Graph Anomaly Detection with Graph Convolutional Networks

Aabid A. Mir, Megat F. Zuhairi, Shahrulniza Musa
Malaysian Institute of Information Technology, Universiti Kuala Lumpur, Kuala Lumpur, Malaysia

***Abstract*—Anomaly detection in network data is a critical task in various domains, and graph-based approaches, particularly Graph Convolutional Networks (GCNs), have gained significant attention in recent years. This paper provides a comprehensive analysis of anomaly detection techniques, focusing on the importance and challenges of network anomaly detection. It introduces the fundamentals of GCNs, including graph representation, graph convolutional operations, and the graph convolutional layer. The paper explores the applications of GCNs in anomaly detection, discussing the graph convolutional layer, hierarchical representation learning, and the overall process of anomaly detection using GCNs. A thorough review of the literature is presented, with a comparative analysis of GCN-based approaches. The findings highlight the significance of graph-based techniques, deep learning, and various aspects of graph representation in anomaly detection. The paper concludes with a discussion on key insights, challenges, and potential advancements, such as the integration of deep learning models and dynamic graph analysis.**

***Keywords*—Anomaly detection; deep learning; dynamic graphs; Graph Convolutional Networks (GCNs); Graph Neural Networks (GNNs); network data**

I. Introduction

Graph anomaly detection has gained significant attention in various domains, including insider threat detection, fraud detection, and network security [1]. The increasing prevalence of complex network data, such as social networks, financial transactions, and blockchain networks, has posed challenges for traditional anomaly detection approaches in capturing the inherent structural dependencies and contextual information encoded in graph-structured data [2]. As a result, there has been a growing interest in leveraging deep learning techniques, particularly graph convolutional networks (GCNs), to address these limitations and achieve more effective anomaly detection [3]. The primary objective of graph anomaly detection is to identify abnormal patterns, behaviors, or entities within a given graph. This involves analyzing the connections, relationships, and attributes of the nodes and edges in the graph to distinguish between normal and anomalous instances [4]. Deep learning-based approaches, especially GCNs, have shown promising results in capturing the complex dependencies and learning meaningful representations from graph-structured data [2].

In this paper, we aim to provide a comprehensive introduction to graph anomaly detection, with a particular focus on GCN-based methods. We will discuss the foundational concepts and techniques in anomaly detection, highlighting the unique challenges posed by graph-structured data. Additionally, we will look into the advancements made in the field, with a specific focus on the utilization of GCNs for modeling and analyzing graphs. We will explore how GCNs leverage graph convolutions to propagate information between nodes, enabling them to capture both local and global structural information.

This study analyzes the field of graph-based anomaly detection in network data in the subsequent sections, beginning with the background and motivation in Section II. Section III explores the details of anomaly detection in network data, establishing the foundation for an in-depth comprehension of its complexities. Section IV then expands on the fundamental backbone of this study, Graph Convolutional Networks (GCNs), providing insights into its structure and pivotal role in anomaly detection. Section V, describes the methodology used for analysis. Section VI then presents a comprehensive overview of the existing literature, focusing on GCN-based techniques and their comparative analysis. Section VII summarizes the findings and conclusions obtained from the review and the discussion section VIII discusses the essential insights, limitations, and issues encountered in graph-based anomaly detection, answering the three research questions of this study. Section IX provides a concise summary of the findings and future research prospects. Finally, in Section X, the conclusion summarizes the findings and implications established during the study.

II. Background and Motivation

Graph anomaly detection has emerged as a critical task in various domains, including network security, fraud detection, and anomaly monitoring in dynamic systems. Traditional methods often rely on handcrafted features or statistical techniques, which may lack the ability to capture complex patterns and hidden anomalies. In recent years, the advent of deep learning and graph convolutional networks (GCNs) has provided new opportunities for more effective and automated graph anomaly detection [1] [5].

The motivation behind this research stems from the growing need to develop advanced techniques that can effectively detect anomalies in complex graph-structured data. With the increasing scale and complexity of real-world networks, there is a pressing demand for anomaly detection methods that can handle large-scale graphs and capture intricate relationships between entities [4] [45]. By leveraging the power of GCNs and deep learning, it is possible to extract high-level representations from graphs and capture both local and global patterns, leading to more accurate and robust anomaly detection [6].

