International Journal of Information Security and Privacy
Volume 18 • Issue 1

An IIoT Temporal Data Anomaly Detection Method Combining Transformer and Adversarial Training

Yuan Tian, Yan'an University, China
Wendong Wang, Yan'an University, China*
Jingyuan He, Yan'an University, China

ABSTRACT

The existing Industrial Internet of Things (IIoT) temporal data analysis methods often suffer from issues such as information loss, difficulty balancing spatial and temporal features, and being affected by training data noise, which can lead to varying degrees of reduced model accuracy. Therefore, a new anomaly detection method was proposed, which integrated Transformer and adversarial training. Firstly, a bidirectional spatiotemporal feature extraction module was constructed by combining Graph Attention Networks (GAT) and Bidirectional Gated Recurrent Unit (BiGRU), which can simultaneously extract spatial and temporal features. Then, by combining multi-scale convolution with Long Short-Term Memory (LSTM), multi-scale contextual information was captured. Finally, an improved Transformer was used to fuse multi-dimensional features, combined with an adversarial-trained variational autoencoder to calculate the anomalies of the input data. This method outperforms other comparison models by conducting experiments on four publicly available datasets.

KEYWORDS

BiGRU, Graph Attention Networks, IIoT, Residual Network, Temporal Data Anomaly Detection, Transformer

Time series data refers to a sequence of data points that are indexed or graphed in chronological order. This type of data typically reflects the developmental patterns and changing characteristics of things over time. Temporal data is recorded in human life everywhere, like stock prices in the financial sector, temperature in specific regions during a certain period, electrocardiogram trends, real-time monitoring data collected by sensors in the industrial sector, etc., (Abdelrahman & Keikhosrokiani, 2020; Chatterjee & Ahmed, 2022). The core of temporal data analysis focuses on discovering the patterns from data and predicting future value with historical observations, providing the reference and basis for decision-making. Therefore, more and more researchers are starting to study how to design a model to analyze the temporal data (Chen et al., 2021a).

The temporal data in industrial production is becoming increasingly widespread and IIoT can be seen as a collaborative work that provides a collection of technologies for businesses and

DOI: 10.4018/IJISP.343306 *Corresponding Author

applications using the Internet as a carrier (Ennaji et al., 2023; Fang et al., 2021; Garg et al., 2022). It can utilize electronic devices connected to the physical object, and heterogeneous sensors can collect process control data. These devices include industrial automation systems, medical instruments, and personal computers (Lai et al., 2021; Li & Jung, 2022; Lu et al., 2021). The data between these sensors is highly correlated, and this correlation has complex topological structures and nonlinear characteristics. However, there may be anomalies in the data in IIoT, which could have adverse effects. Thus, it is necessary to design a model to effectively detect anomalies in IIoT temporal data (Song et al., 2023). As deep learning is increasingly used in various fields, Wu et al. (2024) introduced a website link security detection algorithm that leverages multi-modal fusion to enhance prediction accuracy. Meanwhile, Guendouz et al. (2023) devised a novel feature selection approach based on the Dragonfly algorithm, aiming to enhance Android malware detection performance. The method combines different characteristics of the data to build a classification model of the results with machine learning algorithms.

Transformer is a powerful model structure that effectively captures the features of input data through self-attention and multi-head attention mechanisms (Balaji & Sankaranarayanan, 2022). At the same time, Transformer also has parallel computing capabilities and can handle large-scale datasets. Therefore, applying Transformer to anomaly detection in IIoT temporal data can improve detection efficiency and accuracy (Su et al., 2019).

However, simple Transformer models are often susceptible to overfitting and adversarial attacks. To address these issues, consider incorporating adversarial training into Deep Learning (DL) (Wang et al., 2019). Adversarial training adds some noise or interference during the training process, making it more suitable for noise and anomalies in input data. Meanwhile, adversarial training can also improve the model's generalization ability, making it perform better on unprecedented data (Xia et al., 2022; Zhong et al., 2022).

An IIoT temporal data anomaly detection method was proposed, which integrated Transformer and adversarial training to solve the problem of traditional anomaly detection methods unable to handle complex industrial temporal data with high data dimensions, high noise interference, and fast pattern changes. The contribution of the proposed method is as follows:

Combining GAT and BiGRU to construct a bidirectional spatiotemporal feature extraction module that balances spatial and temporal features.

Combining multi-scale convolution and LSTM networks to capture multi-scale contextual information, implementing deep feature extraction based on residual networks, while preventing phenomena such as vanishing gradients, exploding gradients, overfitting, and network degradation.

Adopting an improved Transformer to achieve multi-dimensional feature fusion, combining pooling to balance global and local features to avoid issues such as information loss.

Combining adversarial training with a variational autoencoder to amplify abnormal reconstruction errors effectively solves the problem of low model performance caused by training data noise in traditional autoencoder models.

RELATED WORK

Abnormal data in IIoT may lead to damage or malfunction of industrial equipment, affecting the quality and efficiency of industrial production, and reducing the safety and reliability of IIoT systems. Therefore, the detection and management of abnormal data is a very important aspect of IIoT. By using effective anomaly detection methods, abnormal data can be detected and processed in a timely manner; thereby, ensuring the normal operation of the IIoT system.

Prediction Based Methods

When detecting temporal anomaly data, using the Recurrent Neural Network (RNN) and the variants network was a common approach. For the simplification and lightweight consideration of the model