resource-constrained edge environments?

• Can intrusion detection outputs be systematically integrated with defense response mechanisms to enable rapid, coordinated, and closed-loop security control?

The main contributions of this work are summarized as follows:

• An attack-oriented feature modeling method tailored for distributed PV communication is proposed, constructing multi-dimensional temporal input features by integrating protocol semantics and operational interaction behaviors;

• An enhanced BiLSTM-Attention intrusion detection model is developed, employing multi-channel attention mechanisms to strengthen the recognition of critical attack patterns;

• A lightweight, detection-driven defense coordination mechanism is designed to support distributed and closed-loop security response;

• Comprehensive experiments are conducted on multi-source PV communication datasets, including baseline comparisons, ablation studies, and false-alarm control evaluations, demonstrating the effectiveness and practicality of the proposed framework.

The remainder of this paper is organized as follows. Section 2 reviews related work on PV communication security and deep learning–based intrusion detection. Section 3 presents the proposed detection and defense framework and key module designs. Section 4 describes the experimental setup, evaluation metrics, and performance analysis. Section 5 discusses deployment feasibility and defense effectiveness. Section 6 concludes the paper and outlines future research directions.

To make the research design more explicit, the three research questions raised above are operationalized through specific model components and evaluation settings. RQ1, which concerns the ability of temporal modeling and attention mechanisms to identify covert and multi-stage attacks, is addressed by the risk-aware intrusion feature modeling in Section 3.1 and the BiLSTM-Attention–based temporal classifier in Section 3.2, and is evaluated mainly through detection metrics such as Accuracy, Precision, Recall, and F1-score in the comparative and ablation experiments reported in Sections 4.3 and 4.4. RQ2, which focuses on balancing detection performance and computational efficiency in edge environments, is tackled by the multi-channel attention fusion and lightweight optimization strategies in Section 3.3, and is examined using Average Inference Time, Real-Time Factor, and Robustness Retention Rate as defined in Section 4.2, together with the ablation results in Section 4.4. RQ3, which asks whether detection outputs can be systematically integrated with coordinated defense, is addressed by the detection-driven defense response and interconnected control mechanism in Section 3.4 and the applicability

verification in Section 5.2, where response latency, false positive rate, and closed-loop response success rate are used to quantify the effectiveness of the proposed security control process.

2 Related research

Distributed photovoltaic communication networks feature widespread deployment, heterogeneous nodes, and real-time transmission capabilities, making them highly susceptible to cyberattacks. With the widespread deployment of smart inverters, remote monitoring modules, and energy gateways, attackers can launch intrusions by hijacking communication links, injecting malicious commands, or manipulating power feedback, thereby compromising system stability and grid security. Consequently, establishing precise and efficient intrusion detection and defense mechanisms has become critical for ensuring the secure operation of photovoltaic systems.

In recent years, intrusion detection for IoT and distributed energy systems has attracted substantial research attention, with a clear trend toward diverse methodologies, model integration, and richer evaluation dimensions. Against the backdrop of traditional signature- and rule-based detection methods revealing limitations in responsiveness and weak generalization capabilities, intrusion detection systems (IDS) leveraging machine learning (ML) and deep learning (DL) have gained significant attention. Particularly in the emerging context of PV communications, AI approaches demonstrate promising application prospects. Harrou et al. (2023) [1] conducted a systematic review of security threats, intrusion vectors, and detection challenges facing PV systems. They noted that currently deployed IDSs predominantly utilize generic models that remain unoptimized for PV scenarios, lacking effective modeling of multimodal temporal data such as voltage, current, and control commands within communication links. Gao et al. (2022) [2] proposed combining CNN with BiLSTM for traffic analysis in cloud computing environments, achieving certain detection performance but neglecting considerations for lightweight deployment and timely response.

Regarding model architecture, BiLSTM is widely adopted in intrusion detection due to its bidirectional context capture capability. Zhang et al. (2023) [3] constructed a detection model based on BiLSTM and multi-head attention mechanisms, achieving high accuracy on public datasets. Similarly, Yin et al. (2024) [4] proposed a hybrid model integrating CNN and BiLSTM under unbalanced traffic conditions, enhancing focus on critical anomaly features through attention mechanisms. Said et al. (2023) [5] deployed the Attention-CNN-BiLSTM architecture in software-defined networking environments, validating its robustness against complex attack behaviors. These studies provide theoretical foundations for applying deep temporal models in photovoltaic communication scenarios.

Given the unique characteristics of photovoltaic energy systems, Di et al. [6] proposed an anomaly detection mechanism based on spatio-temporal feature collaborative modeling. This approach integrates multi-source information—including PV power, network latency, and node characteristics—into a unified analytical framework, enhancing the ability to identify subtle intrusive activities. Ma et al. (2021) [7] designed a programmable IDS architecture specifically tailored for distributed energy systems, employing edge deployment to reduce central processing load. Additionally, Sourav et al. (2022) [8] constructed an attack detection prototype system on a real PV platform, demonstrating the applicability of deep learning-based detection strategies in power scenarios.

From a methodological perspective, the introduction of attention mechanisms has become a key pathway for enhancing model accuracy and interpretability in recent years. Laghrissi et al. (2021) [9] proposed the "IDS-Attention" algorithm, significantly improving intrusion recognition performance by guiding the model to focus on key fields. Wang and Ghaleb (2023) [10] further integrated CNN convolution extraction with Attention-based dynamic weight allocation to construct lightweight, high-precision models suitable for edge computing environments. However, most studies have yet to deeply optimize for the unique data characteristics of PV communications, resulting in issues such as insufficient generalization capabilities, detection delays, and lack of coordinated attack response capabilities.

At the system deployment level, Nandanwar and Katarya (2024) [11] emphasized deployment constraints in industrial IoT, proposing the integration of federated learning and model pruning techniques into lightweight model design. Yu et al. (2022) [12] adopted an evolutionary learning approach, proposing a dynamically optimized detection framework to adapt to evolving attack strategies. Nevertheless, a comprehensive framework combining detection and defense coordination with closed-loop response capabilities remains elusive.

To provide a clearer comparison of representative intrusion detection approaches and their applicability to distributed PV communication scenarios, Table 1 summarizes key characteristics of the most relevant works reviewed in this section, including their target domains, model architectures, datasets, and main limitations.

Table 1: Summary of representative intrusion detection approaches and their limitations in PV-related scenarios

Ref.	Target domain / scenario	Core method	Datasets	Main strengths
[1] Harrou et al., 2023	PV systems (survey)	Review of IDS and security threats	– (survey)	Comprehensive taxonomy of threats and IDS requirements for PV systems
[2] Gao, 2022	Cloud computing traffic	CNN + BiLSTM	UNSW-NB15	Captures local spatial and temporal patterns; improved accuracy over classical ML
[3] Zhang et al., 2023	Generic network traffic	BiLSTM with multi-head attention	Public IDS datasets	Strong sequence modeling with attention-based feature focusing
[4] Yin et al., 2024	Class-imbalanced abnormal traffic	CNN–BiLSTM with attention	Imbalanced traffic datasets	Better handling of imbalanced anomalies with attention
[5] Said et al., 2023	SDN environments	Attention-CNN-BiLSTM	SDN traffic traces	Robust detection under complex SDN attacks
[6] Di et al., 2024	Distributed PV communication	Spatio-temporal feature collaborative modeling	Real PV data	Incorporates PV power, latency, and node attributes into a unified model
[7] Ma et al., 2022	Distributed energy resources	Programmable IDS at the edge	Microgrid datasets	Edge-oriented architecture reduces central processing load
[8] Sourav et al., 2022	Real PV platforms	DL-based attack detection prototype	Real PV platform traces	Demonstrates feasibility of DL-based IDS in PV systems
[9] Laghrissi et al., 2021	Generic IDS	IDS-Attention algorithm	KDD-like datasets	Attention improves feature importance modeling and interpretability
[10] Wang & Ghaleb, 2023	Network intrusion detection	Attention-based CNN	Benchmark IDS datasets	Constructs efficient attention-enhanced CNN model
[11] Nandanwar & Katarya, 2024	Industrial IoT	DL-enabled IDS with pruning and FL	Industrial IoT datasets	Considers federated learning and pruning for lightweight IDS
[12] Yu et al., 2022	Smart grid cybersecurity	Evolving ML-based IDS	Smart grid datasets	Adapts to evolving attack strategies with dynamic optimization

