applied sciences

MDPI

Article

Distributed Photovoltaic Communication Anomaly Detection Based on Spatiotemporal Feature Collaborative Modeling

Li Di [1,*], Zhuo Lv [2], Hao Chang [2] and Junfei Cai [2]

[1] State Grid Henan Electric Power Company, Zhengzhou 450000, China
[2] State Grid Henan Electric Power Research Institute, Zhengzhou 450000, China; zhuanzhuan2325@sina.com (Z.L.); chandy1994@hotmail.com (H.C.); cai_junfei@163.com (J.C.)
* Correspondence: edwarddi@outlook.com

Abstract: As distributed photovoltaic (PV) technology rapidly develops and is widely applied, the methods of cyberattacks are continuously evolving, posing increasingly severe threats to the communication networks of distributed PV systems. Recent studies have shown that the Transformer model, which effectively integrates global information and handles long-distance dependencies, has garnered significant attention. Based on this, our research proposes a model named STformer, which is applied to the task of attack detection in distributed PV communication. Specifically, we propose a temporal attention mechanism and a variable attention mechanism. The temporal attention mechanism focuses on capturing subtle changes and trends in data sequences over time, ensuring a highly sensitive recognition of patterns inherent in time-series data. In contrast, the variable attention mechanism analyzes the intrinsic relationships and interactions between different variables, uncovering critical correlations that may indicate abnormal behavior or potential attacks. Additionally, we incorporate the Uniform Manifold Approximation and Projection (UMAP) dimensionality reduction technique. This technique not only helps reduce computational complexity but, in certain cases, can enhance anomaly detection performance. Finally, compared to classical and advanced methods, STformer demonstrates satisfactory performance in simulation experiments.

Keywords: photovoltaic microgrid; deep learning; cyberattack detection; attention mechanism

Citation: Di, L.; Lv, Z.; Chang, H.; Cai, J. Distributed Photovoltaic Communication Anomaly Detection Based on Spatiotemporal Feature Collaborative Modeling. *Appl. Sci.* **2024**, *14*, 9820. https://doi.org/10.3390/app14219820

Academic Editor: Rodolfo Dufo-López

Received: 20 August 2024
Revised: 25 September 2024
Accepted: 16 October 2024
Published: 27 October 2024

1. Introduction

Information and Communication Technology (ICT) plays a crucial role in significantly enhancing the communication efficiency of distributed photovoltaic (PV) microgrids. It not only enables the real-time monitoring of energy production through sensor devices [1] but also facilitates the efficient transmission and execution of commands, as well as the implementation of optimized control strategies via computing centers. However, behind this progress lie significant challenges, particularly as the reliance of distributed PV microgrids on ICT deepens, making network security issues increasingly prominent [2].

The high degree of informatization has led to more tightly interconnected distributed photovoltaic (PV) microgrid systems, while also exacerbating their vulnerability to diverse network threats [3]. In particular, sensors and actuators, which form the foundation for data acquisition and operational execution, are essentially embedded computing devices and have become frequent research focuses in recent years due to their high susceptibility to cyberattacks [4]. Additionally, commonly used industrial communication protocols in power systems, such as DNP3, MODBUS, and IEC 61850, have been revealed to contain significant security vulnerabilities, making them prone to network attacks [5]. Through these avenues, attackers can effectively target distributed PV microgrids to alter energy output data or even damage critical infrastructure [2].

There have been numerous discussions on network attack detection techniques for photovoltaic microgrids, which can generally be categorized into two main types: model-based strategies and data-driven approaches. The core of model-based strategies lies in

building system models to perform state prediction. When the deviation between the actual monitoring data and the model prediction exceeds a preset threshold, an attack alarm is triggered. For instance, in reference [6], Kalman filtering technology is used to create a state-space model of the photovoltaic converter, identifying potential network attacks through a statistical analysis of residual variations. To further enhance detection accuracy, some studies have introduced a Harmonic State Space (HSS) model based on power electronic induction, which can effectively detect attack activities even with a limited number of sensors [7]. Reference [8] employs synchronized compressed wavelet transform to construct an attack detection framework suitable for rooftop photovoltaics. Additionally, active defense strategies have also gained attention. For example, in [9], dynamic watermarking technology, utilizing detailed model estimation algorithms, can monitor and counteract malicious tampering attempts on photovoltaic system sensors.While model-based detection methods have demonstrated some value in photovoltaic microgrids, they struggle with the complex and dynamic nature of real-world conditions. Nonlinear relationships, external disturbances, and incomplete data can make it difficult for simple models to accurately describe system behavior, leading to reduced detection accuracy.

Data-driven approaches have made significant progress in the field of anomaly detection and network attack identification. Initially, some classical algorithms were proposed, such as the Local Outlier Factor (LOF) introduced by Breunig et al. [10], which measures the degree of anomaly in data objects and evaluates their performance in local neighborhoods. They further explored the formal properties of LOF, proving that objects within a cluster tend to have LOF values close to 1, while providing tight upper and lower bounds, as well as more precise non-tight limits for other objects. Additionally, the authors proposed a heuristic ranking method based on the maximum LOF value, effectively identifying local anomalies that were difficult to detect with previous methods. One-Class Support Vector Machine (OC-SVM) [11] is another important method used to estimate the support set of high-dimensional distributions. It delineates a "simple" subset of the input space through functions expressed in terms of kernel expansions and controls the length of the weight vector in feature space through regularization, ensuring that the probability of test points drawn from the underlying probability distribution falling outside this subset is predetermined. This method is a natural extension of the Support Vector Machine (SVM) for cases with unlabeled data, efficiently optimizing the constrained minimization problem using the Sequential Minimal Optimization (SMO) algorithm. Choi et al. [12] proposed an unsupervised algorithm based on Gaussian Process Regression and OC-SVM for detecting network attacks in microgrids. This method specifically targets false data injection (FDI) attacks, which manipulate the frequency of distributed generator (DG) inverters to affect microgrid stability. By combining a Gaussian process model to predict DG frequency, and using the prediction error and estimated variance as inputs to the OC-SVM, the accuracy of attack detection was improved. This algorithm does not rely on pre-labeled anomalous data, making it suitable for detecting unknown and unpredictable network attacks. Tax et al. [13] introduced Support Vector Data Description (SVDD), a method inspired by Support Vector Classifiers, for data domain description. SVDD is capable of providing a spherical boundary for datasets and increasing flexibility by using other kernel functions while leveraging negative examples to tighten the description and enhance the detection of outliers and anomalies. This method has played an important role in unsupervised or semi-supervised learning. Gholami et al. [14] proposed an integrated approach combining statistical analysis, clustering techniques, and outlier detection methods for identifying data anomalies in operational measurements. This method demonstrates excellent performance in terms of detection accuracy and Precision while being less reliant on hyperparameter tuning. Ali et al. [15] proposed a data-driven photovoltaic (PV) system state monitoring technique. Using voltage sensors and current sensors for each PV string, they modeled the DC power of PV generators through Gaussian Process Regression (GPR) for nonlinear approximation and calculated the residuals to detect faults. The residuals were processed using an exponentially weighted moving average filter, and fault detection was performed

using Kernel Density Estimation (KDE), with fault diagnosis completed through univariate residual analysis. Although these algorithms demonstrate strong capabilities in identifying local or global characteristics of data, they often struggle to capture temporal correlations when handling time-series data. Additionally, they tend to be sensitive to hyperparameters and have limited ability to process noisy or multi-dimensional data, restricting their direct application in dynamic environments.

In recent years, with the increasing power of deep learning in representation learning, neural network-based models have made significant progress in anomaly detection accuracy and generalization performance. Specifically, Su et al. [16] proposed a Stochastic Recurrent Neural Network (OmniAnomaly) for multivariate time-series anomaly detection. This model learns robust representations of time series through a Stochastic Recurrent Neural Network (SRNN), then reconstructs the input data using these representations, and determines anomalies based on the reconstruction probability. Shen et al. [17] introduced a Time Hierarchical One-Class Network (THOC), a time-series anomaly detection model based on one-class classification. It captures temporal dynamics at different scales using a Dilated Recurrent Neural Network (Dilated RNN) with skip connections and defines multi-scale vector data descriptions through hyper-spheres obtained from hierarchical clustering, improving the model's ability to capture time dynamics. Additionally, the model encourages orthogonality between the hyper-sphere centers and optimizes representation learning through the introduction of a self-supervised task in the temporal domain. Li et al. [18] developed an unsupervised multivariate anomaly detection method based on Generative Adversarial Networks (GANs), using Long Short-Term Memory Networks (LSTM-RNNs) as both the generator and discriminator to capture temporal correlations in time-series data. This method considers the entire set of variables to capture latent interactions between variables, detecting anomalies using a newly defined DR score that combines reconstruction errors and discrimination results. Guo et al. [19] proposed a network attack detection framework specifically designed for photovoltaic power stations. By thoroughly analyzing the frequency and temporal features in historical data, the framework significantly improved detection accuracy and model robustness. Mao et al. [20] introduced an integrated method combining the strengths of LSTM and Convolutional Neural Networks (CNNs), effectively capturing temporal dependencies and performing well in time-series analysis. Additionally, transfer learning, as an effective means of reducing the demand for labeled data, has been applied in attack detection for PV systems. Li et al. [21] proposed a transfer learning method that transfers knowledge learned in one domain to another domain with scarce data, greatly enhancing training efficiency and practical applicability. Peng et al. [22] introduced a Dynamic Spatio-Temporal Graph Neural Network (DST-GNN), which combines Graph Neural Networks (GNNs) with a dynamically weighted adjacency matrix to capture spatial correlations in signal data, while using a one-dimensional Convolutional Neural Network (1D-CNN) to extract temporal patterns. This method dynamically determines the number of graph convolution layers based on system dynamics and adjusts the hyperparameters of the 1D-CNN according to the periodicity of the input signals. In the smart grid domain, Zhe et al. [23] developed a denial-of-service (DoS) attack detection model based on Support Vector Machines (SVMs). The model first collects network data and performs feature selection, followed by Principal Component Analysis (PCA) for dimensionality reduction, and finally detects anomalies using the SVM algorithm, validating the effectiveness of the dimensionality reduction process. Seghiour et al. [24] explored the potential of multi-layer autoencoders (AEs) in anomaly detection, where an AE effectively identifies network attack behaviors by comparing differences between the input and decoded output. These research findings provide critical support for the security of photovoltaic microgrids, advancing data-driven network attack detection technologies, making them more precise, efficient, and adaptive.

