International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.com | editor@ijrai.com | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 6, Issue 6, November-December 2023||

DOI:10.15662/IJRAI.2023.0606001

Graph-Based Anomaly Detection in Cyber-Physical Systems

Sheetal Sanjay Yadav

Maharishi Arvind University, Jaipur, Rajasthan, India

ABSTRACT: Cyber-Physical Systems (CPS)—comprising tightly integrated computational and physical components—are foundational in domains like industrial automation, smart grids, and autonomous vehicles. Detecting anomalies in CPS is critical to maintain safety, reliability, and security. Graph-based anomaly detection approaches have emerged as powerful tools capable of capturing complex dependencies among sensors and actuators—modelled as nodes and edges—and identifying deviations in structural or temporal behavior.

This paper reviews key graph-centric methods tailored for CPS anomaly detection that predate 2022. We highlight techniques like graph-augmented predictive models, GAN-based frameworks capturing multivariate interactions, and Bayesian network structures modeling causal dependencies. For instance, **Multi-Level Graph Attention Networks (PCGAT)** model both physical process and controller communication graphs for real-time anomaly localization in industrial control systems MDPI. Additionally, **MAD-GAN** leverages LSTM-based GANs to capture spatial-temporal dependencies across sensor networks, showing efficacy in detecting CPS intrusions in cyber-physical water systems arXiv. Bayesian network approaches such as **TABOR** integrate timing and sensor-actuator relationships for detecting anomalies in CPS environments MDPI.

We synthesize these methodologies, discuss their suitability for CPS architectures, assess relative strengths and limitations, and propose a unified multi-stage methodology integrating graph construction, modeling, and detection phases.

Advantages include modeling spatial-temporal dependencies more naturally and enabling anomaly localization. Challenges involve data labeling scarcity, model complexity, and real-time computational constraints.
Ultimately, integrating graph-based models holds promise for advanced anomaly detection in CPS—especially with improvements in graph learning and streaming capabilities. Future directions include graph neural network adoption, real-time learning, and interpretable causal graph methods for CPS.

KEYWORDS: Cyber-Physical Systems (CPS), Graph-Based Anomaly Detection, Graph Neural Networks (GNN), MAD-GAN, PCGAT, Bayesian Networks, Spatial-Temporal Modeling, Sensor Networks, Industrial Control Systems, Intrusion Detection

I. INTRODUCTION

Cyber-Physical Systems (CPS) integrate computation with physical processes via sensors, actuators, and controllers. Their interconnected nature introduces complex dependencies, making anomaly detection critical yet challenging. Traditional threshold-based or feature-based methods often fall short, failing to capture structural dependencies or dynamics across components. Graph-based approaches naturally fit CPS environments: sensors and actuators become nodes, and functional or communication interactions form edges. This structure allows modeling joint spatial and temporal behaviors—vital in cyber-physical anomaly contexts.

This paper examines graph-based anomaly detection in CPS up to 2022. We focus on methods grounded in deep learning, GANs, attention networks, and probabilistic graph methods.

Key examples include:

- **PCGAT**, applying multi-level graph attention to both physical process and controller communication, enabling accurate detection and localization in industrial control systems MDPI.

- **MAD-GAN**, using GANs with LSTM-based modeling of inter-sensor dependencies to detect anomalies in systems like SWaT and WADI datasets arXiv.
- **TABOR**, employing Time Automata and Bayesian Networks for detecting timing anomalies through dependency modeling MDPI.

By exploring these, we aim to synthesize their contributions, evaluate strengths and limitations, and propose a framework combining graph modeling, anomaly scoring, and interpretability for robust CPS anomaly detection.

II. LITERATURE REVIEW

1. **Multi-Level Graph Attention Networks (PCGAT)**
2. PCGAT constructs both physical process and controller communication graphs from CPS data. It integrates features via graph attention mechanisms to predict sensor behavior and detect/pinpoint anomalies effectively MDPI.
3. **MAD-GAN (Multivariate Anomaly Detection with GAN)**
4. This framework models all sensors jointly using GANs enhanced by LSTM to capture spatial-temporal correlations. Tested on SWaT and WADI datasets, MAD-GAN achieves strong anomaly detection through reconstruction and discriminator-based scoring arXiv.
5. **Bayesian Network Approaches (e.g., TABOR)**
6. TABOR combines Time Automata and Bayesian Networks to model dependencies among CPS components, enabling detection of timing and value anomalies by leveraging dependency violations MDPI.