As summarized in Table 1, existing deep learning–based intrusion detection approaches have made clear progress in sequence modeling, attention-based feature focusing, and lightweight deployment for IoT and smart grid environments. However, three gaps remain in the specific context of distributed PV communication networks. First, only a few studies, such as [6] and [8], explicitly consider PV operational semantics, and they still lack an attack-oriented, risk-aware feature modeling pipeline that integrates protocol behavior with power-side interactions. Second, attention mechanisms and pruning strategies are rarely combined into a unified multi-channel temporal framework that is explicitly optimized for edge deployment in PV communication nodes. Third, most prior work treats detection as an isolated task and does not systematically couple intrusion scores with graded defense responses and closed-loop control. The framework proposed in this paper is designed precisely to address these three gaps by (i) constructing risk-aware temporal features tailored to PV communication, (ii) integrating multi-channel BiLSTM-Attention with pruning and attention sparsification for lightweight edge inference, and (iii) embedding a detection-driven, dual-threshold defense coordination mechanism into the overall architecture.

Overall, while existing research has yielded significant advances in intrusion detection model architecture, training mechanisms, and attention optimization, three major shortcomings persist in the specific context of distributed PV communication: (1) Models lack customization based on PV operational logic and device behavioral characteristics; (2) Precise identification mechanisms for low-frequency, stealthy, and multi-stage attacks are absent; (3) Detection outcomes fail to effectively drive subsequent defensive

responses, resulting in an incomplete security coordination system.

To address the aforementioned limitations, this paper proposes an enhanced BiLSTM-Attention intrusion detection and defense coordination mechanism. By integrating channel attention with lightweight deployment strategies, it achieves efficient identification and rapid response control against photovoltaic communication attacks. The proposed model balances multi-source data fusion, attack behavior modeling, and security policy coordination, aiming to establish a distributed detection framework with high accuracy, low latency, and strong robustness.

3 Methodology

3.1 Intrusion feature modeling and risk classification mechanism for PV communication networks

The intrusion detection process for distributed photovoltaic (PV) communication networks is fundamentally driven by communication behavior modeling and risk-aware feature abstraction. To support dynamic detection and closed-loop security control, the proposed framework continuously collects real-time communication data from multiple sensing sources deployed across PV nodes. These data streams include power command interactions, control parameter transmissions, packet structural attributes, traffic load variations, link delay, and jitter characteristics. By integrating cyber communication indicators with operational interaction behaviors, the system aims to construct a feature representation that accurately reflects the temporal evolution of PV communication states under both normal and malicious conditions.

After data acquisition, all features are standardized and organized into time-series sequences using sliding window segmentation. For each PV communication node, the system abstracts its communication behavior within a given observation window into a unified feature vector for the i-th window, denoted as:

$$X_i = [p_i d_i \tau_i \sigma_i c_i]^T \quad (1)$$

where $x_i \in \mathbb{R}^D$ is a D-dimensional feature vector and i indexes the communication sessions or sliding windows. $p_i \in \mathbb{R}^{dp}$ denotes a vector of transmission power states and related electrical quantities within the observation window, $d_i \in \mathbb{R}^{dd}$ represents packet-level structural features (e.g., protocol fields and length statistics), $\tau_i \in \mathbb{R}^d\tau$ corresponds to aggregated delay statistics, $\sigma_i \in \mathbb{R}^d\sigma$ characterizes link jitter and volatility, and $c_i \in \mathbb{R}^{dc}$ encodes the category of control or operational instructions. The feature dimension satisfies $D = d^p + d^d + d\tau + d\sigma + d^c$, and all components are normalized before being fed into the temporal model to ensure numerical stability during training.This feature composition enables joint characterization of physical operation indicators and network communication attributes, forming a multidimensional representation suitable for subsequent temporal modeling. All feature dimensions are normalized to eliminate scale disparities and ensure stable model convergence.

To enhance the sensitivity of intrusion detection and reduce the impact of redundant information, a risk classification mechanism is introduced prior to temporal learning. By analyzing historical communication behavior patterns under normal operating conditions, the system estimates the statistical distribution of each feature dimension and computes the deviation intensity of current observations as

$$r_i = \frac{|f_i - \mu_i|}{\sigma_i} \quad (2)$$

where f_i represents the current value of the i-th feature, and μ_i and σ_i denote the corresponding mean and standard deviation obtained from baseline behavior profiles. The deviation measure r_i quantifies the anomaly degree of each feature dimension relative to historical norms, providing a normalized indicator of potential security risk.To aggregate the dimension-wise deviations into a sequence-level indicator, the mean absolute deviation is computed as

$$R = \frac{1}{d}\sum_{i=1}^{d} | r_i | \quad (3)$$

where d denotes the number of feature dimensions in the current observation window.

Based on two deviation thresholds $\theta_1$and$\theta_2$and the sequence-level risk score R, communication behaviors are classified into three levels: normal operation $(R < \theta_1)$, security alert $(\theta_1 \le R < \theta_2)$, and high-risk intrusion $(R \ge \theta_2)$. The thresholds θ_1 and θ_2 are selected on the validation set by grid-searching candidate values to maximize the F1-score under the constraint that the false positive rate remains below 4%. Once determined, θ_1 and θ_2 are kept fixed during testing. A small sensitivity study shows that jointly varying both thresholds by ±10%\pm 10\%±10% changes the overall F1-score by less than 0.4 percentage points, indicating that the detection performance is not overly sensitive to the exact threshold values. This risk-tiering strategy enables the system to assign adaptive weights to feature sequences before they are fed into the BiLSTM-Attention model. As a result, the temporal learning process can focus more effectively on critical anomaly-related dimensions while suppressing the influence of benign fluctuations, improving both detection precision and computational efficiency.

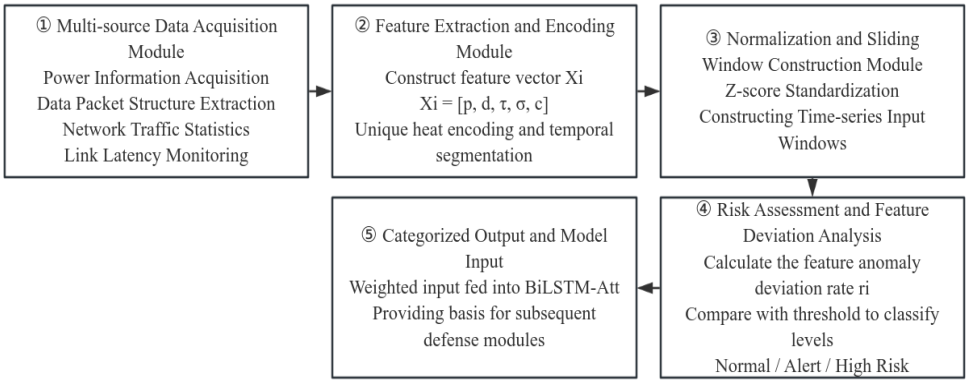


Figure 1: Flowchart of intrusion feature modeling and risk classification mechanism for photovoltaic communication networks.

Figure 1 illustrates the overall workflow of intrusion feature modeling and risk classification for PV communication networks. Through a streamlined pipeline encompassing data collection, feature extraction, normalization, risk evaluation, and classification output, the proposed mechanism supports continuous monitoring and early warning of complex intrusion behaviors. The resulting risk-aware feature sequences provide structured and informative inputs for subsequent temporal detection and defense response modules, laying the foundation for coordinated and closed-loop security control in distributed photovoltaic environments.