This study explores the application of Transformer models in unsupervised time-series anomaly detection. Transformer models have garnered widespread attention due to their significant advancements in fields such as natural language processing, computer vision,

and time-series analysis. Their core advantage lies in their ability to efficiently integrate global information and long-range dependencies. By utilizing the self-attention mechanism of Transformers, we reveal the intricate correlation structures between different time points in time-series data. These correlation structures are reflected in the weight distribution of the self-attention graph, which deeply characterizes the dynamic patterns of time series, including periodicity and trends. It is worth noting that existing Transformer-based models primarily focus on modeling temporal dependencies, often overlooking dependencies between different variables. However, such dependencies are crucial for multivariate time-series anomaly detection. To address this gap, we re-examine the self-attention mechanism from a novel perspective and propose variable attention to capture dependencies between different variables. Furthermore, considering the importance of real-time performance in industrial applications, we employ the Uniform Manifold Approximation and Projection (UMAP) dimensionality reduction technique. This technique not only helps reduce computational complexity but also, in some cases, significantly improves anomaly detection performance. In summary, the main contributions of this paper are as follows:

- Proposed the Time-Block attention module, aimed at efficiently integrating global information and long-range dependencies, thus providing a deep characterization of the dynamic patterns in time-series data.
- Proposed the Variable-Block attention module, aimed at capturing complex interactions between different variables, making it one of the few Transformer models that explicitly explore and utilize cross-variable dependencies for anomaly detection.
- Proposed the STformer framework for unsupervised network attack detection and evaluated its overall performance under DoS attacks and FDIA to validate its effectiveness and feasibility.

2. Network Attacks in Distributed Photovoltaic Microgrids

2.1. Distributed Photovoltaic Microgrid Model

The photovoltaic microgrid model is a small-scale electrical system integrated with photovoltaic generation and energy storage systems, as shown in Figure 1. It can operate independently or be interconnected with the main grid to meet local power demand. This model is based on complex photovoltaic generation systems that utilize photovoltaic cells to capture sunlight and convert it into direct current (DC) electricity. Photovoltaic cells employ different technologies such as monocrystalline silicon and polycrystalline silicon, each with its own efficiency and durability characteristics. To ensure efficient power generation, the photovoltaic microgrid model employs maximum power point tracking (MPPT) control algorithms such as perturb and observe (P&O) and incremental conductance (IncCond), which adjust the operating parameters of the photovoltaic array to maximize power output as sunlight conditions change. DC-DC converters, especially those equipped with insulated gate bipolar transistors (IGBTs), are responsible for seamless energy transfer between the photovoltaic array and the energy storage system. Grid-tied inverters convert DC electricity into alternating current (AC) electricity injectable into the grid and integrate safety mechanisms such as anti-islanding protection. The operation of photovoltaic microgrids heavily relies on real-time monitoring by sensor networks and information transmission through communication channels. Data aggregation equipment (DAE) transmits data packets to the dispatch center of the main grid. Due to the low inertia and fast response time of power electronic devices, even momentary communication delays or denial-of-service (DoS) attacks on sensors can lead to equipment failures and system blackouts. If interconnected with the main grid, these issues may have more severe consequences. The following sections will discuss network attacks and their models in the field of photovoltaic microgrids.

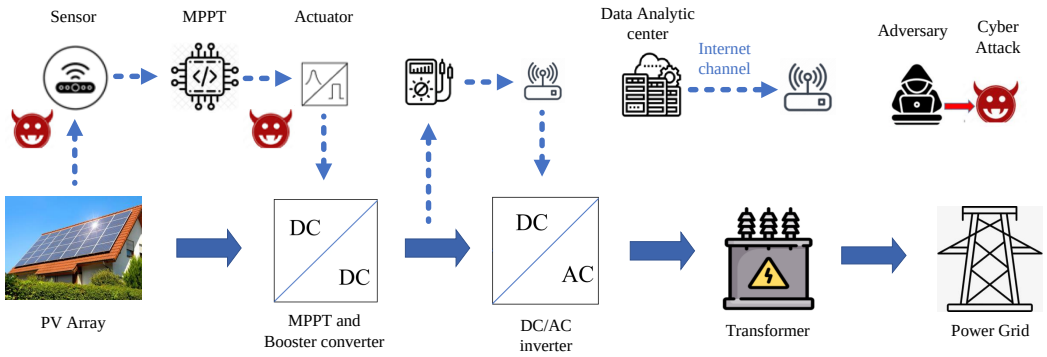

Figure 1. Framework of photovoltaic microgrid energy storage systems and their network attack threats.

2.2. Network Attacks in Photovoltaic Microgrids

False Data Injection Attack (FDIA): The objective of FDIA [25] is to disrupt the normal operation of the system by injecting erroneous data into it. Attackers can manipulate sensor data or data packets in communication channels to provide the control center with incorrect system state information, leading to erroneous decision-making and control operations. In photovoltaic microgrids, attackers may tamper with data related to photovoltaic generation, energy storage status, or grid connection status, causing the system to incorrectly schedule and allocate power resources. Specifically, attackers may launch FDIA against sensors monitoring current, voltage, and power within the photovoltaic array and converters. These sensors utilize the Electromagnetic Interference (EMI) method. As described in [26], the attack model is represented by Equation (1).

$$\begin{cases} V_A = a_V(V_o + A_V) \\ I_A = a_I(I_o + A_I) \\ P_A = a_P(P_o + A_P) \end{cases} \tag{1}$$

In this context, V_A, I_A, and P_A, respectively, represent the measured values of voltage, current, and power output within the target device by the attacked sensors. a_V, a_I, and a_P denote arbitrary attack multipliers for the measurements of different sensors. A_V, A_I, and A_P represent arbitrary attack additions for the measurements of different sensors. This amplification and biasing result in the malicious manipulation of the original measured values V_o, I_o, and P_o of voltage, current, and power, respectively. As a consequence, sensor monitoring is manipulated, leading to the disruption of normal operations, and, potentially, the direct shutdown or damage to the equipment. However, FDIA is subject to intensity constraints and must be carefully designed to maintain stealthiness. The values and rates of change of the attack signal must fall within acceptable ranges; otherwise, the attack will fail to evade defense mechanisms and lead to failure. It is worth noting that stealthy FDIA poses challenges to detection tasks. For example, for voltage sensors, the attack must satisfy the constraints described in Equation (2) as described in [26].

$$\begin{aligned} |V_A| &< V_{MAX} \\ \left|\frac{dV_A}{dt}\right| &< R_{MAX} \end{aligned} \tag{2}$$

where V_{MAX} represents the acceptable magnitude of the attacked voltage measurement, and R_{MAX} is the maximum value of the rate of change.

Denial-of-Service Attack (DoS): A DoS attack [26] aims to disrupt the normal functioning of a system by rendering certain parts of it inaccessible. Attackers achieve this by flooding the system with a large volume of useless data packets or exploiting vulnerabilities to overload critical components (such as sensors or communication networks), rendering them unable to function properly. In a photovoltaic microgrid, a DoS attack may prevent

the control center from obtaining real-time data, thereby impacting the overall operational efficiency and stability of the system. This type of attack can be represented by Equation (3), as described in [26].

$$x(k) = \begin{cases} x(k) & k \leq k_a \\ x(k_a) & k \geq k_a \end{cases} \tag{3}$$

where x represents the data of monitoring or control commands. k is the time index, and k_a is the time index when the DoS attack begins. In the field of photovoltaic microgrids, DoS attacks may pose a serious threat to the operational safety of damaged equipment. For instance, interruptions in voltage sensors within the photovoltaic array and corresponding inverters can disrupt MPPT control, significantly impacting photovoltaic power output and causing deviations in DC bus voltage. Consequently, efficient detection and defense mechanisms need to be researched and developed to safeguard the secure operation of photovoltaic microgrids against common network attacks such as FDIA and DoS.

