Journal of Network Intelligence
Taiwan Ubiquitous Information
 ISSN 2414-8105 (Online)
Volume **9**, Number **2**, May **2024**

Kalman Filter-based Cycle-Consistent Adversarial Learning for Time Series Anomaly Detection

Shu-Tang Liu

Faculty of Humanities and Arts
Macau University of Science and Technology, Macau 999078, China

Academic Affairs Office
Minjiang University, Fuzhou 350108, China
seahippo@126.com

Ji-Jie Fan*

Kyrgyz National University Named after Jusup Balasagyn, Bishkek 720033, Kyrgyzstan
jijiefan@gmail.com

Rui-Dong Wang

School of Computer Science and Technology
Harbin University of Science and Technology, Harbin 150080, China
iswangrd@gmail.com

Han Han

School of Measurement and Control Technology and Communication Engineering
Harbin University of Science and Technology, Harbin 150080, China
ishanhan266@gmail.com

De-Yang Zhang

Henan Provincial Institute of Scientific and Technical Information, Zhengzhou 450003, China
zhdy@qq.com

*Corresponding author: Ji-Jie Fan

Received September 4, 2023, revised December 21, 2023, accepted March 8, 2024.

Abstract. *Anomaly detection in time series is challenging for machine learning due to the uncertainty and complex pattern in time series. In this paper, we propose a Kalman filter-based cycle-consistent adversarial learning framework (KFCGAN) for time series anomaly detection, assuming that the abnormal pattern prevents the model from reconstructing the original and filtered signals. Specifically, KFCGAN comprises a Kalman filter module and a cycle-consistent adversarial learning module that utilizes an autoencoder as its generator. Firstly, the Kalman filter module generates the filtered signals from the original signals as the target domain. Then, the forward direction of the cycle-consistent adversarial learning module learns the transformation of the original time series domain to the filtered time series domain. At the same time, the backward direction optimizes it by transforming the target domain to the original domain. Finally, anomaly detection can be modeled as the signal reconstruction problem between the original and target domains. The experimental results on five real-world datasets show that the proposed method outperforms the start-of-the-art, demonstrating that KFCGAN can effectively capture abnormal time series patterns.*
Keywords: time series, unsupervised anomaly detection, adversarial learning, kalman filter.

1. **Introduction.** Time series data is a type of data that changes over time and is widely present in the real world [1, 2, 3]. Time series analysis is crucial in various fields, including industrial production [4, 5, 6, 7, 8], medicine [9, 10, 11, 12, 13], human activity recognition [14] and financial time series analysis [15, 16]. Specifically, time series anomaly detection is an important problem worthy of study [17, 18, 19]. For example, in the medical field, the status of patients can be judged by analyzing whether an electrocardiogram is abnormal. In the financial field, malicious manipulation of stock prices can be detected by analyzing abnormal fluctuations in stock prices.

Time series anomaly detection aims to identify signals that exhibit significant deviations from other signals [20, 21]. In recent years, there are a lot of methods based on deep learning have been proposed concerning the time series anomaly detection task [22, 23, 24]. The clustering-based methods [25, 26] learn a compact boundary of normal data to distinguish between normal and abnormal signals. Due to the time series data being a kind of complex data that has a strong temporal relationship, the traditional methods such as OC-SVM [26] and Deep-SVDD [27] achieve good performance in the traditional anomaly detection cannot use to detect the anomaly time series directly. Additionally, residual-error-based methods [23, 28] learn a lower-dimensional feature embedding and utilize it to predict future time series or reconstruct the original time series. By computing the error between the predicted/reconstructed time series and the actual time series, these methods are able to detect abnormal time series. Methods based on distribution learning, such as BeatGAN [23] and MADGAN [29], leverage the capabilities of LSTM to capture the temporal information inherent in time series data. These methods employ Generative Adversarial Networks (GAN) [30, 31] to learn the distribution of normal time series data. Subsequently, any signals that deviate from the learned distributions are identified as abnormal.

However, current time series anomaly detection methods primarily concentrate on learning signal representations in low-dimensional feature spaces, neglecting the direct extraction of differentiation information between normal and abnormal time series. Figure 1 shows the main ideas of KFCGAN. Different from other methods, this paper proposed a Kalman filter-based cycle-Consistent adversarial learning framework, which learns the difference between normal signals and abnormal signals for anomaly detection. Specifically, KFCGAN first utilizes the Kalman Filter to convert the original time series into denoised representations. And then, cycle-consistent adversarial learning which has two directions in the loop is designed to learn the transformation between the original signals domain and the domain of the filtered signal. The forward direction of the loop aims to convert the original time series into filtered time series, while the backward direction refines the forward transformation by mapping the time series from the filtered signal domain back to the original signal domain. Subsequently, the discrepancy between the signal in the original signal domain and the filtered signal domain is employed as the anomaly score for detecting time series anomalies. The main contributions are summarized as follows:

- We propose a framework of transformation-based time series anomaly detection named KFCGAN, which aims to learn the transformation between the original signal domain and the filtered signal domain and detect the anomaly by measuring the reconstruction error between the original domain and the target domain.
- We propose a Kalman filter-based method with cycle-Consistent adversarial learning to learn the transformation between the original signal domain and the filtered signal domain. Specifically, it has two directions in the loop to learn the transformations between the original signal domain and the filtered signal domain and optimize

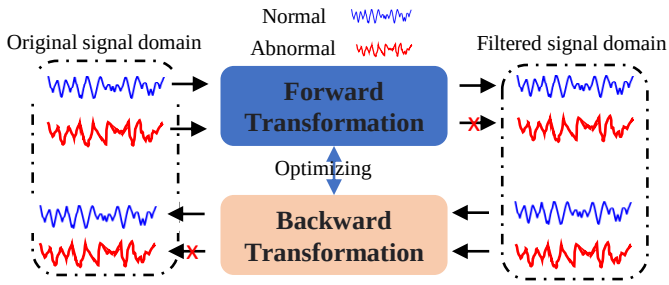

FIGURE 1. The key idea of KFCGAN.

each other in the training process, and define the transformation difference between domains as the anomaly score for time series anomaly detection.