3.2 Construction of a BiLSTM-attention-based temporal intrusion detection model

Abnormal behaviors in photovoltaic (PV) communication networks typically manifest as temporally correlated events rather than isolated anomalies. Repeated control commands, sudden response delays, abnormal traffic bursts, and gradual behavior drifts often emerge over consecutive communication intervals, making temporal dependency modeling a critical requirement for effective intrusion detection. Based on the risk-aware feature sequences generated in the preceding stage, this study constructs a temporal intrusion detection model using a BiLSTM-Attention architecture to capture bidirectional dependencies and dynamically emphasize critical behavioral patterns within PV communication streams.

In the proposed model, continuous PV communication traffic is first reorganized into structured temporal units. Each communication session is segmented into fixed-length sequences through a sliding window mechanism, ensuring consistent temporal granularity while preserving local dependency information. Each segmented sequence is treated as a temporal state node, and the chronological relationships among nodes form a temporal dependency structure. From this perspective, the intrusion detection task can be abstracted as a temporal modeling graph defined as

$$G = (V, E) \tag{4}$$

where $V = (x_1, x_2, \ldots, x_T)$ represents the ordered communication state vectors over time, and E denotes the implicit temporal dependencies between adjacent and distant states. Instead of explicitly constructing graph edges, the BiLSTM implicitly captures these temporal dependencies through its forward and backward information flows.

The BiLSTM network processes the temporal feature sequences in both forward and backward directions, enabling the model to simultaneously capture historical context and future trend information. This bidirectional modeling is particularly suitable for PV communication scenarios, where abnormal behaviors may be influenced by both preceding operational commands and subsequent system responses. To further enhance discrimination capability, an attention mechanism is integrated on top of the BiLSTM hidden representations to adaptively allocate feature importance across time steps.

The attention layer computes the relevance of each hidden state by measuring its alignment with a learnable context vector, and the attention weight for the t-th time step is calculated as

$$a_t = \frac{\exp(h_t^T W_a c)}{\sum_{i=1}^{t} \exp(h_i^T W_a c)} \tag{5}$$

where h_t denotes the hidden state output of the BiLSTM at time step t, W_a is a trainable weight matrix, and c represents the context vector learned during training. Through this mechanism, the model is able to assign higher weights to time steps associated with suspicious behavior patterns while suppressing the influence of benign or redundant fluctuations.

The weighted hidden representations are then aggregated to form a compact temporal feature embedding, which is subsequently fed into a Softmax classifier for attack category prediction. By jointly

integrating bidirectional temporal modeling and attention-based feature focusing, the proposed BiLSTM-Attention model achieves precise and dynamic classification of anomalous communication behaviors in PV networks. The effectiveness of this architecture, including its detection accuracy, recall performance, and computational efficiency under resource-constrained conditions, is systematically evaluated in the experimental section.

To ensure reproducibility, the main architectural configuration and training hyperparameters of the proposed BiLSTM-Attention model are summarized in Table 2. The network consists of two stacked BiLSTM layers with 128 hidden units per direction in each layer, followed by an additive attention layer and a fully connected projection layer with 64 neurons and ReLU activation. A dropout rate of 0.3 is applied between the BiLSTM layers and before the final fully connected layer to mitigate overfitting. The output layer is a Softmax classifier over six behavior categories, corresponding to normal communication and five representative attack types in the constructed dataset.

Table 2: Main architectural configuration and training hyperparameters of the improved BiLSTM-Attention model

Component / hyperparameter	Setting
Input sequence length T	20-time steps per window
Input feature dimension D	52 (after preprocessing and feature fusion)
BiLSTM layers	2 stacked bidirectional LSTM layers
Hidden units per direction	128 per layer
Attention type	Additive attention over time steps
Attention dimension	128
Fully connected layer size	64 neurons, ReLU activation
Dropout rate	0.3 (between BiLSTM layers and before the FC layer)
Output classes	6 (normal + 5 attack types)
Optimizer	Adam
Initial learning rate	1×10^{-3} with step decay
Batch size	128
Number of training epochs	80 (with early stopping, patience = 10 epochs)

3.3 Multi-channel attention fusion mechanism and lightweight detection optimization

To enhance the recognition capability of multi-source attack features while ensuring efficient deployment in resource-constrained photovoltaic (PV) communication nodes, this study integrates a multi-channel attention fusion mechanism with lightweight detection optimization strategies. The objective is to achieve a balanced trade-off between detection accuracy and computational efficiency under practical edge-side operating conditions. During feature preprocessing, the PV communication data stream is decomposed into multiple parallel channels according to protocol semantics, control command characteristics, port-level behavior patterns, and temporal interaction features. Each channel represents a distinct semantic subspace reflecting a specific aspect of communication behavior, thereby enabling finer-grained modeling of heterogeneous attack characteristics.

After independent feature embedding and bidirectional temporal modeling, each channel produces a corresponding feature sequence $H^{(i)}$. These channel-specific representations are subsequently aggregated through a channel-level attention fusion mechanism, which dynamically evaluates the contribution of each channel to the overall detection task. The fused representation is computed as

$$H_{fusion} = \sum_{i=1}^{N} a_i \, H^{(i)} \qquad (6)$$

where a_i denotes the attention coefficient assigned to the i-th channel. The coefficients are adaptively adjusted based on the correlation between channel features and the global context representation learned during training. Through this mechanism, channels that exhibit stronger relevance to abnormal or malicious behaviors are emphasized, while redundant or weakly informative channels are suppressed. This fusion strategy effectively alleviates semantic overlap and noise interference across channels, improving sensitivity to low-frequency and covert attack patterns in PV communication traffic.

To further optimize inference efficiency and support edge-side deployment, lightweight optimization techniques are applied to the BiLSTM-Attention architecture. Channel pruning is employed to remove low-contribution channels by analyzing gradient variation intensity during the training process, thereby reducing model parameters and computational overhead without significantly affecting detection performance. In parallel, attention sparsification is introduced through an

L_1-constrained regularization term, encouraging the concentration of attention weights on a limited number of salient temporal features. This sparsity constraint reduces redundant computations and accelerates inference while preserving critical behavioral information.

In addition, a dual-threshold decision mechanism is incorporated at the model output stage to enhance practical usability. Based on confidence scores produced by the classifier, communication behaviors are categorized into three states: high-confidence intrusion, high-uncertainty alert, and normal operation. This hierarchical discrimination strategy facilitates flexible coordination between detection results and subsequent response modules, enabling differentiated handling of confirmed attacks and ambiguous events. Through the joint application of multi-channel attention fusion, structural pruning, attention sparsification, and adaptive decision control, the proposed model achieves lightweight deployment, real-time intrusion recognition, and robust resource adaptability in dynamic PV communication environments.

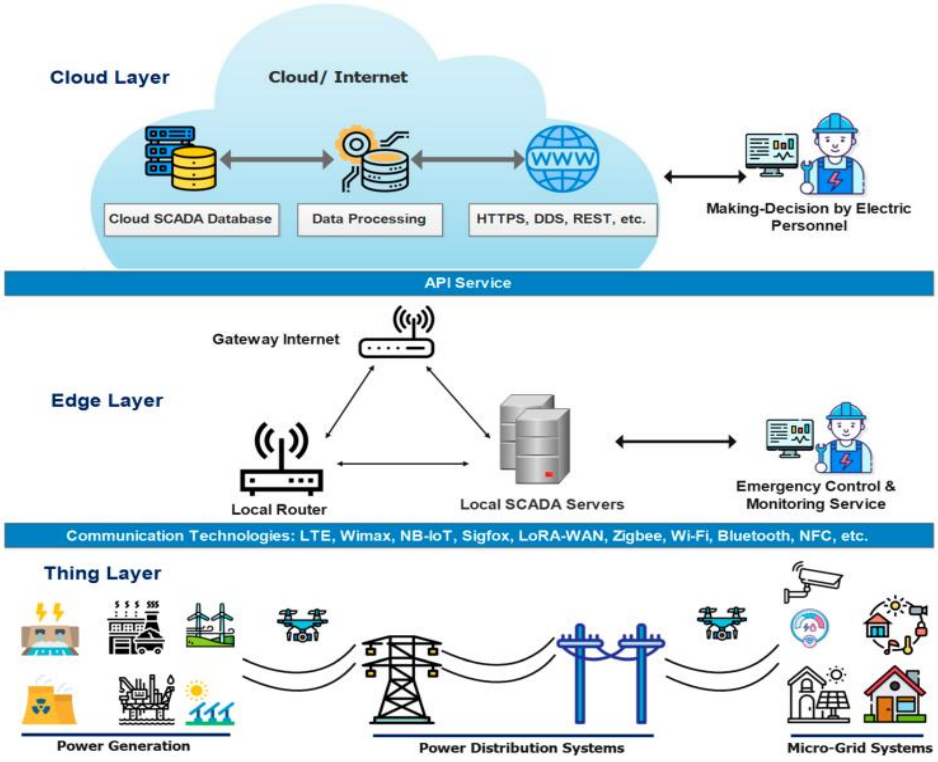


Figure 2:Multi-layer SCADA communication and intrusion detection deployment structure in a distributed PV communication system.