2.3. UMAP Theory

To enhance the model's effectiveness in anomaly detection tasks and focus on the most relevant features, we adopted the advanced dimensionality reduction technique, Uniform Manifold Approximation and Projection (UMAP) [27]. UMAP is particularly suitable for handling high-dimensional data because it effectively reduces the dimensionality while preserving both local and global structures of the data, thus providing concise and information-rich input features for subsequent anomaly detection.

The theoretical foundation of UMAP stems from manifold learning, aiming to preserve the neighborhood relationships in high-dimensional data so that data points with similar characteristics remain adjacent in the low-dimensional space. Compared to traditional dimensionality reduction methods such as Principal Component Analysis (PCA), UMAP is better suited for dealing with non-linear data structures. It not only retains local neighborhood relationships but also maintains a global topological structure, making it particularly effective for visualization and feature extraction from high-dimensional data, especially for capturing key patterns in complex time series.

The UMAP process can be divided into two main steps: first, learning the manifold structure of the data in the high-dimensional space, and second, projecting this manifold into a low-dimensional space. This entire process is based on a series of mathematical operations and is finalized through optimization techniques to achieve the low-dimensional representation of the data. During the manifold structure learning phase in the high-dimensional space, UMAP employs the Nearest-Neighbor Descent algorithm [28] to identify each data point's nearest neighbors. After identifying these neighbors, UMAP constructs a neighborhood graph to further capture the manifold structure of the data. To better reflect the local characteristics of the data, UMAP assumes that data points are uniformly distributed on the manifold and adjusts the distance metric between different regions adaptively. This means that the distances between data points dynamically change based on the density of the regions they reside in, allowing the algorithm to adapt to both sparse and dense areas, and ensuring compatibility with both local and global patterns. Moreover, to prevent disconnected points in the learned manifold structure, UMAP introduces a mechanism to ensure that all points maintain meaningful connections. For this purpose, UMAP assigns weights to the edges of the graph, with the weights reflecting the similarity between data points, and further optimizes these connections through a probabilistic framework. Since UMAP employs adaptive distance metrics, the edge weights between different pairs of points may be asymmetric. UMAP symmetrizes these edge weights to ensure the symmetry of the neighborhood graph, thereby more accurately representing the relationships between data points. Once the manifold structure in the high-dimensional space is learned, UMAP proceeds to the second step, which is to find a low-dimensional representation of the data. In this process, UMAP aims to preserve the manifold structure of the high-dimensional data as much as possible while minimizing the changes in distances between data points. UMAP optimizes the low-dimensional embedding by minimizing a cross-entropy objective

function to find the optimal weights for the edges in the low-dimensional space. These weights are obtained by minimizing the cross-entropy function, as described in Equation (4) from [27]:

$$C(Y) = \sum_{i,j} v_{ij} \log\left(\frac{1}{1 + a \parallel y_i - y_j \parallel^{2b}}\right) + (1 - v_{ij}) \log\left(1 - \frac{1}{1 + a \parallel y_i - y_j \parallel^{2b}}\right) \quad (4)$$

where v_{ij} represents the proximity probability between data points i and j in the high-dimensional space, reflecting the similarity or connection strength between them; $\parallel y_i - y_j \parallel$ denotes the Euclidean distance between data points y_i and y_j in the low-dimensional space, used to measure their relative positions in the new representation. Parameters a and b are tuning factors: a controls the overall scaling of the distance term, while b influences how the distance is translated into a weight for similarity. Together, these parameters help balance the preservation of local structure with the integrity of the global structure.

3. Methods

3.1. Overview

The challenge of unsupervised time-series anomaly detection lies in accurately identifying whether a segment of evenly spaced time series $x_{1:L} = \{x_1, x_2, ..., x_L\} \in R^{L \times N}$ contains anomalies without labeled data. Here, L represents the number of time steps in the input, and N denotes the number of variables considered. Inspired by the DaViT model, we propose a novel method called STformer, as illustrated in Figure 2. The uniqueness of this model lies in its ability to simultaneously capture complex patterns within both the temporal and feature (channel) dimensions of time-series data. It also integrates the Uniform Manifold Approximation and Projection (UMAP) technique—an efficient dimensionality reduction method—further enhancing the model's performance and making it suitable for real-time processing in practical applications. Specifically, we first apply UMAP to reduce the original N-dimensional time-series data to M-dimensions ($M < N$), resulting in the simplified dataset $x_{1:L} \in R^{L \times N}$. This step preserves the most important features while eliminating unnecessary data redundancy, thus improving the overall efficiency of anomaly detection. Next, we perform an embedding operation on the M-dimensional dataset $x_{1:L} \in R^{L \times N}$, mapping it into a higher-dimensional space. This embedding process enables us to capture the intricate interactions between the temporal and feature dimensions while retaining critical time-series patterns. By mapping the features of each time step into a higher-dimensional space, the model is better equipped to learn complex patterns. Then, we introduce the Time-Block component to specifically analyze temporal dependencies within the time series, enhancing the understanding of how data evolves over time. Following this, the Variable-Block module explores the interactions and dependencies between different variables, a crucial step for fully grasping the hidden complex mechanisms underlying time-series data. The overall structure of the model is formalized in Equation (5) as follows:

$$\begin{aligned} x^0 &= Embeding(UMAP(x_{in})) \\ x^k &= \text{Time} - \text{Block}(x^{k-1}) \\ x_{out} &= \text{Variable} - \text{Block}(k^s) \end{aligned} \quad (5)$$

where the initialization of the input is denoted as $x_{in} \in R^{L \times N}$. Embedding linearly projects x_{in} to $x_u^0 \in R^{L \times d_{model}}$. $x^k \in \mathbb{R}^{L \times d_{\text{model}}}$ represents the output of the Time Block. By minimizing the reconstruction error, the loss value decreases, and the model parameters are updated. The loss function is defined as shown in Equation (6). The training process is as shown in Algorithm 1.

$$loss = ||x_{in} - x_{out}||^2 \quad (6)$$

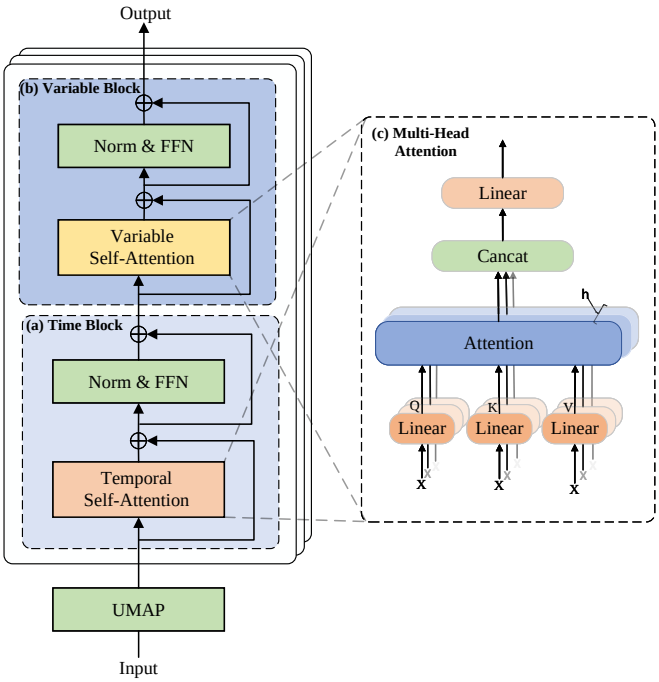

Figure 2. The architecture of STformer primarily includes the UMAP module, Time Block, and Variable Block.

Algorithm 1: Training algorithm

Input: Input sample x_{in}
Output: Output value x_{out}
for $i = 1$ *to epoch* **do**
  for $j = 1$ *to batch* **do**
    x_0^j = Embedding(UMAP(x_{in}^j));
    for $k = 1$ *to* K **do**
      x_k^j = Time-Block(x_{k-1}^j);
      x_k^j = Variable-Block(x_k^j);
    end
    Update model parameters;
  end
end

In Algorithm 1, the term epoch refers to the number of iterations of model training. In each epoch, the data are divided into several equal-sized batches, and the data in each batch are used to compute the loss value and update the model parameters once using an optimizer. Here, K represents the number of Time Blocks and Variable Blocks in STformer. During the testing phase, the process of anomaly detection algorithm is as shown in Algorithm 2.