- We conduct extensive experiments and experimental results show that the proposed KFCGAN outperforms the state-of-art baselines, which proves the effectiveness of the proposed method.

2. Related Works.

2.1. **Generative adversarial networks.** Generative Adversarial Networks (GAN) [32] is a kind of generation model which widely used in many fields. It utilizes game theory ideas to optimize the quality of data generated by the generator. GAN consists of a generator designed to obtain the distribution of training data, and a discriminator to estimate the probability of a sample from the original data or generator. In recent years, numerous GAN-based methods have been proposed [33, 34] to generate high-quality data. Bidirectional Generative Adversarial Network(BiGAN) [35] is an unsupervised method that designs an encoder to extract the data feature which can be used for downstream tasks. Coupled generative adversarial network(CoGAN) [36] utilize the ideas of hierarchical feature representation to learn the joint distribution of data, and achieve good performance. Cycle-Consistent Adversarial Networks (CycleGAN) [37] is designed for domain adaptation. It has two generators, one is responsible for transforming data from the source domain to the target domain, while the other generator performs the reverse transformation, converting data from the target domain back to the source domain. Besides, some GAN-based methods have been proposed for anomaly detection tasks, such as AnoGAN [38] and Ganomaly [39] which utilize the strong generative ability of GAN to generate similar data with original data, and anomalies are detected by computing the similarity between the generated data and the original data.

2.2. **Time series anomaly detection.** Recently, lots of time series anomaly detection methods have been proposed in many domains such as intelligent diagnosis of mechanical faults [40, 41, 42], human activity recognition [14] and financial time series analysis [15, 16], which can be divided into two categories: the clustering-based methods, and residual-error-based methods.

The main idea of the clustering-based methods [43, 44, 45] is to learn compact boundaries of normal data to separate the normal data and abnormal data in the latent space. Such as one-class methods (OC-SVM [26], Deep-SVDD [46]), they first use the neural networks to map the original signals to latent space and optimize the model by the one-class objective function. But those methods cannot be directly used in temporal data. The residual-error-based methods [47] aims to predict the next time's value or reconstruct the original time series, and compute the error between the generated data and

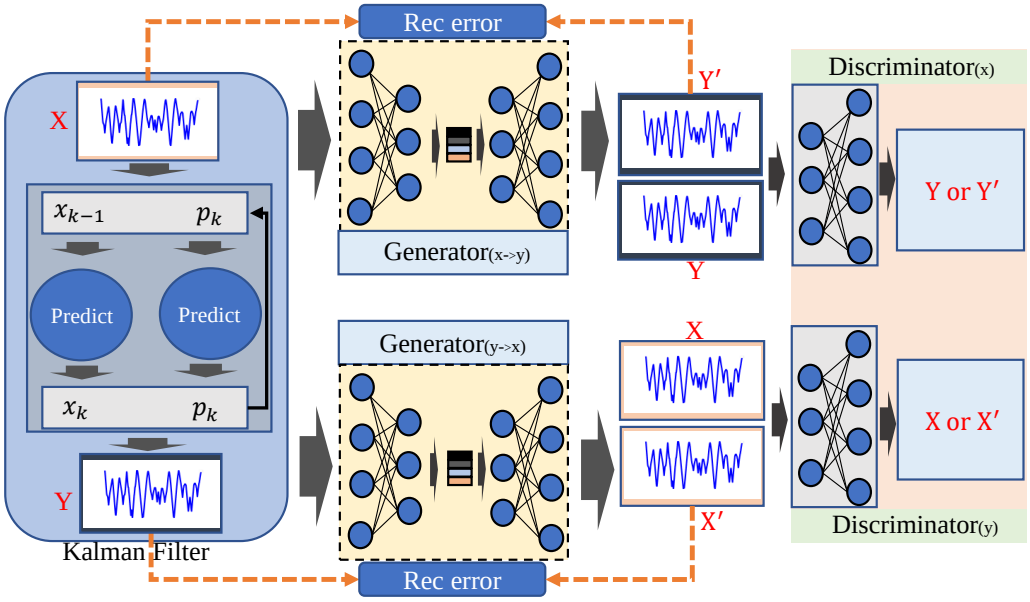

FIGURE 2. The proposed framework of KFCGAN.

the ground truth as anomaly score to detect anomaly. Long short-term Memory(LSTM)-based methods [48, 49] utilize the LSTM to capture the temporal relationship of time series, and predict the next time sequence for anomaly detection. Besides, some methods based on auto-encoder [50, 51] assume that the anomaly data cannot reconstruct from the low-dimensional space, they first map the data into low-dimensional space and then reconstruct them from the latent space. The reconstruction error is then computed as an anomaly score to detect abnormal data. Another residual-error based methods utilize the advantage of generative adversarial networks to generate the data from the learned distribution and detect the anomaly by computing the error between original data and generated data [52, 53]. AnoGAN [54] and Ganomaly [39] are the GAN-based methods for anomaly detection, which learn the latent representation of test data and use the generator to obtain the generated data from latent representation, then, detect the anomaly by computing the residual-error between original data and generated data. ALAD [55] is a bidirectional GAN-based method that avoids the expensive computation process by using the learned low dimensional feature to train Generative Adversarial Networks. However, these methods suffer from gradient disappearance and gradient explosion problems. Beat-GAN [23] utilizes the adversarial regularity in the discriminator to constrain the feature learned by the encoder to avoid those problems. Besides, some multi-modal based methods such as MMGAN [56] learn the distribution from both the time domain and frequency domain perspectives and detect the anomaly by measuring the reconstruction error from both two domains. Although the above methods perform well for time series anomaly detection, those methods just consider the data representation in the low-dimensional feature space, which makes they can not achieve better performance. Different from those methods, KFCGAN directly captures discriminative information between normal and abnormal time series. It learns the transformation between the original time series domain and the filtered time series domain, and anomalies cannot be correctly transformed between the two domains, thus enabling anomaly detection.