Figure 2 illustrates the deployment of the enhanced intrusion detection model within a distributed PV communication system. The architecture spans from physical device layers, including distributed inverters and sensors, through edge-side SCADA control units and local routing components, and extends to cloud-level scheduling and decision support platforms. By performing feature collection, risk modeling, and intrusion detection at edge communication nodes, the proposed framework enables timely anomaly identification and coordinated security response under constrained computational conditions. In the prototype implementation, the intrusion detection module is deployed on edge SCADA gateways as a pruned neural network with approximately 0.65 million trainable parameters (about 2.6 MB in 32-bit floating-point representation) and an estimated single-inference cost of 1.5×10^8 floating-point operations, which fits within the processing and memory budgets of typical industrial PV communication controllers.

3.4 Detection-driven security defense response and interconnected control mechanism

Considering the characteristics of cyberattacks in distributed photovoltaic (PV) communication systems, including strong concealment, rapid propagation, and cascading impact across interconnected nodes, this study designs a detection-driven security defense response and interconnected control mechanism to support coordinated and closed-loop protection. Unlike traditional intrusion detection systems that operate independently of response processes, the proposed mechanism tightly couples detection outputs with

defense execution, enabling timely mitigation and adaptive adjustment under dynamic attack conditions.

Once abnormal communication behavior is identified by the intrusion detection module, a threat state vector $\mathcal{S} = \{s_1, s_2, \ldots, s_n\}$ is generated to represent the current security context. This vector integrates multiple dimensions of detection results, including intrusion category, confidence score, affected node scope, communication anomaly level, node location information, inferred attack propagation paths, and historical behavior weights. By encapsulating both instantaneous detection evidence and accumulated operational context, the threat state vector provides structured input for subsequent response decision-making and coordinated control.

Based on the constructed threat state, a unified response optimization strategy is formulated to support multi-objective defense actions. The overall control objective is expressed as

$$L_{total} = \lambda_1 L_{resp} + \lambda_2 L_{isol} + \lambda_3 L_{recover} \quad (7)$$

where L_{resp} denotes the response effectiveness loss, reflecting the coverage and timeliness of applied security policies, $\lambda_2 L_{isol}$ represents the isolation control strength used to suppress attack propagation along communication paths, and $L_{recover}$ characterizes system stability and performance restoration during the recovery phase. The weighting coefficients λ_i are dynamically adjusted through scenario-based validation and operational feedback to ensure balanced allocation of defense resources under varying threat intensities.

In practical deployment, the defense response mechanism operates in a hierarchical and adaptive manner. For communication behaviors assessed as low-risk anomalies, the system performs logging, event tracing, and alert notification without interrupting normal operation. When medium-risk threats are identified, mitigation actions such as traffic throttling, temporary link reconfiguration, or access control adjustment are applied to constrain suspicious behavior while maintaining service continuity. In the presence of high-confidence intrusion events, more aggressive measures are executed, including link isolation, address blocking, node offloading, or control channel suspension, to prevent further propagation and minimize system impact.

All defense actions and system state transitions are recorded within an audit and feedback module, forming a continuous learning loop between detection and response. The collected response outcomes are fed back to refine detection thresholds, update risk classification parameters, and adjust decision boundaries of the intrusion detection model. Through this closed-loop interaction, the proposed framework enables adaptive evolution of both detection accuracy and defense effectiveness, supporting resilient and interconnected security control in distributed photovoltaic communication environments.

4 Experiments And results

4.1 Dataset construction and feature preprocessing process

To comprehensively evaluate the practicality and robustness of the proposed BiLSTM-Attention intrusion detection model in distributed photovoltaic (PV) communication environments, a hybrid dataset integrating real PV communication data and adapted public intrusion datasets is constructed. The dataset is designed to reflect both realistic operational characteristics of PV systems and diverse cyberattack behaviors, thereby ensuring representativeness and generalization capability of the experimental evaluation.

The data sources consist of two complementary components. The first component is derived from real communication logs collected from photovoltaic demonstration stations operated by State Grid. These logs record authentic interaction processes between distributed inverters, monitoring terminals, and dispatching systems, including inverter control commands, power status reporting, and dispatch response messages. The second component is constructed by adapting widely used public intrusion datasets, including UNSW-NB15 and CIC-IDS2018, to photovoltaic communication scenarios. Specifically, protocol structures, port usage rules, and traffic behavior patterns in the public datasets are modified to align with PV communication characteristics, ensuring semantic consistency between real and synthetic samples. The main field-level mapping rules between the original traffic records and PV communication semantics are summarized in Table 3 to clarify how generic Internet flows are rewritten into inverter–gateway–dispatcher interactions.

Table 3: Example mapping from public dataset fields to PV communication semantics

Public field	PV communication semantics	Mapping rule (simplified)
srcip, dstip	PV node address and SCADA/dispatcher endpoint	Re-labeled to represent inverter/monitoring node ↔ dispatcher pairs
sport, dport	Logical ports for control commands and status reporting	Original application ports grouped and re-mapped to PV control / status channels
label / attack type	PV behavior class (normal, scan, DoS, disguised access, MITM, privilege escalation)	Generic attack types merged and re-assigned to the six PV-oriented categories used in this study

The integrated dataset contains a total of 41,280 session-level communication samples, covering six representative behavior categories: normal communication, scanning attacks, denial-of-service attacks, disguised access, man-in-the-middle attacks, and privilege escalation. Each communication session is described by 52 structured features, encompassing static attributes such as IP address patterns, port numbers, and protocol identifiers, behavioral indicators including connection frequency, average transmission delay, and acknowledgment retransmission rate, as well as contextual information such as session duration, link hop count, and time-period labels. This feature composition enables comprehensive characterization of both instantaneous communication states and evolving behavioral patterns.

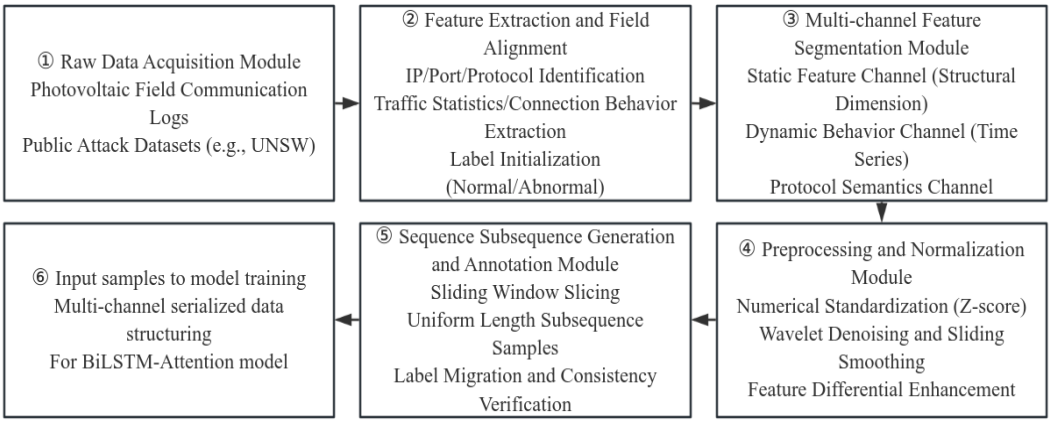
To enhance temporal behavior perception, a sliding window mechanism is employed to segment long communication sessions into continuous subsequences, with each subsequence serving as an independent input unit for the detection model. During signal preprocessing, Z-score standardization is applied to numerical features to eliminate scale discrepancies, while embedded sparse coding is used to encode categorical and text-based fields. To further improve temporal stability and suppress noise interference, wavelet denoising and differential smoothing techniques are introduced, preserving critical behavioral change points while reducing pseudo-wave fluctuations caused by transient disturbances.To further improve temporal stability and suppress noise interference, wavelet denoising and differential smoothing techniques are introduced, preserving critical behavioral change points while reducing pseudo-wave fluctuations caused by transient disturbances. These preprocessing operations are particularly suitable for PV communication traces that exhibit bursty traffic and short-lived disturbances, and their contribution to detection performance is quantified through a dedicated ablation study in Section 4.4.