In Algorithm 2, x_{train} represents training data, x_{val} represents validation data, and x_{test} represents test data. Initially, the training data are fed into the model to obtain model-generated training data. Subsequently, the error between the training data and the generated data is computed. Following this, the same process is repeated with validation data to calculate the error between the validation data and the generated data. Next, the errors of the training and validation data are proportionally divided, with a threshold (thresh) set as the boundary between the top 1% and the remaining 99% of error values. Finally, the error of the test data is calculated and classified according to Equation (7): data with errors greater than the threshold (thresh) are classified as abnormal, while data with errors less than or equal to the threshold are classified as normal.

$$\begin{aligned} \|pred_{\text{test}} - X_{\text{test}}\|_F^2 > thresh \\ \|pred_{\text{test}} - X_{\text{test}}\|_F^2 \leq thresh \end{aligned} \tag{7}$$

Algorithm 2: Test algorithm

Input: Training data x_{train}, validation data x_{val}, testing data x_{test}.

```
for i = 1 to batch do
    pred_train = STformer(x_train);
    loss_train = pred_train − x_train;
end
for i=1 to batch do
    pred_val = STformer(x_val);
    loss_val = pred_val − x_val;
end
thresh = np.percentile(loss_train, loss_val, 99);
for i = 1 to batch do
    pred_test = STformer(x_test);
    loss_test = pred_test − x_test;
    if loss_test > thresh then
        Anomalous
    else
        Normal
    end
end
```

3.2. Preliminaries

Attention mechanisms mimic how humans allocate attentional resources, focusing on key areas while reducing attention to other areas, in order to extract more relevant information and filter out distracting information. Single-headed attention mechanisms tend to focus on a single point, limiting their ability to capture multiple important fragments of information in the input and process diverse contextual information simultaneously. In contrast, multi-headed attention mechanisms concentrate attention across different dimensions, enabling them to capture more comprehensive and nuanced feature representations. In this mechanism, each attention head acts like a feature detector, concentrating on capturing different local features [29]. In our study, we adopted the scaled dot-product attention mechanism. This mechanism uses a dot-product function to map queries (Q), keys (K), and values (V) to outputs, where Q, K, V, and the output are all represented in matrix form. Specifically, this mapping mechanism can be described by the following Formula (8):

$$\begin{aligned} Q &= X_{in} W_Q \\ K &= X_{in} W_K \\ V &= X_{in} W_V \end{aligned} \tag{8}$$

where W_Q, W_K, and $W_V \in R^{d_{model} \times d_{model}}$ represent parameter matrices for the scientific department, $X_{in} \in R^{L \times d_{model}}$, $Q \in R^{L \times d_{model}}$ represents the query matrix, $K \in R^{L \times d_{model}}$ represents the key matrix, and $V \in R^{L \times d_{model}}$ represents the value matrix.

To compute the attention output, the following steps should be followed: Given the Q, the K, the V, and the scaling factor d_{model}, the computation process is as follows. First, compute the dot product between the Q and the transpose of the K to generate similarity scores between each Q and K. To prevent issues with large numerical values leading to gradient vanishing, scale the dot product results by dividing by the d_{model}. Next, apply the Softmax function to the scaled results for normalization, converting the similarity scores into weights that reflect the importance of each K to the corresponding Q. Finally, use

these weights to perform a weighted sum of the V to obtain the final attention output. This process can be represented by Formula (9):

$$Attention(Q, K, V) = Softmax(\frac{QK^T}{\sqrt{d_{model}}})V \tag{9}$$

This study employs a multi-head self-attention mechanism, as shown in Figure 2c. It demonstrates excellent performance in feature extraction while maintaining the same number of parameters. Here, "self-attention" refers to linearly projecting queries (Q), keys (K), and values (V) from the same input matrix $X_{in} \in R^{L \times d_{model}}$. The concept of "multi-headed" implies splitting the output into h-independent blocks (referred to as heads) along the channel dimension, with each block employing different projection weights. Subsequently, the diverse outputs from individual single-headed self-attention mechanisms are concatenated along the channel dimension. Introducing this multi-headed self-attention mechanism is of significant importance for enhancing feature extraction capabilities and capturing complex relationships within the input data. This process can be described by Equation (10).

$$\begin{aligned} head_i &= Attention(Q_i, \quad K_i, \quad V_i) \\ MHSA(X_{in}, X_{in}, X_{in}) &= Concat(head_1, head_2, \ldots, head_h)w^0 \end{aligned} \tag{10}$$

where Q_i, K_i, and $V_i \in \mathbb{R}^{L \times \frac{d_{\text{model}}}{h}}$, respectively, represent the query matrix, key matrix, and value matrix for each attention head. $\text{head}_i \in \mathbb{R}^{L \times \frac{d_{\text{model}}}{h}}$ represents the output of the $i-$th attention head. To combine the results of all attention heads, we introduce an additional weighted matrix $w^0 \in \mathbb{R}^{d_{\text{model}} \times d_{\text{model}}}$.

3.3. Time Block

To model the complex dynamic characteristics of time-dependent relationships in distributed photovoltaic grids, we propose the Time-Block component. Its purpose is to capture both long- and short-term dependencies in time series through a multi-headed self-attention mechanism, while dynamically optimizing weight allocation based on input. The architecture is depicted in Figure 2a. Specifically, the Time Block comprises a multi-headed self-attention mechanism (MHSA), layer normalization with residual design, and a feedforward network.

Assuming we have S Time Blocks, where the input of the s-th Time Block is $X^{en}_{s-1} = \text{Time} - \text{Block}(X^{en}_{s-2})$, the expression for the Time Block is given in Equation (11):

$$\begin{aligned} z^s_T &= Layer - Norm(MHSA(x^{s-1}) + x^{s-1}) \\ x^s &= Layer - Norm(Feedward(z^s_T) + z^s_T) \end{aligned} \tag{11}$$

where $x^{s-1} \in R^{L \times d_{model}}$ represents the input of the Time Block, and $x^s \in R^{L \times d_{model}}$ represents the output of the Time Block. Layer normalization (Layer-Norm) can alleviate issues like gradient vanishing or exploding, while also enhancing the efficiency of neural network training. FeedForward denotes a multi-layer feedforward network.

3.4. Variable Block

We reexamine the self-attention mechanism from a new perspective and introduce Variable Attention, as shown in Figure 2b. In past time-series analyses, self-attention mechanisms mainly focused on the dynamic changes and long-term dependencies exhibited by time series over time, meaning they primarily allocated attention weights along the time dimension. However, our proposed Variable Attention mechanism aims to consider not only the temporal correlations through Time Blocks in multivariate time-series data but also emphasizes the importance and interactions among different variables. This implies that, at any given time point, the model will not only focus on which past time points have the

greatest impact on the current time point but also on which variables among all observed variables are crucial for understanding the entire data pattern. This approach enhances the model's ability to filter key information in complex data structures, particularly in cases where significant interactions exist among variables.

Assuming we have S Variable Blocks, where the input of the $s-$th Variable Block is $X_{s-1}^{en} = Variable - Block(X_{s-2}^{en})$, the expression for the Variable Block is given in Equation (12):

$$\begin{aligned} x_v^{s-1} &= Permute(x^{s-1}) \\ z_v^s &= Layer - Norm(MHSA(x_v^{s-1}) + x_v^{s-1}) \\ x_v^s &= Layer - Norm(Feedward(z_v^s) + z_v^s) \\ x^s &= Permute(x_v^s) \end{aligned} \tag{12}$$

where $x^{s-1} \in R^{L \times d_{model}}$; the Permute function exchanges the first and second dimensions, resulting in $x_v^{s-1} \in R^{d_{model} \times L}$. $z_v^s, x_v^s \in R^{d_{model} \times L}$. After obtaining x_v^s , applying the Permute function exchanges the first and second dimensions again, resulting in $x^s \in R^{L \times d_{model}}$.

4. Experiment

4.1. Data Sources and Simulation Setup

To validate the effectiveness of our proposed algorithm for detecting communication anomalies in distributed photovoltaic power generation systems, we constructed a simulation model using the Simulink environment of MATLAB R2021b. This model, referred to as Case 1, is illustrated in Figure 1. This microgrid model was connected to a 380 V grid to ensure constant power output and integrated a 200 Ah energy storage battery with accompanying converters. The 380V DC bus was responsible for mediating the flow of electrical energy between the photovoltaic array and the grid-connected inverter. The simulated experiment was set to run under conditions of solar irradiance ranging from 800 to 1500 W/m² and an ambient temperature of 25 °C. The monitored parameters were summarized as a vector x, as shown in Equation (13):

$$x = \{V_{PV}, I_{PV}, P_{PV}, V_{DC}, I_{DC}, P_T, V_B, I_B, S_B\} \tag{13}$$

where V_{PV}, I_{PV}, and P_T are the measured values of voltage, current, and power output of the photovoltaic array, respectively; V_{DC} and I_{DC} are the measured values of voltage and current of the DC bus; P_T is the measured power transmission from the microgrid to the 380V grid; V_B,I_B, and S_B are the measured values of voltage, current, and state of charge of the battery, respectively.

For the detection task, we developed a 2-second sliding time window, generating a time series every 2 s. The dataset includes 3000 s of simulated results (totaling 15,000 scenarios), covering common features of the operational process, with a sampling frequency of 5 samples per second. To validate the effectiveness of the detection method under different conditions, we applied signal interference with an amplitude of 10–40% of the sensor's maximum measurement value to V_{PV}, I_{PV}, and P_T every 2 s across a total of 1500 scenarios, while conducting a denial-of-service (DoS) attack every 4 s. The dataset was divided into 70% for training, 10% for validation, and 20% for testing the network's performance.