3. **Overview of proposed method.** The proposed framework KFCGAN is shown in Figure 2. KFCGAN consists of a Kalman filter to generate the target domain of time series

and a cycle-consistent adversarial learning module which have two identically constructed generators and discriminators to detect the anomaly signals. Firstly, we take the Kalman filter to generate the filtered signals as the target domain. Then, the cycle-consistent adversarial learning utilizes the original signals space as the source domain and filtered signals space as the target domain to learn the transformation between original signals and filtered signals. Specifically, the forward direction of cycle-consistent adversarial learning is used to learn the transformation from the source domain to the target domain. Conversely, the backward direction optimized the forward direction by transforming the signals from the target domain back to the source domain. Furthermore, the generators utilize the auto-encoder to map the signals to low dimensional feature space to learn the signals embedding. After the training process, we detect the anomaly by measuring the reconstruction error between the original signal domain and the filtered signal domain.

3.1. **Filtered Signal Domain Generation.** For time series, Kalman Filter can filter the noises and estimate the filtered signals, which has an estimate process and state update process. Specifically, give an original time series $\mathbf{X} = \{\boldsymbol{x_t}|i = 0, 1, ..., K\}$, and input the value of $\mathbf{X}$ on $\boldsymbol{t-1}$ time step, the optimal estimate value of the next time step can be computed as follows:

$$\boldsymbol{x_t} = \boldsymbol{A}\boldsymbol{x_{t-1}} + \boldsymbol{B}\boldsymbol{u_{t-1}} \tag{1}$$

with a measurement model equation:

$$\boldsymbol{P_t} = \boldsymbol{A}\boldsymbol{P_{t-1}}\boldsymbol{A^T} + \boldsymbol{Q} \tag{2}$$

where the $\boldsymbol{x_t}$ and $\boldsymbol{P_t}$ is the estimate value of $\mathbf{X}$ and the variance on $\boldsymbol{k}$ time step, $\boldsymbol{Q}$ is the variance of the noise in the original time series. $\boldsymbol{A}$ is the state transition matrix, $\boldsymbol{B}$ is the input matrix, and $\boldsymbol{u_{t-1}}$ is the input signal

Then, the Kalman filter updates the optimal estimator variance:

$$\boldsymbol{K_t} = \boldsymbol{P_t}\boldsymbol{H^T}(\boldsymbol{H}\boldsymbol{P_t}\boldsymbol{H^T} + \boldsymbol{R}) \tag{3}$$

where the $\boldsymbol{K_t}$ is the Kalman gain of the time state $\boldsymbol{t}$, $\boldsymbol{R}$ is the variance of the observation noise, and $\boldsymbol{H}$ is the observation matrix. Then, the optimal estimated value $\boldsymbol{x_t}$ can be computed as follows:

$$\boldsymbol{x_t} = \hat{\boldsymbol{x}}_{\boldsymbol{t}} + \boldsymbol{K_t}(\boldsymbol{z_t} - \boldsymbol{H}\hat{\boldsymbol{x}}_{\boldsymbol{t}}) \tag{4}$$

where $\hat{\boldsymbol{x}}_{\boldsymbol{t}}$ and $\boldsymbol{z_t}$ is the estimate value and observation value of this moment. And the optimally estimated variance over covariance at time step $\boldsymbol{t}$ can be computed:

$$\hat{\boldsymbol{P}}_{\boldsymbol{t}} = (\boldsymbol{I} - \boldsymbol{K_t}\boldsymbol{H})\boldsymbol{P_t} \tag{5}$$

where $\hat{\boldsymbol{P}}_{\boldsymbol{t}}$ is the estimated variance of this moment.

In this paper, we input the time series $\mathbf{X} = \{\boldsymbol{x_t}|i = 0, 1, ..., K\}$ into the Kalman Filter and obtain the filtered time series as the target domain of cycle-Consistent adversarial learning.

3.2. **Cycle-Consistent adversarial learning.** Figure 2 show the overall architecture of the KFCGAN. In this paper, we name the original domain as $\mathbf{X} = \{x_i|i = 1, 2, ..., N\}$ and the filtered signal domain as $\mathbf{Y}$. In order to learn the transformation between $\mathbf{X}$ and $\mathbf{Y}$, we define two generators, $G_{fw}(\bullet)$ and $G_{bw}(\bullet)$, as well as two discriminators, D_{fw} and D_{bw}. The generators are designed to capture the mapping from X to Y and from Y to X respectively. The discriminators provide feedback to optimize the performance of both generators. We denote the generate original domain signal and filtered domain signal as $\mathbf{X}^{'}$ and $\mathbf{Y}^{'}$. Then, $\mathbf{X}^{'}$ and $\mathbf{Y}^{'}$ would be transformed back to the original domain

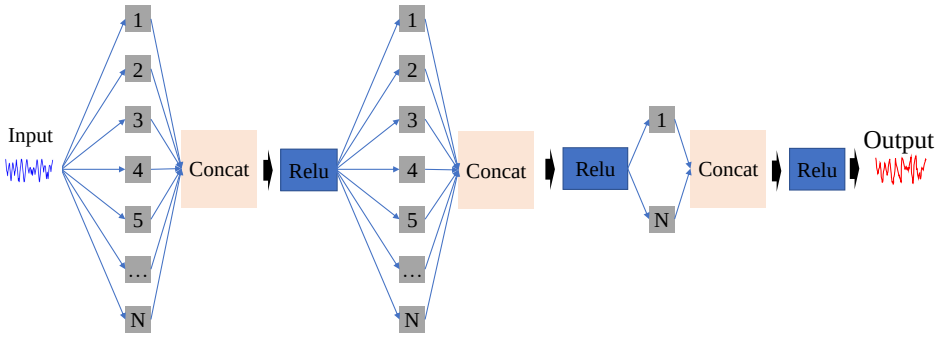

FIGURE 3. The architecture of generator.

and filtered signal domain respectively. Specifically, all the layers in the generator and discriminator utilize omni-scale CNN (OSCNN)[57] to learn the information of time series.

When training the $G_{fw}(\bullet)$, we take the original signal $\mathbf{X}$ as input to learn the transformation from the original signal domain to the filtered signal domain by the generator $G_{fw}(\bullet)$. Then, the $G_{bw}(\bullet)$ transforms the $\mathbf{Y}^{'}$ back to the original domain. The same process for training $G_{bw}(\bullet)$.

$$\mathbf{Y}^{'} = \mathbf{G}_{fw}(\mathbf{X}) \tag{6}$$

$$\mathbf{X}^{'} = \mathbf{G}_{bw}(\mathbf{Y}) \tag{7}$$

When training discriminator D_{fw}, both $\mathbf{Y}$ and $\mathbf{Y}'$ are are provided as inputs. D_{fw} classifies $\mathbf{Y}$ as true and $\mathbf{Y}^{'}$ as false. And the same operation for discriminator D_{bw}.