III. Anomaly Detection in Network Data

A. Overview of Anomaly Detection Techniques

Anomaly detection is a critical task in network data analysis, aiming to identify abnormal patterns or behaviors that deviate from the expected norm. Various techniques have been proposed to tackle this problem. Traditional approaches include statistical methods, clustering algorithms, and rule-based systems [1] [2]. However, these methods often struggle to capture complex dependencies and subtle anomalies in large-scale network data. Recent advancements in deep learning and graph theory have led to the emergence of novel anomaly detection techniques that leverage the structural information of networks. These techniques have shown promising results in detecting anomalies in diverse domains, including cybersecurity, fraud detection, and insider threat detection [5].

B. Importance and Challenges of Network Anomaly Detection

Network anomaly detection plays a vital role in maintaining the security and integrity of network systems. Anomalies in network data can indicate malicious activities, system failures, or emerging threats. However, detecting anomalies in complex networks poses several challenges. First, networks often exhibit dynamic behavior, making it difficult to distinguish between normal fluctuations and anomalous events [6]. Second, network data is high-dimensional and heterogeneous, containing various attributes and interdependencies. Third, anomalies can manifest in different forms, such as structural changes, attribute deviations, or unusual patterns. These challenges highlight the need for advanced anomaly detection techniques that can effectively capture the complex characteristics of network data and adapt to evolving network dynamics [7] [8] [9]. Furthermore, the work of [11] proposes new approaches to address these challenges.

C. Graph-based Anomaly Detection Methods

Graph-based anomaly detection methods have gained significant attention due to their ability to model and exploit the inherent structure of network data. These methods represent network data as graphs, where nodes represent entities (e.g., users, devices) and edges capture relationships or interactions. By leveraging graph theory and network analysis techniques, graph-based anomaly detection methods can effectively capture local and global dependencies, identify abnormal patterns, and distinguish between different types of anomalies [12]. These methods often utilize graph-based features, such as node degrees, clustering coefficients, and centrality measures, to detect anomalies [5]. Furthermore, [21] introduced a novel graph-based anomaly detection algorithm that incorporates additional attributes and contextual information associated with nodes and edges.

D. Introduction to Graph Convolutional Networks (GCNs)

Graph Convolutional Networks (GCNs) have emerged as a powerful deep learning technique for graph-based anomaly detection [13]. GCNs extend convolutional neural networks (CNNs) to operate directly on graph-structured data. They leverage a localized aggregation scheme, where each node aggregates information from its neighboring nodes, capturing the graph's structural properties. By stacking multiple graph convolutional layers, GCNs can capture hierarchical representations of the network data [14]. This hierarchical representation allows GCNs to learn discriminative features and identify anomalous patterns in the network. Moreover, GCNs can handle attributed graphs, where additional features are associated with nodes or edges, enabling the integration of both structural and attribute information for more accurate anomaly detection [11] [16]. The researchers in [41] propose an enhanced version of GCNs for graph-based anomaly detection.

IV. Graph Convolutional Networks (GCNs)

A. Fundamentals of Graph Convolutional Networks (GCNs)

Graph Convolutional Networks (GCNs) have emerged as a powerful deep learning technique for analyzing graph-structured data. GCNs extend the convolutional operation from regular grids, such as images, to irregular graph structures, enabling effective representation learning and analysis of complex relational data [48]. Graph Convolutional Networks provide a powerful framework for learning representations and analyzing graph-structured data. Through graph convolutional layers, spectral-based or spatial-based approaches, and effective training techniques, GCNs enable deep learning on complex relational data, offering promising solutions in diverse application domains [47] [49].