These works illustrate progression from early dependency modeling toward deep graph-aware techniques, each addressing CPS-specific characteristics like temporal dependencies, sensor interactions, and system hierarchy.

III. RESEARCH METHODOLOGY

To consolidate graph-based anomaly detection methods in CPS up to 2022, we:

1. **Identification of Key Graph-Based Methods**
2. Focused on PCGAT, MAD-GAN, and TABOR, representing attention mechanisms, generative modeling, and probabilistic graphs.
3. **Method Comparative Analysis**
4. Compared graph construction strategies, anomaly scoring mechanisms, computational frameworks, and evaluation environments (e.g., SWaT, WADI datasets).
5. **Architectural Synthesis**
6. Proposed a reference pipeline with: graph creation (structural + temporal edges), model selection (attention, GAN, Bayesian), anomaly scoring, and localization modules.
7. **Evaluation of Trade-offs**
8. Highlighted modeling strength vs. complexity, suitability for real-time deployment, and explainability.

This methodology enables an integrative understanding, guiding CPS practitioners in selecting suitable graph-based tools.

IV. ADVANTAGES

- **Captures structural and temporal dependencies** beyond value thresholds.
- **Localizes anomalies** by node-level scoring in structured graphs (e.g. PCGAT).
- **Robust in multivariate settings** via joint modeling of sensor interactions (e.g. MAD-GAN).
- **Probabilistic interpretation** through Bayesian networks aids explainability (e.g. TABOR).

V. DISADVANTAGES

- **High computational complexity**, particularly with deep graph models.
- **Label scarcity** in CPS datasets limits supervised training or tuning.
- **Model interpretability** and justification of anomalies remain challenging.
- **Real-time deployment barriers** due to heavy graph computation and training overhead.

VI. RESULTS AND DISCUSSION

- **PCGAT**: Demonstrated accurate anomaly detection and localization in industrial CPS; relies on pre-defined graph construction MDPI.
- **MAD-GAN**: Effective on real datasets; capturing latent dependencies improves detection, though GAN training is sensitive to hyperparameters arXiv.
- **TABOR and similar**: Offers structured anomaly reasoning via dependencies, but may not handle large-scale CPS directly MDPI.

Combined, these methods show promise. Attention-based models may balance performance and interpretability, while GANs excel in unlabelled domains. Probabilistic graphs are robust for causal anomaly reasoning, but each has trade-offs in computation and data needs.

VII. CONCLUSION

Graph-based anomaly detection significantly enhances CPS monitoring by accommodating structural and temporal dependencies. Pre-2022 methods offer diverse approaches—from attention networks to GANs and Bayesian structures—each with pros and limitations. The evolution toward graph-informed modeling marks progress, but requires careful balancing of complexity, interpretability, and deployment feasibility.

VIII. FUTURE WORK

- **Graph Neural Networks (GNNs)**: Explore GNNs for more expressive modeling and real-time inference.
- **Real-Time Streaming Models**: Adapt existing models to process continuous CPS data.
- **Explainability**: Enhance model transparency using causal graph analysis.
- **Dataset Expansion**: Create and use larger benchmarks for CPS anomaly detection.

REFERENCES

1. Authors of PCGAT (Multi-Level Graph Attention Network Based Anomaly Detection in Industrial Control System) MDPI.
2. Li, Chen, Shi, et al. (2019). MAD-GAN: Multivariate Anomaly Detection for Time Series Data with GANs arXiv.
3. Lin et al. (TABOR): Time Automata and Bayesian Network model for anomaly detection in CPS MDPI.
4. Luo, Xiao, Cheng, Peng & Yao (2021). Survey on Deep Learning-Based Anomaly Detection in CPS