In the training process, the forward and backward directions of the loop mutually optimize each other, enabling the generators to learn the transformation between the original time series and the filtered time series.

3.3. **Generator.** To make full use of signal information and solve the parameter sensitivity problem caused by modal feature dimension transformation, the generator adopts an adaptive convolution architecture covering all scales (omni-scale CNN, OSCNN)[57]. During the learning process, this architecture dynamically selects the optimal convolution kernel size to prevent the loss of temporal feature representation and noise due to excessively large or small convolution kernels. As shown in Figure 3, the size of the convolution kernel is 1 to the number of primes, the size of the convolution kernel is 1 to the number of primes, and the size of is positively related to the dimension of each modal feature. In the last layer of convolution, there are only convolution kernels of sizes 1 and 2. With this convolution architecture, the receptive field of convolution can cover the temporal samples of all scales to ensure the efficient learning of temporal features.

3.4. **Objective Function and Anomaly Score.** In cycle-consistent adversarial learning, both the discriminators in the forward direction and the backward direction of the loop are employed to optimize the respective generators in the cycle-consistent adversarial learning framework. The Equation 8 is the objective function of the discriminator in the forward direction and The Equation 9 is the objective function of the discriminator in the backward direction.

$$\begin{aligned}\mathcal{L}_{D_{fw}} = &-\mathbb{E}_{\mathbf{X}\sim p_{\mathbf{x}}}[\log D_{fw}(\mathbf{X})]- \\ &\mathbb{E}_{\mathbf{Y}'\sim p_{\mathbf{y}'}}[\log(1 - D_{fw}(\mathbf{Y}^{'}))]\end{aligned} \tag{8}$$

TABLE 1. Statistics of the used UCR dataset.

Dataset	Dim	Numbers	Class	Type
CBF	128	930	3	Sensor
MSST	1024	2525	5	Image
FST	301	2878	2	Sensor
TPAs	128	5000	4	Simulated
EleD	96	16637	7	Device

$$\begin{aligned}\mathcal{L}_{D_{bw}} = -\mathbb{E}_{\mathbf{Y}\sim p_{\mathbf{y}}}[\log D_{bw}(\mathbf{Y})]- \\ \mathbb{E}_{\mathbf{X}'\sim p_{\mathbf{x}'}}[\log(1-D_{bw}(\mathbf{X}^{'}))]\end{aligned} \tag{9}$$

where $p_{\mathbf{x}}$ and $p_{\mathbf{y}}$ is the distributions of original signals and filtered signals. And the $p_{\mathbf{x}'}$ and $p_{\mathbf{y}'}$ are the prior distributions of original signals and filtered signals learned by both generators $G_{fw}(\bullet)$ and $G_{bw}(\bullet)$.

For the generators of both the forward direction and backward direction of the loop in cycle-Consistent adversarial learning, we use the reconstruction error and pairwise feature matching loss of $\mathbf{G}_{fw}(\bullet)$ and $\mathbf{G}_{bw}(\bullet)$ to minimizing the difference between the original signals and the learned signals from the hidden layer of the discriminators.

$$\mathcal{L}_{G_{fw}} = ||\mathbf{X} - \mathbf{Y}^{'}|| + ||D_{fw}(\mathbf{X}) - D_{fw}(\mathbf{Y}^{'})|| \tag{10}$$

$$\mathcal{L}_{G_{bw}} = ||\mathbf{Y} - \mathbf{X}^{'}|| + ||D_{bw}(\mathbf{Y}) - D_{bw}(\mathbf{X}^{'})|| \tag{11}$$

After the training process, the generators can effectively transform normal signals from the source domain to the target domain. However, abnormal signals cannot be accurately reconstructed from the latent space, rendering them unable to be converted between the source and target domains. The anomaly score is defined as follows:

$$Score = \alpha(||\mathbf{X} - \mathbf{X}^{'}||) + (1-\alpha)(||\mathbf{Y} - \hat{\mathbf{Y}}^{'}||) \tag{12}$$

where α is the trade-off parameter, it can be computed by Equation 13:

$$\alpha = \frac{size(\mathbf{X})}{size(\mathbf{X}) + size(\mathbf{Y})} \tag{13}$$

where the $size(\bullet)$ is the size of signals.

4. **Experiment.** In this section, we described the details of the experimental setup. First, we introduce the datasets and state-of-the-art used in this paper. Then, we compared the results of the anomaly detection task between KFCGAN and other methods. Lastly, we assess the proposed methods through ablation studies and parameter analysis, affirming their effectiveness.

4.1. **Datasets.** In this paper, we use UCR time series dataset [58] to verify the proposed model, which has become the benchmark data in the field of time signal processing. In this paper, we select five different categories of datasets in UCR including CBF, MixedShapesSmallTrain(MSST), FreezerSmallTrain(FST), TwoPattens(TPAs), ElectricDevices(EleD). The statistical information for these five datasets is presented in Table 1.

In the experiment, for each dataset, we select one of the classes of it as a normal class and the others as the abnormal class, and random choice 60% normal data as the training set, and the remaining 40% data were divided into the validation set and test set respectively.

4.2. **Experimental Parameters And Comparison Methods.** The hardware parameters of the experimental platform in this paper are as follows: Intel(R)-Xeon(R)-Gold-5220R, 2.20GHz and 256G memory for CPU, NVIDIA 3090, and 24G video memory for GPU. The experimental environment is Pytorch[1]. All methods are performed under 10 different random seeds. For the training process, the Adam algorithm is used to optimize KFCGAN, and the learning rate is set as 0.001. KFCGAN run 1000 epoch for training and the batch size is set as 64. For all experiments, the baseline methods use the implementation of the original public code and select the optimal parameters by grid search.