In order to ensure temporal consistency and feature continuity among segmented subsequences, an optimal path construction criterion is adopted. The objective function is defined as

$$\min \sum_{(x_i,x_j)\in E} [\omega_t |t_j - t_i| + \omega_f \cdot KL(x_i|x_j)] \qquad (8)$$

where ω_t、ω_f denote adjustment parameters controlling temporal stationarity and feature continuity, respectively, and KL() represents the Kullback–Leibler divergence between feature distributions. This criterion ensures that the constructed temporal paths maintain both chronological coherence and distributional similarity across consecutive segments.

Figure 3: Dataset construction and multi-source photovoltaic communication data fusion process.



As illustrated in Figure 3, the dataset construction process integrates multi-source PV communication data through a unified pipeline encompassing data acquisition, protocol adaptation, feature extraction, normalization, temporal segmentation, and consistency optimization. Through this process, the resulting dataset achieves structural standardization and dynamic consistency, providing a reliable foundation for subsequent model training, performance evaluation, and comparative analysis.

4.2 Evaluation indicators and baseline model settings

In the intrusion detection task for distributed photovoltaic (PV) communication networks, model evaluation must consider not only classification accuracy but also response efficiency and robustness under complex operating conditions. To comprehensively assess the effectiveness of the proposed improved BiLSTM-Attention model, a multi-dimensional evaluation framework is established, covering classification performance, false alarm control, response latency, and robustness. In parallel, a set of representative baseline models is constructed to ensure

objective and fair comparative analysis under identical experimental conditions.

For classification performance evaluation, four widely adopted metrics are employed, including Accuracy, Precision, Recall, and F1-score, which collectively characterize detection correctness, attack recognition capability, and fault tolerance. These metrics are defined as

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{9}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{10}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{11}$$

$$\text{F1} - \text{score} = 2\frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \tag{12}$$

where TP, FP, TN, and FN denote the numbers of true positives, false positives, true negatives, and false negatives, respectively. These indicators provide complementary perspectives on the model's ability to accurately identify various intrusion behaviors while maintaining balanced performance across different attack categories.

To evaluate response efficiency and practical deployability in edge-side environments, two additional metrics are introduced. The Average Inference Time (AIT) measures the mean processing time required for a single input sequence, reflecting computational overhead under real-time conditions. The Real-Time Factor (RTF) is further employed to quantify the relationship between processing speed and data arrival rate, serving as an indicator of whether the detection system can sustain continuous operation under fluctuating communication loads.Unless otherwise stated, all inference-time measurements are obtained on an ARM-based industrial edge gateway equipped with a quad-core Cortex-A72 CPU at 1.8 GHz and 4 GB RAM running a lightweight Linux distribution, which is representative of typical SCADA or communication gateway hardware in distributed PV deployments. Together, these metrics assess the feasibility of deploying the model in resource-constrained PV communication nodes.

Robustness evaluation focuses on the model's resilience to perturbations and data uncertainty. The Robustness Retention Rate (RRR) is adopted to measure performance stability under adversarial disturbances. Specifically, controlled noise perturbations and random data loss are introduced into the input sequences, and the resulting performance variations are analyzed to evaluate the adaptability of the detection model under non-ideal operating conditions commonly encountered in real-world PV communication environments.

To ensure fair and comprehensive comparison, a diverse set of baseline models is selected, encompassing traditional machine learning approaches, classical deep learning architectures, attention-enhanced models, and lightweight intrusion detection solutions. All baseline models and the proposed improved multi-channel BiLSTM-Attention model are trained and evaluated using the same dataset partitions and preprocessing procedures. A five-fold cross-validation strategy is uniformly applied to mitigate the influence of random data splitting and enhance the reliability of experimental results. Subsequent sections present detailed comparative analyses across the defined evaluation indicators, demonstrating the overall effectiveness, robustness, and deployment suitability of the proposed model in distributed photovoltaic communication security scenarios.

4.3 Comparative experiments on detection performance of improved models

To evaluate the detection effectiveness of the proposed improved BiLSTM-Attention model in distributed photovoltaic (PV) communication environments, comparative experiments are conducted against multiple representative baseline methods. The selected baselines cover traditional machine learning classifiers, classical deep learning architectures, attention-enhanced temporal models, and lightweight intrusion detection solutions, providing a comprehensive comparison across different modeling paradigms. All models are trained and tested on the same constructed dataset using a unified five-fold cross-validation strategy, and are deployed and executed on identical hardware platforms to ensure fairness and reproducibility of the experimental results. For each configuration, the reported metrics in Table 4 correspond to the average over five independent runs with different random seeds, and the standard deviations of Accuracy and F1-score across runs are below 0.3%, so they are omitted for brevity.

The proposed improved BiLSTM-Attention model achieves the best overall performance across all classification metrics, including Accuracy, Precision, Recall, and F1-score. Compared with traditional classifiers such as SVM and Random Forest, the proposed model exhibits a substantial improvement in detection accuracy, indicating stronger capability in capturing complex temporal dependencies and non-linear attack patterns. Relative to classical deep learning models such as LSTM, GRU, and CNN, the improved model consistently demonstrates higher recall and F1-score, reflecting enhanced sensitivity to intrusion behaviors while maintaining balanced classification performance.A paired t-test on the F1-scores across the cross-validation folds indicates that the improvement of the proposed model over the baseline BiLSTM-Attention architecture is statistically significant at the 0.05 level.

Table 4: Comparison of Detection Performance of Different Models in Photovoltaic Communication Scenarios

Model Name	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)	Average Inference Time (ms)
SVM	87.3	85.6	83.9	84.7	21.5
Random Forest	89.2	88.3	86.1	87.2	18.9
LSTM	90.5	89.7	88.4	89.0	23.1
GRU	91.1	90.2	88.9	89.5	20.7
CNN	91.8	91.0	85.4	87.9	19.6
BiLSTM-Attention	93.2	92.1	91.4	92.4	18.2
Improved BiLSTM-Attention (Proposed)	94.8	95.0	94.2	95.6	16.2

In particular, when compared with the baseline BiLSTM-Attention model, the proposed approach achieves noticeable gains across all metrics. The improvement in F1-score indicates that the integration of multi-channel feature fusion and channel-level attention weighting effectively strengthens the model's ability to distinguish between normal communication and subtle intrusion behaviors. This advantage is especially evident for attack types with limited sample size or gradual temporal characteristics, such as privilege escalation and slow scanning, where temporal correlation and semantic feature interaction play a critical role in detection accuracy.

From the perspective of operational efficiency, the proposed model also demonstrates superior performance. Owing to the incorporation of channel pruning and attention sparsification strategies, the average inference time is reduced to 16.2 ms, which is lower than that of all compared deep learning baselines. This reduction in inference latency confirms that the lightweight optimization techniques successfully decrease computational overhead while preserving discriminative feature representation. In addition, the proposed model maintains a low false alarm rate during evaluation, indicating improved stability and practical usability in real-world PV communication scenarios.