To enhance the reliability of the results, we employed various network attack identification and classification mechanisms proposed by Zhang et al. [30], and, on this basis, we introduced an additional simulation experiment, referred to as "Case 2", for evaluation on the IEEE 39-bus test system. This power system consists of 10 generators, 39 buses, and 46 lines, with detailed topological models and parameters available in the study by Moeini et al. [31]. To assess the power system's response to disturbances, we applied a power change (active power of 20 MW and reactive power of 0.2 MVar) at the end of the line between bus 3 and bus 4, close to bus 3. The disturbance lasted from $\tau = 0.2$ s to $\tau = 0.4$ s.

Based on the above state responses, various random network attacks were generated as the training dataset for the proposed neural network. For stealthy False Data Injection Attacks (FDIAs), the randomness depends on the construction algorithm and boundary constraints. In this paper, the maximum allowable threshold for bad data detection is listed in Table 1. The randomness of replay attacks lies in the start and end times of the recording and replay. The randomness of the periodic denial-of-service (DoS) attack is reflected in sleep time. The randomness of delay attacks is reflected in the random delays. The randomness of spoofing attacks is characterized by the attack probability and the upper limit of nonlinearity.

Table 1. The boundary restrictions of BDD.

Boundary	Pmax	Pmin	Qmax	Qmin	pmax
Value	1.5 P	0.5 P	1.5 QP	0.5 QP	1.5 P
Boundary	qmax	Vmax	Vmin	θ max	θ min
Value	1.5 q	1.2 p.u.	0.8 p.u.	15°	−15°

In this paper, we set the channel number of the hidden state d_{model} to 32 and used the Adam optimizer with an initial learning rate of 10^{-4}. The batch size was set to 64. The experiments were conducted on a hardware platform equipped with an Intel Core i7-13700KF CPU (Intel, Santa Clara, CA, USA) and accelerated using an NVIDIA GeForce RTX 4070Ti GPU (Nvidia, Santa Clara, CA, USA). The software platform was implemented using Python 3.10 and the PyTorch 2.1.1framework. To ensure that each variable had a fair impact on the model and to avoid certain variables dominating the results due to differences in scale, we applied mean–variance normalization to the raw data. Specifically, for each feature x, we first computed its sample mean μ and standard deviation σ, and then used the formula $x' = \frac{x-\mu}{\sigma}$ to transform the feature into a new one with zero mean and unit variance. This normalization method ensures that all input features are on the same scale, allowing the model to more objectively evaluate the importance of each feature. In this way, our model can more effectively learn the complex patterns in time-series data without being dominated by the scale of specific variables.

To evaluate the performance of the model, we used Precision, Recall, and F1-score as evaluation metrics. The formulas for these metrics are shown in Equation (14):

$$\begin{aligned} Precision &= \frac{TP}{TP+FP} \\ Recall &= \frac{TP}{TP+FP} \\ F1\text{-}score &= 2 \times \frac{Precision \times Recall}{Precision + Recall} \end{aligned} \tag{14}$$

where true positive (TP) is the number of detected attack scenarios, True Negative (TN) is the number of normal scenarios where no alarm is triggered, false positive (FP) is the number of normal scenarios where an alarm is incorrectly triggered, and False Negative (FN) is the number of attack scenarios that were not detected.

4.2. Experiment Results

To comprehensively evaluate the performance of the STformer model in anomaly detection tasks, we meticulously designed a series of experiments and compared it with 10 different baseline methods. These baseline methods included OCSVM [32], Deep-SVDD [33], VAR [34], LSTM [35], LSTM-VAE [36], BeatGAN [37], OmniAnomaly [16], InterFusion [16], THOC [17], and LSSL [38].

According to Table 2, STformer performs exceptionally well in the anomaly detection task, achieving a Precision of 98.19%, which significantly surpasses other methods. This

indicates STformer's notable advantage in reducing false positives and ensuring prediction reliability. Its Recall rate of 96.76% is also among the top, highlighting STformer's ability to identify more true positives and enhance detection comprehensiveness. With an F1-score of 97.47%, STformer excels in balancing Precision and Recall, showcasing its superior accuracy and comprehensive detection capability. Although OmniAnomaly and InterFusion also perform well in terms of Precision and F1-score, they do not match STformer's overall balance. Other methods, such as LSSL and THOC, also show strong performance but still fall short of STformer's outstanding metrics. Overall, STformer outperforms all evaluated models, and Figure 3 clearly illustrates that the proposed model excels in Precision, Recall, and F1-score compared to baseline models.

Table 2. Performance comparison of STformer and 10 baseline methods in Case 1.

Models	Precision	Recall	F1-Score
OCSVM	85.13	84.93	85.03
Deep-SVDD	88.45	90.97	89.69
VAR	89.02	86.37	87.67
LSTM	89.77	88.52	89.14
LSTM-VAE	91.98	94.72	93.33
BeatGAN	88.31	96.24	92.10
OmniAnomaly	98.01	93.25	95.57
InterFusion	97.93	94.15	96.00
THOC	93.12	98.31	95.72
LSSL	90.17	96.42	93.19
Ours	98.19	96.76	97.47

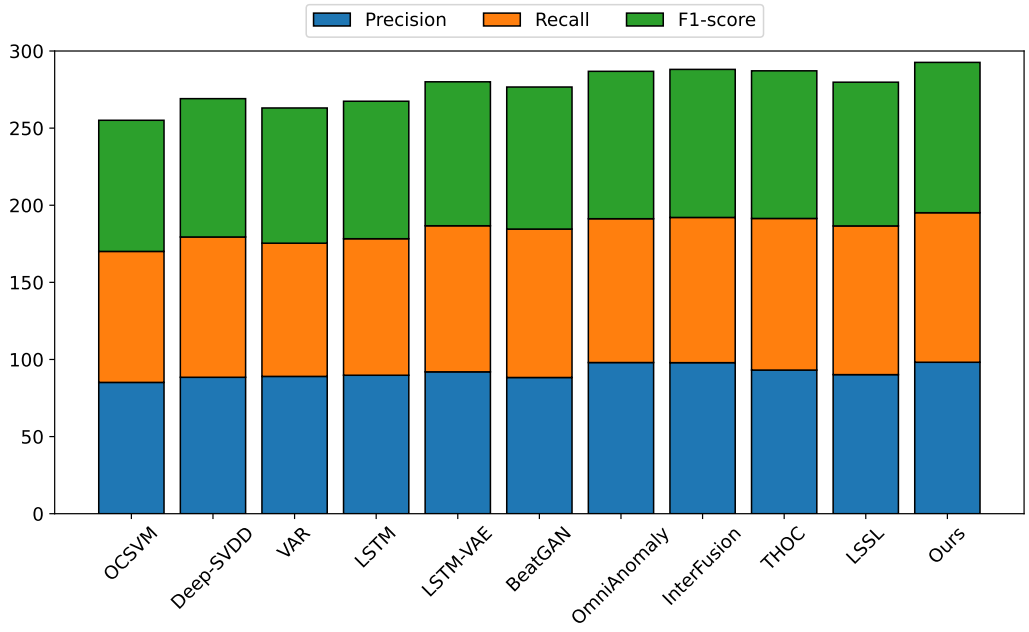

Figure 3. Comparison of Precision, Recall, and F1-score of anomaly detection models in Case 1.

In Case 2, we evaluated the performance of the STformer model against 10 baseline methods in the anomaly detection task. Table 3 presents the performance of each model in terms of Precision, Recall, and F1-score. The STformer model excels across all evaluation metrics. Specifically, STformer achieves a Precision of 99.07%, which is significantly higher

than other methods, indicating its effectiveness in reducing false positives and ensuring the high reliability of predicted positives. Additionally, STformer has a Recall of 98.68%, also ranking among the top compared to all baseline methods, meaning that it identifies more true positives and enhances the comprehensiveness of anomaly detection. Considering the balance between Precision and Recall, STformer's F1-score of 98.87% reflects its exceptional capability in accurate prediction and comprehensive detection. Among the baseline methods, OmniAnomaly and InterFusion also perform remarkably well. OmniAnomaly has a Recall of 96.88% and an F1-score of 97.32%, ranking high in these metrics. InterFusion shows strong performance as well, with a Recall of 97.13% and an F1-score of 97.99%, although its Precision of 98.87% is slightly lower than that of STformer. Other methods like LSSL and THOC also perform well, with LSSL achieving a Precision and F1-score of 95.36% and 96.71%, respectively, and THOC with a Precision and F1-score of 94.49% and 95.23%. Although LSTM-VAE and BeatGAN show good performance in anomaly detection, their Precision and F1-scores do not reach the level of STformer. LSTM-VAE has a Precision of 92.83% and an F1-score of 91.98%, while BeatGAN achieves a Precision of 90.35% and an F1-score of 92.32%. The VAR model has relatively lower Precision and Recall, at 84.52% and 82.88%, respectively, indicating its limitations in the anomaly detection task.