The details of the comparison methods of this paper are as follows:

- **AnoGAN** [54]: is the pioneering work that utilizes Generative Adversarial Networks for anomaly detection. During the training process, it learns the underlying distribution of normal data in the latent space. When testing, it defines a loss function for test data to perform the multiple back propagations and generate the latent representation of test data. Then, the latent representation is used to generate the test data, and the residual error between the generated data and the original data is computed to detect anomalies.
- **ALAD** [55]: is an anomaly detection model based on bidirectional Generative Adversarial Networks. It uses an encoding network to map the input data to a latent space and leverages the encoded data for training Generative Adversarial Networks which avoids the expensive computation process. For anomaly detection, it evaluates the difference between generated data and original data to detect abnormal data.
- **Ganomaly** [39]: is an anomaly detection method specifically designed for image data using generative adversarial networks. The generator in Ganomaly employs an encoder-decoder-encoder framework to generate latent representations for both the original and reconstructed data. The generator is optimized by assessing the errors between the latent representations of the original and reconstructed data, as well as the reconstruction error itself. Finally, detect the anomaly by using the error of the original data and reconstruction data.
- **BeatGAN** [23]: is a generative adversarial model applied to time series. Different from other methods, it utilizes the adversarial regularity in the discriminator to constrain the feature learned by the encoder, which solves the gradient disappearance and explosion problems to some extent.
- **MMGAN** [56]: is a multi-modal generative adversarial network model that simultaneously learns the distributions of normal data in both the time domain and frequency domain. It utilizes the reconstruction error as an anomaly score and detects the anomaly data by measuring the anomaly score of the time series from both the time domain and frequency domain perspectives.

4.3. **Experimental Results.**

4.3.1. *Anomaly Detection Analysis.* Table 2 show the results of KFCGAN and stat-of-the-arts. We can find that KFCGAN outperforms other methods. This is because KFCGAN learns an effective signal conversion pattern where normal signals can be efficiently

[1] `https://pytorch.org/`

TABLE 2. Anomaly Detection Performance of All methods. The results in the upper table are AUC and the results in the lower table are AP. Specifically, all values are percentages (%) over 5 seeds. The best results are marked in **bold**.

Dataset	CBF	MSST	FST	TPAs	EleD
AnoGAN	62.49%	72.21%	68.80%	59.80%	65.91%
ALAD	76.10%	78.91%	76.41%	65.87%	75.10%
Ganomaly	79.17%	76.73%	75.34%	65.18%	84.89%
BeatGAN	81.65%	88.85%	85.70%	62.53%	71.64%
MMGAN	91.86%	91.83%	89.50%	72.61%	89.34%
KFCGAN	**99.58%**	**95.21%**	**99.16%**	**96.12%**	**95.70%**
AnoGAN	59.64%	81.89%	73.05%	59.99%	65.91%
ALAD	71.77%	76.16%	77.70%	58.20%	77.16%
Ganomaly	69.91%	62.16%	75.34%	54.54%	82.29%
BeatGAN	73.51%	72.48%	85.70%	47.83%	57.99%
MMGAN	89.38%	81.70%	89.50%	61.50%	88.23%
KFCGAN	**99.79%**	**86.90%**	**98.95%**	**99.27%**	**92.51%**

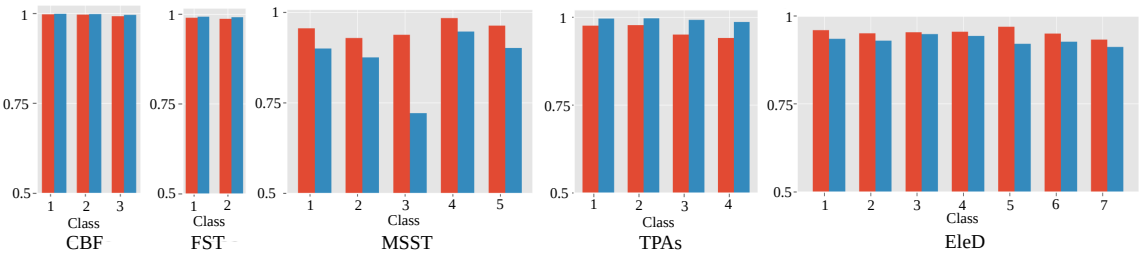

FIGURE 4. The results of anomaly detection by using each class as normal class, the red is AUC and the blue is AP. The horizontal axis is the class, and the vertical axis is the AUC and AP values.

TABLE 3. Anomaly Detection Performance. The results in the upper table are AUC and the results in the lower table are AP. Specifically, all values are percentages (%) over 5 seeds. The best results are marked in **bold**.

Dataset	CBF	MSST	FST	TPAs	EleD
GAN	50.32%	70.91%	63.21%	55.16%	63.54%
forward-GAN	96.70%	92.21%	96.99%	93.32%	88.87%
backward-GAN	95.43%	91.87%	96.04%	93.19%	86.41%
wo-pfm	91.24%	95.21%	95.25%	93.93%	94.28%
KFCGAN	**99.58%**	**97.33%**	**99.16%**	**96.12%**	**95.70%**
GAN	53.25%	72.21%	64.74%	59.80%	65.91%
forward-GAN	97.40%	92.88%	96.01%	94.15%	86.41%
backward-GAN	97.16%	92.87%	95.27%	94.09%	86.28%
wo-pfm	93.04%	86.90%	95.58%	95.26%	91.63%
KFCGAN	**99.79%**	**93.55%**	**98.95%**	**99.27%**	**92.51%**

transformed between the two domains, while abnormal signals cannot undergo arbitrary conversions. Specifically, for the small dataset CBF, the AUC and AP over 7.72% and 10.41% with the best baseline method MMGAN, which proves that KFCGAN can accurately capture abnormal information in the case of a small amount of training information.