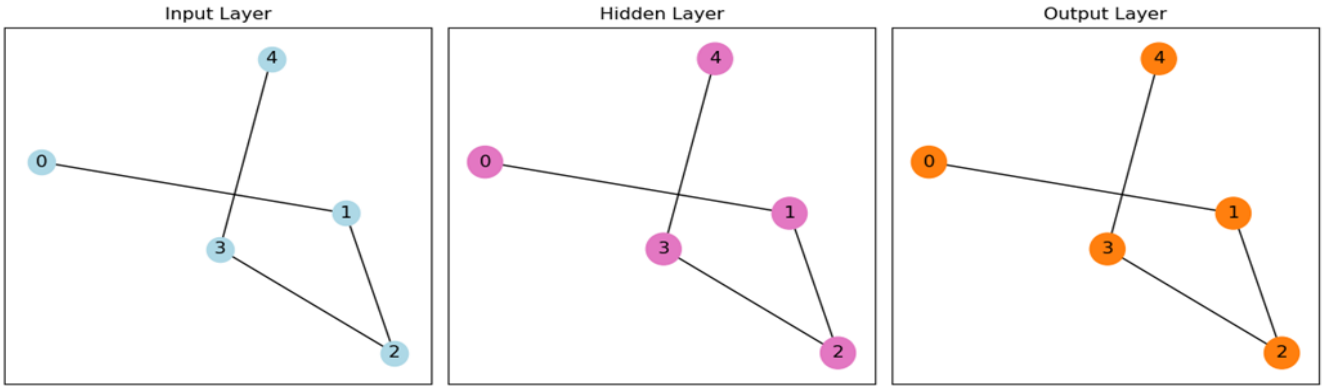

Fig. 1. Graph Convolutional Network (GCN) applied to a sample graph.

B. Graph Representation

A graph is a mathematical representation that consists of nodes and edges, where nodes represent entities or elements, and edges capture relationships or connections between nodes. Graphs are widely used to model various real-world systems, such as social networks, citation networks, and biological networks. Formally, a graph can be represented as G = (V, E), where V denotes the set of nodes and E represents the set of edges connecting pairs of nodes [47].

C. Graph Convolutional Operations

The core operation in GCNs is the graph convolution, which generalizes the convolutional operation to graph-structured data. In traditional convolutional neural networks (CNNs), convolutions are performed on regular grids using fixed-size filters. In contrast, GCNs leverage the graph structure to define a neighborhood aggregation scheme. Given a graph G = (V, E) with node features $X \in R^{N \times D}$, where N is the number of nodes and D is the feature dimension, the graph convolution operation aims to update the node representations by aggregating information from their neighboring nodes [48].

D. Graph Convolutional Layer

The graph convolutional layer is the building block of GCNs. It combines the graph convolution operation with non-linear transformations to learn expressive node representations. The output of a graph convolutional layer can be computed as $H = \sigma(AXW)$, where $H \in R^{N \times F}$ is the output matrix of node representations, A is the adjacency matrix that encodes the graph structure, X is the input node feature matrix, W is the learnable weight matrix, and σ denotes the activation function. By iteratively stacking multiple graph convolutional layers, GCNs can capture increasingly complex and abstract features [48].

E. Spectral-based and Spatial-based Approaches

GCNs can be categorized into spectral-based and spatial-based approaches based on the underlying mathematical framework. Spectral-based GCNs leverage the graph Laplacian matrix to transform the graph convolution operation into the spectral domain, where the eigenvectors of the Laplacian matrix serve as the basis for filtering the node features. Spatial-based GCNs, on the other hand, operate directly on the spatial relationships between nodes without relying on the eigenvalue decomposition. They typically employ local neighborhood aggregation schemes to capture information propagation on the graph [45] [46].

F. Training and Learning

GCNs are trained using labeled data through a supervised learning process. The training objective typically involves minimizing a loss function that measures the discrepancy between the predicted labels and the ground truth labels. To mitigate overfitting and enhance generalization, regularization techniques such as dropout and weight decay can be applied. Moreover, the backpropagation algorithm, coupled with gradient descent optimization, is employed to update the parameters of the GCN model iteratively [48].

G. GCNs in Anomaly Detection

Graph Convolutional Networks (GCNs) have gained significant attention in anomaly detection due to their ability to capture complex relational information and extract meaningful features from graph-structured data. GCNs leverage graph convolution operations to propagate information among nodes and learn node representations that encode both local and global structural characteristics of the graph. By exploiting the relational dependencies encoded in the graph, GCNs can effectively capture complex patterns and identify anomalies that would be challenging to detect using traditional methods. Several studies have demonstrated the effectiveness of GCNs in anomaly detection across various domains, such as insider threat and fraud detection [1], Ethereum blockchain network [5], and network anomaly detection [7]. Researchers have explored techniques like adaptive graph convolutional layers, local and global aggregation strategies [4], data augmentation [8], and community detection [9] to enhance the performance of GCNs in anomaly detection. Continued research aims to develop novel GCN architectures and techniques to further improve accuracy and robustness in diverse application domains.