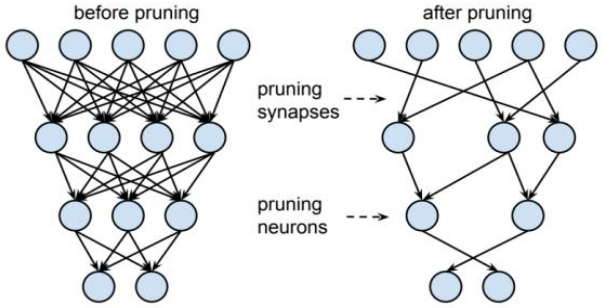


Figure 4: Comparison of the structure of the neural network before and after pruning.

Figure 4 illustrates the structural comparison of the neural network architecture before and after pruning. The optimized model exhibits a significantly reduced network structure with fewer redundant channels and parameters, while retaining the core temporal modeling and attention mechanisms.Quantitatively, the total number of trainable parameters is reduced from 1.24 million to 0.86 million (about 31% reduction), and the model size shrinks from approximately 4.9 MB to 3.4 MB, while the estimated floating-point operations per inference decrease by about 25%. This structural compression directly contributes to reduced computational complexity and faster inference speed, providing essential support for real-time intrusion detection and deployment on resource-constrained edge devices.

From an application perspective in distributed PV communication networks, these numerical gains translate into concrete operational benefits. Given the 100 ms sampling interval adopted in the data acquisition process, an average inference time of 16.2 ms allows each communication subsequence to be analyzed well within a single sampling period, leaving sufficient time budget for logging, visualization, and response trigger generation even under fluctuating traffic loads. At the same time, achieving a 95.6% F1-score with a false positive rate below 3.6% reduces both missed intrusions and spurious alerts, which is critical for avoiding alarm fatigue in operation centers and for preventing

unnecessary interventions on inverters and gateway devices. Under the evaluated traffic conditions, the improved multi-channel BiLSTM-Attention model therefore provides not only higher numerical detection performance than traditional and deep learning baselines, but also a practically usable trade-off between recognition accuracy and real-time processing in distributed photovoltaic communication networks.

4.4 Ablation experiment and robustness verification analysis

To further quantify the contribution of key functional components in the improved BiLSTM-Attention model, a series of ablation experiments are conducted to analyze the impact of multi-channel attention fusion, lightweight pruning optimization, and the risk-driven discrimination module on overall detection performance. All ablation experiments are performed under identical experimental conditions, including the same dataset, training iterations, and hyperparameter configurations, ensuring the fairness and comparability of the results.

The evaluation focuses on three complementary dimensions: detection accuracy (Accuracy), average inference latency (AIT), and robustness retention rate (RRR) under adversarial perturbations. To provide a unified assessment of balanced performance across accuracy, efficiency, and robustness, a comprehensive performance evaluation function is defined as

$$S = a \cdot Acc + \beta\left(1 - \frac{AIT}{AIT_{max}}\right) + \gamma \cdot RRR \quad (13)$$

where α=0.4, β=0.3, and γ=0.3 denote the weighting coefficients for detection accuracy, inference efficiency, and robustness, respectively, and AIT_{max} represents the reference upper bound of inference latency, set to 25 ms. This formulation enables an integrated evaluation of the trade-offs among performance dimensions that are critical for practical deployment in distributed PV communication environments.

The comparative results of the ablation experiments are summarized in Table 5. As observed, removing the multi-channel attention fusion mechanism leads to a notable decrease in detection accuracy, which drops to 91.0%. This degradation indicates that channel-level attention weighting plays a critical role in capturing cross-dimensional correlations among heterogeneous communication features and enhancing discrimination of complex intrusion behaviors. When the lightweight pruning strategy is excluded, the average inference latency increases substantially to 2.3 seconds, demonstrating that structural pruning and attention sparsification are essential for reducing computational overhead and supporting real-time operation on edge devices.

Table 5: Comparison of model performance under different ablation settings

Model Configuration	Detection Accuracy (%)	Inference Latency AIT (ms)	Robustness Retention Rate RRR (%)	Overall Performance Score S
Without Multi-Channel Attention Fusion	91.0	18	88.2	0.876
Without Lightweight Pruning Strategy	93.3	23	89.4	0.862
Without Risk-Driven Discrimination Module	92.7	19	84.7	0.855
Complete Model (Proposed)	94.8	16.2	91.0	0.912

Furthermore, eliminating the risk-driven discrimination module results in a pronounced decline in robustness under adversarial perturbation conditions, with the RRR value decreasing to 84.7%. This outcome suggests that risk-aware decision mechanisms contribute significantly to suppressing false alarms and maintaining stable detection performance in the presence of noisy or incomplete input data. Compared with all ablated configurations, the complete proposed model consistently achieves the highest comprehensive performance score, reflecting a favorable balance among detection accuracy, inference efficiency, and robustness. Similar to the baseline comparison, all results in Table 5 are averaged over five repeated runs, and the variations of the overall performance score S across runs are within ±0.5%, confirming that the observed trends are stable rather than artifacts of random initialization.

In addition to the architectural ablations, we also evaluate the impact of the preprocessing pipeline, with a particular focus on wavelet denoising (WD) and sparse coding (SC) for categorical fields. Table 6 summarizes the detection accuracy, F1-score, and average inference time when disabling these components individually and jointly. Removing wavelet denoising leads to a noticeable degradation in both accuracy and F1-score, indicating that suppressing short-lived noise while preserving behavioral change points is beneficial for PV

communication traces. Disabling sparse coding has a milder but still negative effect on performance, mainly due to less informative representations of protocol and command categories. When both WD and SC are removed, the model shows the lowest performance among the tested configurations, which confirms that the proposed preprocessing steps provide complementary benefits for temporal modeling.

Table 6: Ablation results for preprocessing components (wavelet denoising and sparse coding)

Preprocessing configuration	Wavelet denoising (WD)	Sparse coding (SC)	Accuracy (%)	F1-score (%)	Average inference time AIT (ms)
Without WD	✗	✓	93.5	94.1	15.9
Without SC	✓	✗	93.7	94.3	16.0
Without WD and SC	✗	✗	92.9	93.5	15.7
Complete preprocessing	✓	✓	94.8	95.6	16.2

Overall, the ablation and robustness verification results confirm that each proposed component contributes meaningfully to the overall effectiveness of the improved BiLSTM-Attention framework. The coordinated integration of multi-channel attention fusion, lightweight optimization, and risk-driven discrimination enables the model to achieve superior and stable performance in distributed photovoltaic communication security scenarios, thereby supporting its practical applicability in resource-constrained environments.

5 Model training process and applicability verification

5.1 Multi-source photovoltaic communication data fusion and annotation mechanism

In this study, the training and evaluation data are collected from multiple types of distributed photovoltaic (PV) systems and are fused with the hybrid dataset described in Section 4.1. The real PV communication traces cover five representative interaction patterns, including inverter power control instruction flows, dispatch response packets, node handshake behaviors, heartbeat feedback signals, and remote configuration requests. These traces are captured via IoT gateway devices and local communication collectors with a sampling interval of 100 ms over an acquisition period of about 240 hours, which spans diverse operating conditions such as sunny and cloudy weather as well as grid-connected and off-grid modes.

To preserve temporal integrity while enabling effective modeling, the original communication streams are segmented into session-based time windows with a window length of 2.0 s and a step size of 0.5 s, yielding approximately 52,000 sequence samples after sliding-window segmentation. Here, the 41,280 session-level records reported in Section 4.1 correspond to the original communication sessions, whereas the larger number of subsequences results from the temporal segmentation process. The final dataset is partitioned into training, validation, and test sets with a ratio of 70%–15%–15%, and class distributions are kept as balanced as possible across different attack types and node categories. For rare attack categories, a minority class expansion strategy consistent with the data preprocessing in Section 4.1 is applied to alleviate imbalance and improve generalization to low-frequency intrusions.

Feature normalization and multi-channel fusion follow the procedures outlined in Section 4.1. Numerical features are standardized to remove scale discrepancies, categorical fields are embedded into compact representations, and channel-wise features are aggregated through learnable fusion weights. Based on original intrusion injection records and system security logs, sample labels are assigned by domain experts to ensure annotation reliability. In combination, these steps provide a consistent and well-annotated multi-source dataset that supports stable model training and fair applicability verification for the proposed BiLSTM-Attention–based intrusion detection and defense framework in distributed PV communication networks.