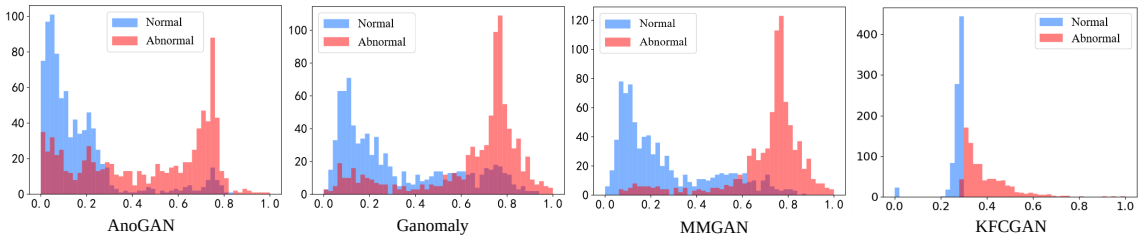

FIGURE 5. Anomaly score Distributions of KFCGAN and compared methods. The horizontal axis is the anomaly score and the vertical axis is the number of samples.

For the high-dimensional dataset MSST, KFCGAN increases the AUC and AP by 3.38% and 5.20%, and for the low-dimensional dataset FST TPAs and EleD, KFCGAN also outperforms other methods, that because that KFCGAN directly uses the difference information between the normal and abnormal signal for anomaly detection, which makes the model independent of the dimension of data.

Figure 4 show the results of KFCGAN by considering each class of signal as normal in the given datasets. It can be observed that KFCGAN exhibits stability and effectively segments normal and abnormal time series when different classes are regarded as normal.

4.3.2. *Ablation Study.* In this section, we verify the effectiveness of each part of the proposed model KFCGAN on UCR datasets. Specifically, cycle-GAN just uses the original signal to train KFCGAN to verify the effectiveness of the Kalman Filter. Besides, we also train the original signal by using the GAN model. To verify the role of the cycle-Consistent adversarial learning, forward-GAN and backward-GAN are just used forward direction and backward direction of the loop of KFCGAN. Besides, in order to study the effectiveness of the discriminator, wo-pfm is the model that removes the pairwise feature matching loss from the objective function of KFCGAN. The ablation study result is shown in Table 3.

From the results shown in Table 3, we can find that KFCGAN performs better than other models. Among them, the results of GAN perform significantly worse than KFCGAN, the reason is they just learn the feature of original signals, which makes them cannot learn the difference between normal and abnormal signals. The forward-GAN and backward-GAN also perform lower than KFCGAN, the main reason is that without the guides of the other direction of the loop, the model can not fully capture the different information between normal and abnormal signals. Different from them, the model wo-pfm is take full advantage of different information between normal and abnormal signals, but without the pairwise feature matching, it cannot learn the difference between normal and abnormal time series. Overall, the analysis proves the effectiveness of the proposed method KFCGAN.

4.3.3. *Visualization.* In this section, we visualize the anomaly score distribution of KFCGAN and other methods. The results are shown in Figure 5. Compared with other methods, KFCGAN can find the boundary of abnormal score distribution more clearly. For the other methods, both normal and abnormal data exhibit similar scores, making them predict more abnormal samples to be normal, which is the reason for their poor performance. For the proposed method KFCGAN, there are also abnormal samples that are detected as normal, but their number is much less than that of other methods. This proves that KFCGAN can effectively separate normal and abnormal data.

5. **Conclusions.** This paper proposes a time series anomaly detection framework named KFCGAN, which detects the anomaly time series by learning the difference between normal and abnormal signals directly. Specifically, KFCGAN employs a Kalman Filter to generate the filtered time series. Then, cycle-consistent adversarial learning is used to learn the transformation between the original time series and the filtered time series. Finally, the anomaly time series is detected by determining whether it can be converted between the original time series domain and the filtered time series domain. The experimental results prove that the proposed KFCGAN is effective in time series anomaly detection tasks.

However, in this paper, the method of filtered time series domain generation is very important. Therefore, in the future, we can explore and design a filtering method which more suitable for anomaly detection to generate the filtered signal domain, and improve the performance of anomaly detection.

Acknowledgment. This work is partially supported by the Research on Related Ethical Issues in Higher Education Reform in the Era of Weak Artificial Intelligence—Based on the Perspective of Technology Intermediary Theory (Minjiang University Scientific Research Project in 2020, Project No. MYS20007), and the Research on the college students'anomie of online courses learning andinterventionof their online courses learning (Minjiang University Scientific Research Project in 2019, Project No. MYS19045).

REFERENCES

[1] J. F. Torres, D. Hadjout, A. Sebaa, F. Martínez-Álvarez, and A. Troncoso, "Deep learning for time series forecasting: a survey," *Big Data*, vol. 9, no. 1, pp. 3–21, 2021.

[2] H. Zhou, S. Zhang, J. Peng, S. Zhang, J. Li, H. Xiong, and W. Zhang, "Informer: Beyond efficient transformer for long sequence time-series forecasting," in *AAAI Conference on Artificial Intelligence*, vol. 35, no. 12, 2021, pp. 11 106–11 115.

[3] Q. Duan, J. Fan, X. Wei, C. Wang, X. Jiao, and N. Wei, "Automatic modulation recognition based on hybrid neural network," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–12, 2021.

[4] J.-L. Cui, B. Lian, Z.-M. Lu, and H.-L. Li, "Research on wheel x-ray defect recognition algorithm based on deep learning," *Journal of Network Intelligence*, vol. 6, no. 4, pp. 753–762, 2021.

[5] Y.-J. Zhang, F.-S. Xiao, and Z.-M. Lu, "Safety helmet wearing detection based on contour and color features," *Journal of Network Intelligence*, vol. 7, pp. 516–525, 2022.

[6] J. Li, B. Yang, H. Li, Y. Wang, C. Qi, and Y. Liu, "Dtdr–alstm: Extracting dynamic time-delays to reconstruct multivariate data for improving attention-based lstm industrial time series prediction models," *Knowledge-Based Systems*, vol. 211, p. 106508, 2021.

[7] Y.-H. Li, L. N. Harfiya, and C.-C. Chang, "Featureless blood pressure estimation based on photoplethysmography signal using cnn and bilstm for iot devices," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–10, 2021.

[8] F. Zhang, T.-Y. Wu, Y. Wang, R. Xiong, G. Ding, P. Mei, and L. Liu, "Application of quantum genetic optimization of lvq neural network in smart city traffic network prediction," *IEEE Access*, vol. 8, pp. 104 555–104 564, 2020.