Table 3. Performance comparison of STformer and 10 baseline methods in Case 2.

Models	Precision	Recall	F1-Score
OCSVM	87.61	88.29	87.95
Deep-SVDD	88.09	88.17	88.13
VAR	84.52	82.88	83.69
LSTM	89.99	90.89	90.89
LSTM-VAE	92.83	91.15	91.98
BeatGAN	90.35	94.37	92.32
OmniAnomaly	97.76	96.88	97.32
InterFusion	98.87	97.13	97.99
THOC	94.49	95.23	94.86
LSSL	95.36	96.71	96.03
Ours	99.07	98.68	98.87

4.3. Impact of Dimensionality Reduction

To further explore the impact of dimensionality reduction techniques on model performance, we applied dimensionality reduction to the dataset, specifically reducing it to 4, 6, and 8 dimensions, and recorded the detailed experimental results (see Table 4). It is noteworthy that the impact of dimensionality reduction on model performance is not uniform; in fact, when the dataset dimensions were reduced to 6, we observed an effective improvement in the F1-score. This improvement indicates that reducing the data complexity to a moderate level can help the model focus more on the most critical features closely related to anomaly detection, thereby effectively enhancing the model's recognition ability and accuracy.

Table 4. Effect of dimensionality reduction on performance of Case 1.

Dimensions Remaining	Precision	Recall	F1-Score
4	97.31	97.16	97.23
6	98.19	96.76	97.47
8	98.37	95.97	97.15
Original	97.82	96.76	97.29

4.4. Ablation Study

To systematically analyze the necessity and contribution of each component in our approach, we adopted a strategy of gradually removing individual components and meticulously recorded the changes in model performance after each removal. First, we removed the UMAP (Uniform Manifold Approximation and Projection) dimensionality reduction step and labeled this version of the model as "-WO-UMAP". This allowed us to assess whether UMAP dimensionality reduction had a significant impact on the overall performance of STformer. Next, we removed the Time-Block function and labeled this version of the model as "-WO-Time-Block" to investigate the extent to which the temporal attention mechanism affects the overall model performance. Finally, we removed the Variable Block from the model and labeled it as "-WO-Variable-Block" to evaluate the contribution of the unique design that considers correlations among variables to the model's performance. Through these steps, we were able to gain a detailed understanding of the importance of each component to the overall model performance and the specific roles they each play.

Table 5 summarizes the performance results of different ablation variants. First, after removing UMAP, the Precision was 97.82%, Recall was 96.76%, and F1-score was 97.29%. Compared to the complete model, removing UMAP led to a slight decrease in F1-score from 97.47% to 97.29%. This suggests that, while UMAP is not a decisive component, it helps select a small set of representative features from a large pool, thereby reducing the computational burden and slightly enhancing model performance. Next, after removing the Time Block, Precision dropped to 91.88%, Recall was 94.73%, and F1-score was 93.29%. This result clearly demonstrates that the Time Block is crucial for capturing subtle dynamics and trends in data sequences over time, particularly having a significant impact on Precision and F1-score. Finally, after removing the Variable Block, Precision was 98.07%, Recall dropped to 92.29%, and F1-score was 95.09%. In comparison, the complete model achieved a Precision of 98.19%, Recall of 96.76%, and F1-score of 97.47%. The significant drop in Recall led to an overall reduction in F1-score, highlighting the key role of the variable attention mechanism in analyzing complex relationships and potential interactions among different variables, which are often crucial for detecting anomalous activities or security threats. Overall, the model achieved its best performance when all components worked together. The Time Block is the most critical for ensuring high Precision and balanced performance, while the Variable Block and UMAP also play important roles in maintaining Recall and enhancing model performance. These results validate the significant contributions of each proposed component to the overall model performance.

Table 5. Performance analysis of ablation variants in Case 1.

Models	Precision	Recall	F1-Score
-WO-UMAP	97.82	96.76	97.29
-WO-Time-Block	91.88	94.73	93.29
-WO- Variable-Block	98.07	92.29	95.09
STformer	98.19	96.76	97.47

4.5. Robustness to Noise

In this section, we evaluated the performance of the proposed distributed photovoltaic communication anomaly detection algorithm under different signal-to-noise ratio (SNR) conditions. Since communication links in actual power systems are often subject to noise interference, assessing the algorithm's performance across various SNR conditions is crucial for validating its stability and effectiveness. To simulate the different noise levels that may be encountered in real-world environments, we added zero-mean white noise to the training and testing datasets and compared the performance metrics across an SNR range of 30 to 100 dB. Subsequently, we compared the performance of our proposed STformer algorithm with several advanced baseline models, including LSSL, THOC, InterFusion, and

Omni anomaly. This comparative analysis helps to comprehensively evaluate the ability of STformer to detect communication anomalies in various noise environments.

As shown in Table 6, the experimental results demonstrate that STformer outperforms the baseline models across different noise levels. Specifically, the Recall rate slightly decreases as the signal-to-noise ratio (SNR) drops. This decrease occurs because higher noise levels impact the detection performance of the proposed algorithm, requiring an increase in the threshold to accommodate the noise. As a result, the detection algorithm struggles to identify attacks with magnitudes lower than the noise level present in the data samples.

Table 6. Performance metrics comparison at different noise levels in Case 1.

SNR (dB)	Models	Precision	Recall	F1-Score
30	OmniAnomaly	95.96	89.89	92.83
	InterFusion	94.88	90.37	92.57
	THOC	90.32	92.51	91.41
	LSSL	88.14	90.99	89.54
	Ours	98.22	92.21	95.21
60	OmniAnomaly	96.64	91.37	93.93
	InterFusion	95.81	91.96	93.85
	THOC	91.88	94.19	93.02
	LSSL	88.98	92.81	90.81
	Ours	98.37	95.97	97.15
90	OmniAnomaly	97.49	92.07	94.70
	InterFusion	96.81	92.33	94.52
	THOC	92.19	95.01	93.58
	LSSL	89.51	95.83	92.56
	Ours	97.82	96.76	97.29

5. Discussion

This study proposes a Transformer-based model, STformer, for detecting communication anomalies in distributed photovoltaic (PV) systems. Compared to traditional methods, STformer demonstrates significant advantages in capturing temporal dependencies and interactions between variables, particularly excelling in complex multivariate time-series scenarios. However, despite its outstanding performance in simulation experiments, several issues warrant further discussion. The following sections provide a detailed discussion of model performance, limitations, and comparisons with existing methods, aiming to offer insights and references for future research.

First, from the perspective of model performance, STformer exhibits strong anomaly detection capabilities. In various experimental scenarios, STformer achieved leading levels in accuracy, Recall, and F1-score, particularly performing well in high-dimensional data and long-horizon forecasting tasks. Unlike traditional LSTM and RNN models, STformer effectively avoids sequential dependency issues by leveraging a multi-head self-attention mechanism, efficiently capturing global information. Furthermore, STformer introduces a variable attention mechanism that identifies and utilizes the complex dependencies among sensor variables while modeling temporal data, significantly enhancing detection accuracy. Experimental results indicate that STformer maintains high detection performance against various types of network attacks (such as DoS and FDIA), demonstrating its strong adaptability in handling diverse anomalies in PV systems.

However, despite STformer's satisfactory performance, there are some limitations worthy of further exploration. First, the data used in this study primarily came from a

simulated environment. Although these data provided a solid validation basis for model development, their complexity and diversity are limited compared to actual operating conditions in PV systems. Data from real PV systems are often influenced by uncertain factors such as environmental changes, equipment aging, and sensor failures, which may significantly impact the model's practical performance. Second, the computational complexity of STformer may pose a challenge for large-scale applications. Although STformer's architecture has distinct advantages in capturing complex temporal relationships, its multi-head self-attention mechanism and high-dimensional data processing requirements increase computational costs, especially in large-scale deployments of distributed PV systems, where real-time performance may be difficult to ensure. Therefore, future research needs to focus on optimizing resource utilization while maintaining model performance and enhancing real-time processing capabilities.