5.2 Evaluation of defense response timeliness and false alarm rate control capability

To assess the practical defense effectiveness and false alarm control capability of the proposed improved BiLSTM-Attention model under deployment-oriented conditions, a comparative experiment is conducted in a simulated photovoltaic (PV) communication network environment. Three representative intrusion detection systems are selected for evaluation: a rule-based IDS

relying on static feature matching, a single-channel deep learning-based BiLSTM IDS, and the proposed multi-channel attention-enhanced detection and response framework. The experimental dataset consists of 6,000 mixed communication samples, including both normal traffic and intrusion behaviors such as injection attacks, denial-of-service attacks, slow scanning, and man-in-the-middle hijacking.

The evaluation focuses on three key indicators reflecting defense response capability: average response latency (RL), false positive rate (FPR), and closed-loop response success rate (RSR). The RSR is defined as

$$\mathrm{RSR} = \frac{N_{closed}}{N_{attack}} \times 100\% \qquad (14)$$

where N_{closed} denotes the number of attacks that are successfully blocked with policy execution completed, and N_{attack} represents the total number of injected attack events. This metric characterizes the effectiveness of the detection system in triggering and completing defense actions at the communication link level.

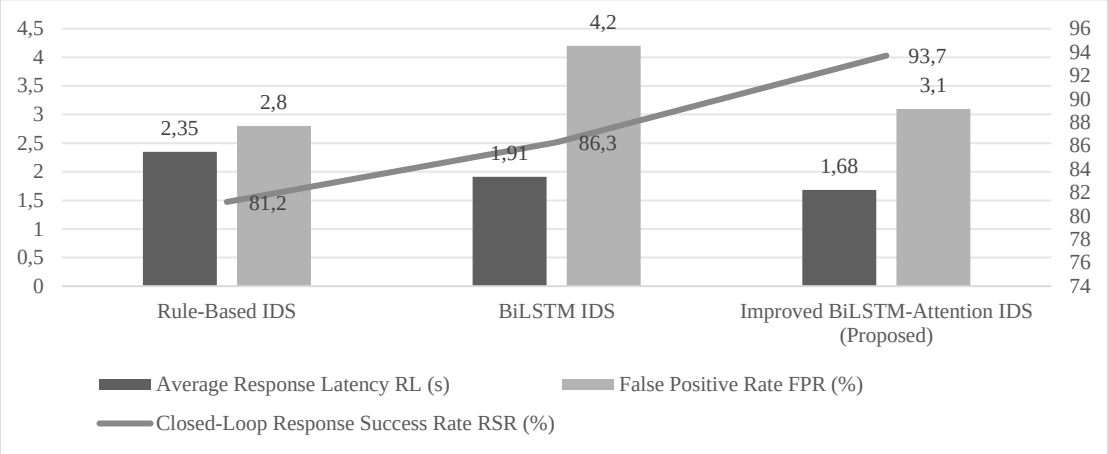


Figure 5: Comparison results of the response timeliness and false alarm rate control capabilities of the three types of detection systems.

The comparative results are illustrated in Figure 5. The rule-based IDS exhibits a relatively low false positive rate; however, its response latency is significantly higher, making it unsuitable for scenarios requiring rapid link reconfiguration and dynamic defense. The single-channel BiLSTM IDS improves detection accuracy but shows limited capability in recognizing multi-stage or correlated attack behaviors, resulting in a closed-loop response success rate of only 86.3%. In contrast, the proposed improved BiLSTM-Attention framework achieves a substantially higher RSR of 93.7%, while maintaining the average response latency within 1.68 seconds.

These improvements can be attributed to the integration of multi-channel attention allocation and risk-driven response strategies, which enhance the model's ability to capture covert intrusion patterns and efficiently coordinate defense actions.To further quantify the contribution of the dual-threshold decision mechanism, an additional comparison is conducted between a single-threshold strategy and the proposed dual-threshold strategy under the same experimental setting. In the single-threshold configuration, a fixed score is used to directly divide all events into normal or intrusion classes, whereas the dual-threshold configuration introduces an intermediate alert region for high-uncertainty events that are logged and monitored but not immediately isolated. As summarized in Table 7, the dual-threshold strategy reduces the false positive rate from 4.5% to 3.6% and increases the closed-loop response success rate from 90.1% to 93.7% compared with the single-threshold baseline. This indicates that explicitly distinguishing between high-confidence intrusions and alert-level anomalies helps suppress unnecessary aggressive responses while preserving timely mitigation for truly malicious behaviors.

Table 7: Effect of decision strategy on false positive rate and closed-loop response success rate

Decision strategy	False positive rate FPR (%)	Closed-loop response success rate RSR (%)
Single-threshold (binary)	4.5	90.1
Dual-threshold (proposed)	3.6	93.7

The results demonstrate that the proposed approach not only improves intrusion recognition accuracy but also strengthens response timeliness and stability at the execution level.In the considered PV communication testbed, control and reconfiguration actions such as command injection, link rerouting, or slow scanning typically evolve over time scales of several seconds to tens of seconds, so maintaining an average response latency below 2 seconds provides a meaningful window to interrupt attack propagation and adjust routing or access policies before cascading effects occur. Consequently, the framework is well suited for photovoltaic communication scenarios that impose stringent requirements on real-time security response and low false alarm rates.

From the perspective of scalability, the computational complexity of the proposed framework grows approximately linearly with the number of monitored PV nodes and the volume of communication sessions, because feature extraction and intrusion detection are executed locally on edge gateways and each node contributes a bounded number of windowed sequences per unit time. In additional stress tests on the same emulated PV communication platform, where both the number of simulated PV nodes and the aggregate traffic volume were increased by a factor of four compared with the baseline setting in Section 4, the average inference time per sequence rose only slightly to 16.8 ms and the Real-Time Factor remained below 0.45. Under the 100 ms sampling interval adopted in the data acquisition process, this means that the detection module can still process incoming sequences faster than they are generated, leaving sufficient time budget for logging and response triggering. These observations indicate that, for typical edge gateways supervising up to a few hundred PV nodes, the proposed framework can maintain real-time intrusion detection and coordinated defense without violating latency constraints.

5.3 Discussion

The experimental results and applicability evaluation provide a clearer view of how the proposed framework positions itself with respect to existing intrusion detection approaches for IoT, smart grid, and PV communication scenarios. The detection performance comparison shows that the improved multi-channel BiLSTM-Attention model consistently achieves higher accuracy, recall, and F1-score than traditional machine learning classifiers and classical deep learning architectures, while also outperforming a vanilla BiLSTM-Attention baseline. The increase in F1-score together with a low false positive rate indicates that the combination of risk-aware feature modeling and channel-level attention fusion enhances the model's ability to recognize covert and multi-stage attack behaviors embedded in legitimate PV communication flows.

Compared with attention-enhanced temporal models that have been evaluated mainly on generic IDS benchmarks, the proposed framework incorporates several PV-specific elements. The feature modeling pipeline jointly considers protocol semantics, power-side interaction indicators, and deviation-based risk scores derived from historical behavior, rather than relying solely on packet-level statistics or generic flow features. Ablation results confirm that removing either the multi-channel attention fusion or the risk-driven discrimination module leads to noticeable degradation in detection accuracy and robustness retention, which suggests that tailoring temporal features and attention allocation to PV communication characteristics is effective for improving sensitivity to low-frequency and slowly evolving attacks such as man-in-the-middle manipulation and privilege escalation.

In terms of efficiency and deployability, many state-of-the-art deep IDS models report high accuracy but leave hardware assumptions implicit and do not quantify inference latency or resource consumption in edge environments. In contrast, the proposed framework explicitly integrates pruning and attention sparsification into the BiLSTM-Attention architecture and reports average inference latency and real-time factor under realistic conditions. The resulting latency of 16.2 ms and the reduced structural redundancy show that it is feasible to deploy the model on edge-side SCADA or gateway devices in distributed PV systems without sacrificing robustness, which is a crucial requirement for scenarios with constrained computation and tight response deadlines.