[9] J.-N. Chen, Y.-P. Zhou, Z.-J. Huang, T.-Y. Wu, F.-M. Zou, and R. Tso, "An efficient aggregate signature scheme for healthcare wireless sensor networks," *Journal of Network Intelligence*, vol. 6, no. 1, pp. 1–15, 2021.

[10] H. Abbasimehr, R. Paki, and A. Bahrini, "A novel approach based on combining deep learning models with statistical methods for covid-19 time series forecasting," *Neural Computing and Applications*, vol. 34, no. 4, pp. 3135–3149, 2022.

[11] M. Alsulami, H. Abu-Zinadah, and A. H. Ibrahim, "Machine learning model and statistical methods for covid-19 evolution prediction," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–6, 2021.

[12] Y. Hu, Y.-F. Zhang, H. Huang, and Y.-P. Zhou, "Attribute-based message recovery designated verifier proxy signature scheme in telemedicine system," *Journal of Network Intelligence*, vol. 7, pp. 101–113, 2022.

[13] Y. Ma, Y. Peng, and T.-Y. Wu, "Transfer learning model for false positive reduction in lymph node detection via sparse coding and deep learning," *Journal of Intelligent & Fuzzy Systems*, vol. 43, no. 2, pp. 2121–2133, 2022.

[14] F. Zhang, T.-Y. Wu, J.-S. Pan, G. Ding, and Z. Li, "Human motion recognition based on svm in vr art media interaction environment," *Human-centric Computing and Information Sciences*, vol. 9, pp. 1–15, 2019.

[15] L. F. S. A. Cruz and D. F. Silva, "Financial time series forecasting enriched with textual information," in *2021 20th IEEE International Conference on Machine Learning and Applications (ICMLA)*. IEEE, 2021, pp. 385–390.

[16] Y. Ma, H. Liu, G. Zhai, and Z. Huo, "Financial risk early warning based on wireless network communication and the optimal fuzzy svm artificial intelligence model," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–20, 2021.

[17] K. Choi, J. Yi, C. Park, and S. Yoon, "Deep learning for anomaly detection in time-series data: review, analysis, and guidelines," *IEEE Access*, vol. 9, pp. 120 043–120 065, 2021.

[18] S. Schmidl, P. Wenig, and T. Papenbrock, "Anomaly detection in time series: a comprehensive evaluation," *the VLDB Endowment*, vol. 15, no. 9, pp. 1779–1797, 2022.

[19] H. Fan, F. Zhang, R. Wang, X. Huang, and Z. Li, "Semi-supervised time series classification by temporal relation prediction," in *ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2021, pp. 3545–3549.

[20] J.-R. Jiang, J.-B. Kao, and Y.-L. Li, "Semi-supervised time series anomaly detection based on statistics and deep learning," *Applied Sciences*, vol. 11, no. 15, p. 6698, 2021.

[21] Y. Alharbi, A. Alferaidi, K. Yadav, G. Dhiman, and S. Kautish, "Denial-of-service attack detection over ipv6 network based on knn algorithm," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–6, 2021.

[22] T. Kieu, B. Yang, C. Guo, R.-G. Cirstea, Y. Zhao, Y. Song, and C. S. Jensen, "Anomaly detection in time series with robust variational quasi-recurrent autoencoders," in *2022 IEEE 38th International Conference on Data Engineering (ICDE)*. IEEE, 2022, pp. 1342–1354.

[23] B. Zhou, S. Liu, B. Hooi, X. Cheng, and J. Ye, "Beatgan: Anomalous rhythm detection using adversarially generated time series." in *IJCAI*, 2019, pp. 4433–4439.

[24] H. Zhao, Y. Wang, J. Duan, C. Huang, D. Cao, Y. Tong, B. Xu, J. Bai, J. Tong, and Q. Zhang, "Multivariate time-series anomaly detection via graph attention network," in *2020 IEEE International Conference on Data Mining (ICDM)*. IEEE, 2020, pp. 841–850.

[25] Y. Ji and H. Lee, "Event-based anomaly detection using a one-class svm for a hybrid electric vehicle," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 6, pp. 6032–6043, 2022.

[26] K. Vos, Z. Peng, C. Jenkins, M. R. Shahriar, P. Borghesani, and W. Wang, "Vibration-based anomaly detection using lstm/svm approaches," *Mechanical Systems and Signal Processing*, vol. 169, p. 108752, 2022.

[27] Y. Zhou, X. Liang, W. Zhang, L. Zhang, and X. Song, "Vae-based deep svdd for anomaly detection," *Neurocomputing*, vol. 453, pp. 131–140, 2021.

[28] A. Deng and B. Hooi, "Graph neural network-based anomaly detection in multivariate time series," in *AAAI Conference on Artificial Intelligence*, vol. 35, no. 5, 2021, pp. 4027–4035.

[29] C. Han, L. Rundo, K. Murao, T. Noguchi, Y. Shimahara, Z. Á. Milacski, S. Koshino, E. Sala, H. Nakayama, and S. Satoh, "Madgan: Unsupervised medical anomaly detection gan using multiple adjacent brain mri slice reconstruction," *BMC Bioinformatics*, vol. 22, no. 2, pp. 1–20, 2021.

[30] H.-B. Ma, X.-G. Chen, Y.-L. Wang, and P.-J. Ji, "Efficient face attribute editing method based on gan," *Journal of Network Intelligence*, vol. 6, no. 3, pp. 646–655, 2021.

[31] P. Ji, H. Ma, Q. Ma, and X. Chen, "A novel method to generate pseudo-random sequence based on gan," *Journal of Network Intelligence*, vol. 7, no. 1, pp. 222–230, 2022.

[32] J. Gui, Z. Sun, Y. Wen, D. Tao, and J. Ye, "A review on generative adversarial networks: Algorithms, theory, and applications," *IEEE Transactions on Knowledge and Data Engineering*, vol. 35, no. 4, pp. 3313–3332, 2021.

[33] A. Odena, C. Olah, and J. Shlens, "Conditional image synthesis with auxiliary classifier gans," in *International Conference on Machine Learning*. PMLR, 2017, pp. 2642–2651.