In recent years, various methods for detecting network attacks in distributed PV systems have emerged, each demonstrating their advantages and limitations in different scenarios. To comprehensively assess the superiority of STformer, it is essential to conduct a detailed comparative analysis with current mainstream methods. OCSVM (One-Class Support Vector Machine), a commonly used unsupervised learning method suitable for scenarios with only normal samples, performs well on simple datasets but shows limited performance in complex and diverse anomaly detection contexts like distributed PV systems. In experiments, OCSVM performed poorly with high-dimensional data, achieving only 87.61% accuracy and 88.29% Recall in Case 1, 88.09% accuracy, and 88.17% Recall in Case 2. In contrast, STformer effectively captured temporal dependencies through its multi-head self-attention mechanism, significantly improving detection accuracy and Recall in both cases to 98.19% and 99.07%, with Recall rates increasing to 96.76% and 98.68%. This indicates that STformer significantly outperforms OCSVM in handling complex time series. Deep-SVDD (Deep One-Class Classification), which expands SVDD by incorporating deep neural networks, aims to enhance its ability to handle high-dimensional data. Although Deep-SVDD performs well in certain scenarios, it struggles with long-range dependencies in time-series data. In our experiments, Deep-SVDD achieved 88.45% accuracy and 90.97% Recall in Case 1, and its performance was similarly limited in Case 2 with 88.09% accuracy and 88.17% Recall. In contrast, STformer's multi-head self-attention mechanism captures both long-term and short-term dependencies in time-series data more efficiently, with accuracy and Recall approximately 10% higher than those of Deep-SVDD, especially excelling in complex distributed PV systems. VAR (Vector Autoregression), a traditional time-series forecasting model, is widely used for modeling linear dependency data. However, due to the highly nonlinear and dynamic characteristics of data in distributed PV systems, VAR's performance in these contexts is limited. Experimental results indicate that VAR achieved only 84.52% accuracy and 82.88% Recall in Case 1, with a similar performance in Case 2. STformer, leveraging its multi-head self-attention mechanism, effectively responds to the nonlinear dynamic changes in multivariate time-series data, achieving accuracy and Recall approximately 15% higher than those of VAR, demonstrating STformer's significant advantages in handling nonlinear data. Traditional anomaly detection methods, such as OC-SVM and SVDD, mainly rely on local data features and distance metrics. These methods perform well on low-dimensional data and small datasets but often struggle with high-dimensional, complex time-series data. This is because traditional methods find it challenging to capture the dynamic changes and complex dependencies among multivariate data in time series. In contrast, STformer introduces a self-attention mechanism that can simultaneously handle the complex relationships between time dimensions and variable dimensions, significantly enhancing detection capabilities on large-scale, high-dimensional data.

LSTM (Long Short-Term Memory) and its variant LSTM-VAE (LSTM with Variational Autoencoder) are classical models for handling sequence data, capable of capturing long- and short-term dependencies through memory units. However, LSTM and its variants often face issues of high complexity and a large number of parameters, making them prone to overfitting, particularly when data are limited. Experiments show that LSTM-VAE

achieved 92.83% accuracy and 91.15% Recall in Case 1, and, although it performed well with time-series data, it still fell short of STformer. STformer not only captures temporal dependencies but also effectively models interactions between multiple variables through its variable block, enhancing anomaly detection performance. The F1-score improved by approximately 5% to 7% compared to LSTM-VAE in both cases. Additionally, BeatGAN, a GAN-based model for anomaly detection, generates synthetic data for detection purposes. While it performs well in specific scenarios, the GAN training process can be unstable, often leading to mode collapse or gradient vanishing issues. In our experiments, BeatGAN achieved an F1-score of 92.32%, whereas STformer's F1-score reached 97.47%, exceeding BeatGAN by 5%. Furthermore, BeatGAN struggles to generate precise synthetic data for long time series, while STformer models both temporal dependencies and multivariate interactions more effectively through its self-attention mechanism, ensuring accuracy and stability in detection results. Deep learning methods have made significant progress in anomaly detection, particularly with models like LSTM, LSTM-VAE, and GAN, which perform well with time-series data. These models effectively identify anomalous behaviors by learning dependencies within time series. However, their shortcomings lie in neglecting the interrelations between variables. STformer addresses this issue by incorporating a variable attention mechanism into its architecture, allowing it to model both temporal dependencies and variable interactions simultaneously, thereby outperforming traditional models in multivariate anomaly detection tasks.

OmniAnomaly and InterFusion are recent deep learning-based anomaly detection models that combine autoencoders and graph convolutional networks (GCNs) to enhance detection capabilities. OmniAnomaly achieved F1-scores of 95.57% in Case 1 and 97.32% in Case 2, while InterFusion scored 96.00% in Case 1 and 97.99% in Case 2. Although the performances of these two methods are close to that of STformer, they exhibit significant disadvantages in computational complexity, particularly in handling large datasets, where STformer's efficient architecture maintains high detection accuracy while significantly reducing computational complexity, showcasing its strong practical application advantages. Transformer-based models have gradually become mainstream in time-series analysis, with models like OmniAnomaly and InterFusion excelling in detecting anomalies in multidimensional time series. OmniAnomaly employs Stochastic Recursive Neural Networks (SRNNs) and generative models to effectively detect anomalies in time series. However, it overly relies on temporal dimensions and overlooks potential dependencies between different variables. In contrast, STformer not only utilizes time blocks to capture long- and short-term temporal dependencies but also models interactions among different variables through variable blocks, addressing the shortcomings of existing Transformer models. Additionally, STformer reduces model complexity through UMAP dimensionality reduction techniques, improving computational efficiency while maintaining high detection accuracy.

6. Conclusions and Future Work

In response to the increasing vulnerability of distributed photovoltaic (PV) microgrid interconnected systems during the informatization process, we propose an advanced network attack detection method, STformer, based on the Transformer model. First, we employed the innovative dimensionality reduction technique UMAP to compress the complex raw data, preserving essential features while minimizing losses, thus laying the foundation for real-time and accurate anomaly detection. Second, we integrated temporal and variable attention mechanisms to deeply explore sequence dynamics and the complexity between variables, uncovering potential anomalies or threats. The synergistic use of these two mechanisms constructed a robust and comprehensive analytical framework that effectively analyzes and highlights anomalies in distributed PV communication monitoring, demonstrating strong detection capabilities, particularly in addressing DoS and FDIA attacks.

The results of this study are of great significance to the cybersecurity of PV microgrids. As distributed PV technology becomes more widely applied, the system's digitization

and interconnectedness heighten its vulnerability. The method proposed in this paper not only effectively detects network attacks but also provides an extensible solution for future smart grid systems, contributing to improved robustness in energy management systems. Moreover, this research reveals the potential of deep learning models in detecting complex network anomalies through spatiotemporal feature collaborative modeling, providing a technical foundation for the automated security defense of future grid systems.

Future research can proceed in several directions. First, the model's adaptability should be further validated in complex scenarios, particularly in the robustness of multi-energy integrated systems, and the model's capability to handle uncertainties should be optimized. Second, while the model performs well in detection accuracy, improving real-time performance remains a key focus for future efforts. Optimizing computational efficiency and reducing detection latency will help ensure the method's rapid response in practical applications. Future studies can also explore integrating information from different data sources, such as image data and sensor data, to enhance the model's detection capabilities in multimodal data environments. Additionally, exploring proactive defense and automatic recovery mechanisms is a promising direction. Through deep learning-based strategies, these mechanisms can strengthen the system's resilience following an attack and enhance the security of distributed energy systems. Finally, although this study focuses on anomaly detection in PV microgrid communications, the principles and technical framework of the proposed method have broad applicability. Future research could explore its extension to other industrial fields, such as smart manufacturing and smart cities. Through continued research and improvement in these areas, the proposed method has the potential to provide a more comprehensive solution for the cybersecurity of distributed energy systems, advancing the intelligent development of smart grids and other complex systems.

Author Contributions: Conceptualization, L.D. and Z.L.; methodology, L.D.; software, L.D.; validation, L.D., J.C. and H.C.; formal analysis, L.D.; investigation, H.C.; resources, Z.L.; data curation, J.C.; writing—original draft preparation, L.D.; writing—review and editing, L.D.; visualization, Z.L.; supervision, Z.L.; project administration, J.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Acknowledgments: We would like to thank State Grid Henan Electric Power Company and State Grid Henan Electric Power Research Institute for their support of this research. Special thanks to State Grid Henan Electric Power Company for providing valuable data and technical support, and to State Grid Henan Electric Power Research Institute for their valuable advice and resources throughout the study.

Conflicts of Interest: Author Li Di was employed by the company State Grid Henan Electric Power Company. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Khan, K.R.; Rahman, A.; Nadeem, A.; Siddiqui, M.S.; Khan, R.A. Remote monitoring and control of microgrid using smart sensor network and internet of thing. In Proceedings of the 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 4–6 April 2018; pp. 1–4.
2. Liu, X.; Shahidehpour, M.; Cao, Y.; Wu, L.; Wei, W.; Liu, X. Microgrid risk analysis considering the impact of cyber attacks on solar PV and ESS control systems. *IEEE Trans. Smart Grid* **2016**, *8*, 1330–1339. [CrossRef]
3. Ye, J.; Giani, A.; Elasser, A.; Mazumder, S.K.; Farnell, C.; Mantooth, H.A.; Kim, T.; Liu, J.; Chen, B.; Seo, G.S.; et al. A review of cyber–physical security for photovoltaic systems. *IEEE J. Emerg. Sel. Top. Power Electron.* **2021**, *10*, 4879–4901. [CrossRef]

