ICCSNT

October 18-19, 2025
Harbin, China

Graph Contrastive Learning for Service Security Risk Analysis in Power Communication Networks

Yuanpeng Ge[1], Songlei Zhang[2], Huang Lin[3*], Liangsong Zhang[4], Jialu Li[5]

State Grid Fujian Electric Power Company Limited Information Communication Branch

MOTIVITION

- **The increasing complexity of power communication networks, driven by system expansion and emerging technologies, poses significant challenges for ensuring secure and reliable operations.**
- **To address the scarcity of abnormal samples and the difficulty of obtaining labels in real-world scenarios, we propose a security verification framework based on digital twin segments for communication optical cables. The proposed methodology is expected to offer new strategies for intelligent security protection and to contribute significant theoretical insights and practical guidance for enhancing the safety and reliability of modern power systems.**

PROBLEM DEFINITION

A power communication network:

$$G = \{V, E, X\}$$

Adjacency matrix: A

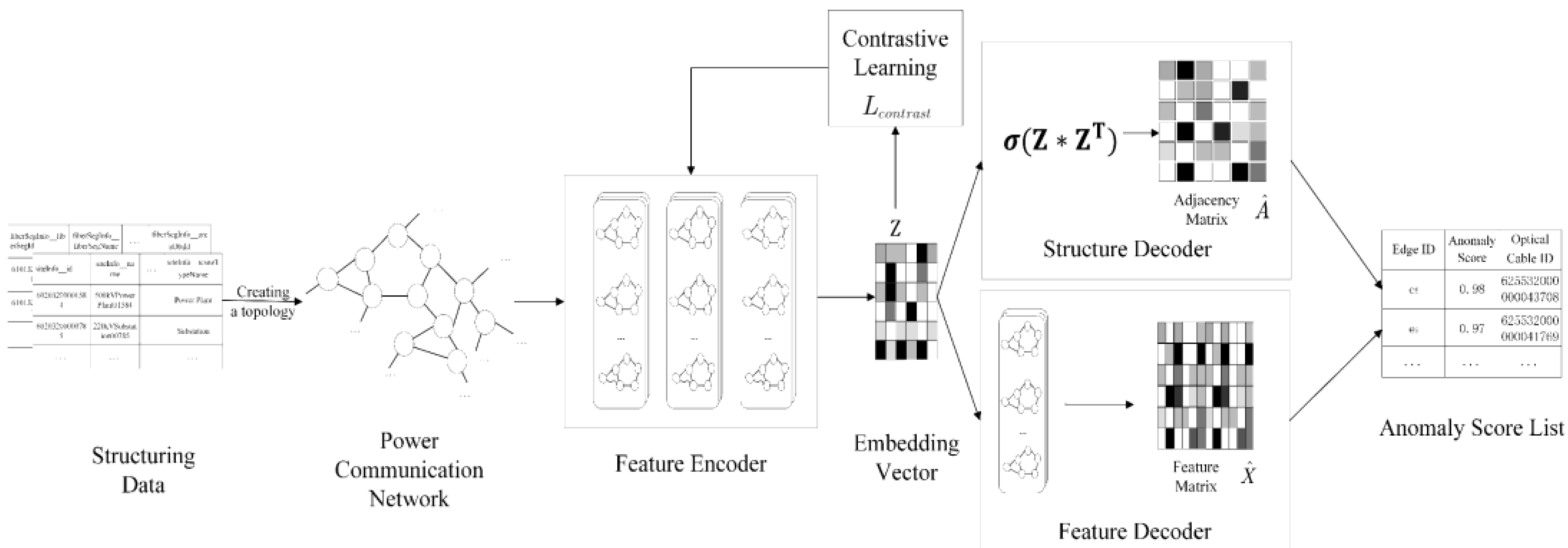
Set of edge attributes: X

Set of optical cables:

$$E = \{e_1, e_2, \ldots, e_m\}$$

Set of sites (nodes): V

Incremental Anomaly Detection Model



Framework of the incremental anomaly detection

EXPERIMENT RESULTS

Evaluation metrics

✓ ROC-AUC:

- The ROC curve is a plot of the True Positive Rate (TPR) against the False Positive Rate (FPR).
- The AUC (Area Under Curve) refers to the area under the ROC curve.

✓ Recall@K:

$$\text{Recall@}K = \frac{\text{TP@}K}{N_{\text{anom}}}$$

Comparison of Methods

Method	*Algorithm*	*Deep learning*	*Graph contrast learning*
SCAN[10]	Graph clustering	×	×
GCNAE[11]	GCN+AE	√	×
ours	GCN+AE	√	√

Comparison of Experimental Results

Method	*AUC*	*Recall@K(K=300)*	*Recall@K(K=500)*
SCAN[10]	0.66	0.1255	0.5623
GCNAE[11]	0.77	0.2556	0.6596
ours	0.87	0.7523	0.8644