[34] M. K. Baowaly, C.-C. Lin, C.-L. Liu, and K.-T. Chen, "Synthesizing electronic health records using improved generative adversarial networks," *Journal of the American Medical Informatics Association*, vol. 26, no. 3, pp. 228–241, 2019.
[35] H. Li, S. J. Pan, S. Wang, and A. C. Kot, "Domain generalization with adversarial feature learning," in *IEEE Conference on Computer Vision and Pattern Recognition*, 2018, pp. 5400–5409.
[36] S. M. Iranmanesh, B. Riggan, S. Hu, and N. M. Nasrabadi, "Coupled generative adversarial network for heterogeneous face recognition," *Image and Vision Computing*, vol. 94, p. 103861, 2020.
[37] J.-Y. Zhu, T. Park, P. Isola, and A. A. Efros, "Unpaired image-to-image translation using cycle-consistent adversarial networks," in *IEEE International Conference on Computer Vision*, 2017, pp. 2223–2232.
[38] T. Schlegl, P. Seeböck, S. M. Waldstein, G. Langs, and U. Schmidt-Erfurth, "f-anogan: Fast unsupervised anomaly detection with generative adversarial networks," *Medical Image Analysis*, vol. 54, pp. 30–44, 2019.
[39] S. Akcay, A. Atapour-Abarghouei, and T. P. Breckon, "Ganomaly: Semi-supervised anomaly detection via adversarial training," in *Asian Conference on Computer Vision*. Springer, 2018, pp. 622–637.
[40] T. Han, C. Liu, W. Yang, and D. Jiang, "A novel adversarial learning framework in deep convolutional neural network for intelligent diagnosis of mechanical faults," *Knowledge-based Systems*, vol. 165, pp. 474–487, 2019.
[41] Y. Xiao, H. Shao, S. Han, Z. Huo, and J. Wan, "Novel joint transfer network for unsupervised bearing fault diagnosis from simulation domain to experimental domain," *IEEE/ASME Transactions on Mechatronics*, vol. 27, no. 6, pp. 5254–5263, 2022.
[42] Y. Lei, B. Yang, X. Jiang, F. Jia, N. Li, and A. K. Nandi, "Applications of machine learning to machine fault diagnosis: A review and roadmap," *Mechanical Systems and Signal Processing*, vol. 138, p. 106587, 2020.
[43] A. Degirmenci and O. Karal, "Efficient density and cluster based incremental outlier detection in data streams," *Information Sciences*, vol. 607, pp. 901–920, 2022.
[44] J. Li, H. Izakian, W. Pedrycz, and I. Jamal, "Clustering-based anomaly detection in multivariate time series data," *Applied Soft Computing*, vol. 100, p. 106919, 2021.
[45] P. D'Urso, L. De Giovanni, and R. Massari, "Trimmed fuzzy clustering of financial time series based on dynamic time warping," *Annals of Operations Research*, vol. 299, no. 1, pp. 1379–1395, 2021.
[46] L. Ruff, R. Vandermeulen, N. Goernitz, L. Deecke, S. A. Siddiqui, A. Binder, E. Müller, and M. Kloft, "Deep one-class classification," in *International Conference on Machine Learning*. PMLR, 2018, pp. 4393–4402.
[47] H. Ren, B. Xu, Y. Wang, C. Yi, C. Huang, X. Kou, T. Xing, M. Yang, J. Tong, and Q. Zhang, "Time-series anomaly detection service at microsoft," in *25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, 2019, pp. 3009–3017.
[48] K. Greff, R. K. Srivastava, J. Koutník, B. R. Steunebrink, and J. Schmidhuber, "Lstm: A search space odyssey," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 28, no. 10, pp. 2222–2232, 2016.
[49] K. Park, Y. Choi, W. J. Choi, H.-Y. Ryu, and H. Kim, "Lstm-based battery remaining useful life prediction with multi-channel charging profiles," *IEEE Access*, vol. 8, pp. 20 786–20 798, 2020.
[50] H. Fan, F. Zhang, R. Wang, L. Xi, and Z. Li, "Correlation-aware deep generative model for unsupervised anomaly detection," in *Pacific-Asia Conference on Knowledge Discovery and Data Mining*. Springer, 2020, pp. 688–700.
[51] T. Kieu, B. Yang, C. Guo, and C. S. Jensen, "Outlier detection for time series with recurrent autoencoder ensembles." in *International Joint Conference on Artificial Intelligence (IJCAI)*, 2019, pp. 2725–2732.
[52] F. Lüer, D. Mautz, and C. Böhm, "Anomaly detection in time series using generative adversarial networks," in *2019 International Conference on Data Mining Workshops (ICDMW)*. IEEE, 2019, pp. 1047–1048.
[53] M. A. Bashar and R. Nayak, "Tanogan: Time series anomaly detection with generative adversarial networks," in *2020 IEEE Symposium Series on Computational Intelligence (SSCI)*. IEEE, 2020, pp. 1778–1785.
[54] T. Schlegl, P. Seeböck, S. M. Waldstein, U. Schmidt-Erfurth, and G. Langs, "Unsupervised anomaly detection with generative adversarial networks to guide marker discovery," in *International Conference on Information Processing in Medical Imaging*. Springer, 2017, pp. 146–157.

[55] H. Zenati, M. Romain, C.-S. Foo, B. Lecouat, and V. Chandrasekhar, "Adversarially learned anomaly detection," in *2018 IEEE International Conference on Data Mining (ICDM)*. IEEE, 2018, pp. 727–736.

[56] X. Huang, F. Zhang, H. Fan, and L. Xi, "Multimodal adversarial learning based unsupervised time series anomaly detection," *Journal of Computer Research and Development*, vol. 58, no. 08, pp. 1655–1667, 2021.

[57] W. Tang, G. Long, L. Liu, T. Zhou, J. Jiang, and M. Blumenstein, "Rethinking 1d-cnn for time series classification: A stronger baseline," *arXiv preprint arXiv:2002.10061*, 2020.

[58] H. A. Dau, E. Keogh, K. Kamgar, C.-C. M. Yeh, Y. Zhu, S. Gharghabi, C. A. Ratanamahatana, Yanping, B. Hu, N. Begum, A. Bagnall, A. Mueen, G. Batista, and Hexagon-ML, "The ucr time series classification archive," October 2018, `https://www.cs.ucr.edu/~eamonn/time_series_data_2018/`.