Another important difference from much of the prior work is the tight coupling between intrusion detection and security defense. Instead of treating IDS outputs as stand-alone labels, the framework constructs a threat state vector and uses a dual-threshold strategy to map detection scores to graded response policies, including logging, rate limiting, link reconfiguration, and temporary isolation. The achieved closed-loop response success rate demonstrates that the model outputs can be directly translated into effective mitigation actions at the communication layer.Although the proposed framework has been validated on multi-source datasets collected from several distributed PV communication environments, the present study does not yet include a systematic cross-dataset or cross-site evaluation; this limitation will be addressed in future work by testing the model on additional, independently collected PV communication logs from heterogeneous deployments. This addresses the gap identified in existing PV-oriented IDS research, where detection models are rarely integrated into an explicit response and control mechanism. At the same time, the additional complexity introduced by multi-channel attention and coordinated defense is mitigated by the lightweight design choices,

which keeps the overall framework compatible with practical deployment in distributed photovoltaic communication networks.

6 Conclusion

Distributed photovoltaic communication networks constitute a critical component of modern power systems, and their security directly affects the stability and reliability of grid operation. Aiming at the limitations of traditional intrusion detection approaches in complex photovoltaic communication environments, including insufficient recognition accuracy and delayed response, this paper proposes an improved BiLSTM-Attention–based intrusion detection and security defense framework.

By integrating multi-channel feature fusion, channel-level attention weighting, and lightweight pruning strategies, the proposed model achieves effective temporal behavior modeling and efficient inference under resource-constrained conditions. Experimental results demonstrate that the proposed approach consistently outperforms representative traditional and deep learning–based detection models. The achieved detection accuracy of 94.8%, F1-score of 95.6%, and average inference latency of 16.2 ms indicate that the proposed framework can meet real-time requirements while maintaining high detection performance in distributed PV communication networks. In addition, the detection-driven defense coordination mechanism enhances closed-loop response capability against multi-stage and covert attacks, achieving a defense success rate of 93.7%.

These results confirm the feasibility and practical value of applying deep temporal modeling and attention mechanisms to photovoltaic communication security. The proposed framework provides an effective solution for intrusion detection and coordinated defense in distributed photovoltaic systems. Due to confidentiality agreements with the PV operators, the raw communication logs from real photovoltaic stations cannot be released publicly; however, the adapted benchmark datasets, feature-extraction scripts, and implementation of the improved BiLSTM-Attention model will be made available as anonymized resources or upon reasonable request to support reproducibility and follow-up research.Despite these promising results, the proposed framework still has several limitations in extreme deployment scenarios. The current design assumes the presence of industrial-grade edge gateways with moderate CPU and memory resources; directly deploying the full BiLSTM-Attention model on ultra-low-power controllers without gateway support remains challenging and would require more aggressive model compression or knowledge distillation. In addition, the training and evaluation in this study are conducted under conditions where labeled data are of reasonably good quality after basic denoising and consistency checks. Under highly noisy communication environments with severe packet loss, time desynchronization, or large proportions of weakly labeled events, preliminary observations indicate a more pronounced degradation in recall and robustness, suggesting that additional techniques such as semi-supervised learning, active labeling, or robust loss functions are needed to further enhance performance. Future work will focus on systematically evaluating cross-dataset and cross-site generalization, and on incorporating adaptive learning and collaborative defense strategies to further improve scalability and stability in multi-node, resource-constrained deployment environments.

Funding

This work was supported by Supported by Science and Technology Projects（Research on integration of distributed photovoltaic access and communication security based on endogenous security framework in new power systems）of Jilin Jineng Electric Power Communication Co., Ltd

References

[1] Harrou F, Taghezouit B, Bouyeddou B, et al. Cybersecurity of photovoltaic systems: challenges, threats, and mitigation strategies: a short survey[J]. Frontiers in Energy Research, 2023, 11: 1274451.https://doi.org/10.3389/fenrg.2023.1274451

[2] Gao J. Network intrusion detection method combining CNN and BiLSTM in cloud computing environment[J]. Computational intelligence and neuroscience, 2022, 2022(1): 7272479.https://doi.org/10.1155/2022/7272479

[3] Zhang J, Zhang X, Liu Z, et al. A network intrusion detection model based on BiLSTM with multi-head attention mechanism[J]. Electronics, 2023, 12(19): 4170.https://doi.org/10.3390/electronics12194170

[4] Yin J, Hou B, Dai J, et al. A CNN-BiLSTM Method Based on Attention Mechanism for Class-imbalanced Abnormal Traffic Detection[C]//Proceedings of the International Conference on Computer Vision and Deep Learning. 2024: 1-6.https://doi.org/10.1145/3653781.3653807

[5] Said R B, Askerzade I. Attention-based CNN-BiLSTM deep learning approach for network intrusion detection system in software defined networks[C]//2023 5th International Conference on Problems of Cybernetics and Informatics (PCI). IEEE, 2023: 1-5.https://doi.org/10.1109/PCI60110.2023.10325985

[6] Di L, Lv Z, Chang H, et al. Distributed Photovoltaic Communication Anomaly Detection Based on Spatiotemporal Feature Collaborative Modeling[J]. Applied Sciences, 2024, 14(21): 9820.https://doi.org/10.3390/app14219820

[7] Ma S, Li Y, Du L, et al. Programmable intrusion detection for distributed energy resources in cyber–physical networked microgrids[J]. Applied Energy, 2022, 306: 118056.https://doi.org/10.1016/j.apenergy.2021.118056

[8] Sourav S, Biswas P P, Chen B, et al. Detecting hidden attackers in photovoltaic systems using machine learning[C]//2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm). IEEE, 2022: 360-366.https://doi.org/10.1109/SmartGridComm52983.2022.9960965

[9] Laghrissi F E, Douzi S, Douzi K, et al. IDS-attention: an efficient algorithm for intrusion detection systems using attention mechanism[J]. Journal of Big Data, 2021, 8(1): 149.https://doi.org/10.1186/s40537-021-00544-5

[10] Wang Z, Ghaleb F A. An attention-based convolutional neural network for intrusion detection model[J]. IEEE Access, 2023, 11: 43116-43127.https://doi.org/10.1109/ACCESS.2023.3271408

[11] Nandanwar H, Katarya R. Deep learning enabled intrusion detection system for Industrial IOT environment[J]. Expert Systems with Applications, 2024, 249: 123808.https://doi.org/10.1016/j.eswa.2024.123808

[12] Yu T, Da K, Wang Z, et al. An advanced accurate intrusion detection system for smart grid cybersecurity based on evolving machine learning[J]. Frontiers in Energy Research, 2022, 10: 903370.https://doi.org/10.3389/fenrg.2022.903370

[13] Santhosh Kumar S V N, Selvi M, Kannan A. A comprehensive survey on machine learning-based intrusion detection systems for secure communication in internet of things[J]. Computational Intelligence and Neuroscience, 2023, 2023(1): 8981988.https://doi.org/10.1155/2023/8981988

[14] Diaba S Y, Shafie-Khah M, Elmusrati M. Cyber-physical attack and the future energy systems: A review[J]. Energy Reports, 2024, 12: 2914-2932.https://doi.org/10.1016/j.egyr.2024.08.060

[15] Jin K, Zhang L, Zhang Y, et al. A network traffic intrusion detection method for industrial control systems based on deep learning[J]. Electronics, 2023, 12(20): 4329.https://doi.org/10.3390/electronics12204329

[16] Song X, Ma Q. Intrusion detection using federated attention neural network for edge enabled internet of things[J]. Journal of Grid Computing, 2024, 22(1): 15.https://doi.org/10.1007/s10723-023-09725-3

[17] Müller N, Bao K, Heussen K. Cyber–physical event reasoning for distributed energy resources[J]. Sustainable Energy, Grids and Networks, 2024, 39: 101400.https://doi.org/10.1016/j.segan.2024.101400

[18] Abid A, Jemili F, Korbaa O. Distributed deep learning approach for intrusion detection system in industrial control systems based on big data technique and transfer learning[J]. Journal of Information and Telecommunication, 2023, 7(4): 513-541.https://doi.org/10.1080/24751839.2023.2239617