4. Madichetty, S.; Mishra, S. Cyber attack detection and correction mechanisms in a distributed DC microgrid. *IEEE Trans. Power Electron.* **2021**, *37*, 1476–1485.
5. Duo, W.; Zhou, M.; Abusorrah, A. A survey of cyber attacks on cyber physical systems: Recent advances and challenges. *IEEE/CAA J. Autom. Sin.* **2022**, *9*, 784–800. [CrossRef]
6. Zhang, J.; Ye, J. Cyber-attack detection for active neutral point clamped (anpc) photovoltaic (pv) converter using kalman filter. In Proceedings of the 2022 IEEE Applied Power Electronics Conference and Exposition (APEC), Houston, TX, USA, 20–24 March 2022; pp. 1939–1944.
7. Zhang, J.; Guo, L.; Ye, J. Cyber-attack detection for photovoltaic farms based on power-electronics-enabled harmonic state space modeling. *IEEE Trans. Smart Grid* **2021**, *13*, 3929–3942. [CrossRef]
8. Qiu, W.; Sun, K.; Li, K.J.; Li, Y.; Duan, J.; Zhu, K. Cyber-attack detection: Modeling and roof-PV generation system protection. In Proceedings of the 2022 IEEE/IAS 58th Industrial and Commercial Power Systems Technical Conference (I & CPS), Las Vegas, NV, USA, 2–5 May 2022; pp. 1–6.
9. Ramos-Ruiz, J.; Kim, J.; Ko, W.H.; Huang, T.; Enjeti, P.; Kumar, P.; Xie, L. An active detection scheme for cyber attacks on grid-tied PV systems. In Proceedings of the 2020 IEEE CyberPELS (CyberPELS), Miami, FL, USA, 13 October 2020; pp. 1–6.
10. Breunig, M.M.; Kriegel, H.P.; Ng, R.T.; Sander, J. LOF: Identifying density-based local outliers. In Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data, Dallas, TX, USA, 16–18 May 2000; pp. 93–104.
11. Schölkopf, B.; Platt, J.C.; Shawe-Taylor, J.; Smola, A.J.; Williamson, R.C. Estimating the support of a high-dimensional distribution. *Neural Comput.* **2001**, *13*, 1443–1471. [CrossRef] [PubMed]
12. Choi, J.; Roshanzadeh, B.; Martínez-Ramón, M.; Bidram, A. An unsupervised cyberattack detection scheme for AC microgrids using Gaussian process regression and one-class support vector machine anomaly detection. *IET Renew. Power Gener.* **2023**, *17*, 2113–2123. [CrossRef]
13. Tax, D.M.; Duin, R.P. Support vector data description. *Mach. Learn.* **2004**, *54*, 45–66. [CrossRef]
14. Gholami, A.; Tiwari, A.; Qin, C.; Pannala, S.; Srivastava, A.K.; Sharma, R.; Pandey, S.; Rahmatian, F. Detection and Classification of Anomalies in Power Distribution System Using Outlier Filtered Weighted Least Square. *IEEE Trans. Ind. Inform.* **2024**, *20*, 7513–7523. [CrossRef]
15. Ali, M.G.; Gaafar, M.A.; Orabi, M. Photovoltaic Systems Status Monitoring Utilizing Machine Learning Technique. In Proceedings of the 2023 IEEE Conference on Power Electronics and Renewable Energy (CPERE), Luxor, Egypt, 19–21 February 2023; pp. 1–5.
16. Su, Y.; Zhao, Y.; Niu, C.; Liu, R.; Sun, W.; Pei, D. Robust anomaly detection for multivariate time series through stochastic recurrent neural network. In Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, Anchorage, AK, USA, 4–8 August 2019; pp. 2828–2837.
17. Shen, L.; Li, Z.; Kwok, J. Timeseries anomaly detection using temporal hierarchical one-class network. *Adv. Neural Inf. Process. Syst.* **2020**, *33*, 13016–13026.
18. Li, D.; Chen, D.; Jin, B.; Shi, L.; Goh, J.; Ng, S.K. MAD-GAN: Multivariate anomaly detection for time series data with generative adversarial networks. In Proceedings of the International Conference on Artificial Neural Networks, Munich, Germany, 17–19 September 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 703–716.
19. Guo, L.; Zhang, J.; Ye, J.; Coshatt, S.J.; Song, W. Data-driven cyber-attack detection for pv farms via time-frequency domain features. *IEEE Trans. Smart Grid* **2021**, *13*, 1582–1597. [CrossRef]
20. Mao, J.; Zhang, M.; Xu, Q. CNN and LSTM based data-driven cyberattack detection for grid-connected PV inverter. In Proceedings of the 2022 IEEE 17th International Conference on Control & Automation (ICCA), Naples, Italy, 27–30 June 2022; pp. 704–709.
21. Li, Q.; Zhang, J.; Ye, J.; Song, W. Data-driven cyber-attack detection for photovoltaic systems: A transfer learning approach. In Proceedings of the 2022 IEEE Applied Power Electronics Conference and Exposition (APEC), Houston, TX, USA, 20–25 March 2022; pp. 1926–1930.
22. Peng, S.; Liu, M.; Chai, L.; Deng, R. DST-GNN: A Dynamic Spatiotemporal Graph Neural Network for Cyberattack Detection in Grid-Tied Photovoltaic Systems. *IEEE Trans. Smart Grid* **2024** . [CrossRef]
23. Zhe, W.; Wei, C.; Chunlin, L. DoS attack detection model of smart grid based on machine learning method. In Proceedings of the 2020 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS), Shenyang, China, 28–30 July 2020; pp. 735–738.
24. Seghiour, A.; Abbas, H.A.; Chouder, A.; Rabhi, A. Deep learning method based on autoencoder neural network applied to faults detection and diagnosis of photovoltaic system. *Simul. Model. Pract. Theory* **2023**, *123*, 102704. [CrossRef]
25. Musleh, A.S.; Chen, G.; Dong, Z.Y.; Wang, C.; Chen, S. Attack detection in automatic generation control systems using LSTM-based stacked autoencoders. *IEEE Trans. Ind. Inform.* **2022**, *19*, 153–165. [CrossRef]
26. Liu, Q.; Guo, S.; Qiu, S.; Fei, J.; Zhang, B.; Yu, X.; Pan, K. Cyber-Attack Detection Approach In Photovoltaic Microgrids Using LSTM-based Autoencoders. In Proceedings of the 2023 4th International Conference on Power Engineering (ICPE), Macau, China, 11–13 December 2023; pp. 183–188.
27. McInnes, L.; Healy, J.; Melville, J. Umap: Uniform manifold approximation and projection for dimension reduction. *arXiv* **2018**, arXiv:1802.03426.
28. Dong, W.; Moses, C.; Li, K. Efficient k-nearest neighbor graph construction for generic similarity measures. In Proceedings of the 20th International Conference on World Wide Web, Hyderabad, India, 28 March–1 April 2011; pp. 577–586.

29. Vaswani, A. Attention is all you need. In Proceedings of the Advances in Neural Information Processing Systems 30 (NIPS 2017), Long Beach, CA, USA, 4–9 December 2017.
30. Zhang, G.; Li, J.; Bamisile, O.; Xing, Y.; Cao, D.; Huang, Q. Identification and classification for multiple cyber attacks in power grids based on the deep capsule CNN. *Eng. Appl. Artif. Intell.* **2023**, *126*, 106771. [CrossRef]
31. Moeini, A.; Kamwa, I.; Brunelle, P.; Sybille, G. Open data IEEE test systems implemented in SimPowerSystems for education and research in power grid dynamics and control. In Proceedings of the 2015 50th International Universities Power Engineering Conference (UPEC), Stoke-on-Trent, UK, 1–4 September 2015; pp. 1–6.
32. Qiao, Y.; Wu, K.; Jin, P. Efficient anomaly detection for high-dimensional sensing data with one-class support vector machine. *IEEE Trans. Knowl. Data Eng.* **2021**, *35*, 404–417. [CrossRef]
33. Ruff, L.; Vandermeulen, R.; Goernitz, N.; Deecke, L.; Siddiqui, S.A.; Binder, A.; Müller, E.; Kloft, M. Deep one-class classification. In Proceedings of the International Conference on Machine Learning, PMLR, Stockholm, Sweden, 10–15 July 2018; pp. 4393–4402.
34. Abbracciavento, F.; Formentin, S.; Balocco, J.; Rota, A.; Manzoni, V.; Savaresi, S.M. Anomaly detection via distributed sensing: A VAR modeling approach. *IFAC-PapersOnLine* **2021**, *54*, 85–90. [CrossRef]
35. Hundman, K.; Constantinou, V.; Laporte, C.; Colwell, I.; Soderstrom, T. Detecting spacecraft anomalies using lstms and nonparametric dynamic thresholding. In Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, London, UK, 19–23 August 2018; pp. 387–395.
36. Park, D.; Hoshi, Y.; Kemp, C.C. A multimodal anomaly detector for robot-assisted feeding using an lstm-based variational autoencoder. *IEEE Robot. Autom. Lett.* **2018**, *3*, 1544–1551. [CrossRef]
37. Zhou, B.; Liu, S.; Hooi, B.; Cheng, X.; Ye, J. Beatgan: Anomalous rhythm detection using adversarially generated time series. In Proceedings of the IJCAI, Macao, China, 10–16 August 2019; Volumr 2019, pp. 4433–4439.
38. Gu, A.; Goel, K.; Ré, C. Efficiently modeling long sequences with structured state spaces. *arXiv* **2021**, arXiv:2111.00396.