Fig. 1 represents a Graph Convolutional Network (GCN) model applied to a sample graph. The visualization consists of three subplots: the input layer, the hidden layer, and the output layer. In the input layer, nodes are shown as circles with light blue colors representing the input features. In the hidden layer, nodes are colored based on the features extracted by the GCN model using the 'coolwarm' colormap. Finally, in the output layer, nodes are colored according to the predicted class labels using the 'Set1' colormap. This visualization helps understand how the GCN model transforms the input features, captures meaningful representations in the hidden layer, and makes predictions in the output layer, providing insights into the model's inner workings. Anomaly detection using GCNs involves computing anomaly scores, which quantify the likelihood of an anomaly, by comparing predicted representations with reconstructed representations. Training on labeled data allows GCNs to learn normal patterns and discriminate between normal instances and anomalies. The mathematical equations that underpin GCN-based anomaly detection provide a formal framework for understanding the key components of the approach.

1) Graph convolutional layer: Node Representation Update: The update rule for a single graph convolutional layer can be defined as:

$$h_v^{(l+1)} = \sigma\left(\sum_u \quad h_u^{(l)} W^{(l)}\right) \qquad (1)$$

Here,

$h_u^{(l)}$ represents the representation of node *v* at layer *l*,

$W^{(l)}$ denotes the learnable weight matrix at layer *l*,

σ is an activation function, and the sum is taken over the neighboring nodes *u* of *v*.

2) Hierarchical representation learning: Stacked Graph Convolutional Layers: Multiple layers of graph convolutions

can be stacked to capture increasingly complex patterns and higher-order relationships. The hierarchical representation learning can be expressed as,

$$h_v^{(L)} = GCN(h_v^{(L-1)}, A) \quad (2)$$

Here,

$h_v^{(L)}$ represents the final representation of node *v* after *L* layers of graph convolutions,

GCN denotes the graph convolutional operation, and

A is the adjacency matrix representing the graph structure.

3) Anomaly detection anomaly score calculation: Anomaly detection can be performed by computing anomaly scores for nodes based on their predicted representations and reconstructed representations. The anomaly score can be calculated as:

$$s_v = f(h_v^{(L)}, h_v^{(L")}) \quad (3)$$

Here,

s_v represents the anomaly score assigned to node *v*,

$h_v^{(L)}$ is the predicted representation of node *v* using the GCN,

$h_v^{(L")}$ is the reconstructed representation of node *v*, and

f is a function that measures the difference between the predicted and reconstructed representations.

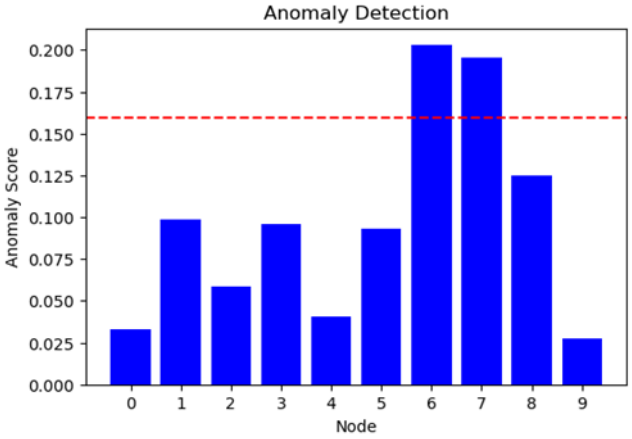

Fig. 2. Bar chart visualization of the anomaly detection results, allowing for quick identification of nodes with higher anomaly scores and potential outliers in the graph.

Fig. 2 provides a visualization of anomaly scores for each node in the graph. The x-axis represents the nodes, numbered from 0 to 9, and the y-axis represents the anomaly scores. The height of each bar corresponds to the anomaly score of the respective node.

The blue bars in the chart represent the anomaly scores of the nodes, indicating the level of deviation from the expected pattern. Higher bars indicate higher anomaly scores, suggesting nodes with more significant deviations. The red dashed line represents the anomaly threshold, separating the nodes into normal and anomalous categories. Nodes above the threshold are considered anomalous, while nodes below the threshold are considered normal.

4) Training and evaluation training on labeled data: GCNs can be trained on a labeled dataset containing normal and anomalous instances to learn to distinguish between them. The training objective can be defined as:

$$min \sum \quad Loss(y_v, GCN(h_v^{(L)}, A)) \quad (4)$$

Here, Loss is a loss function that compares the predicted labels y_v^ with the ground truth labels, and the sum is taken over all nodes in the training dataset.

V. Methodology

This systematic literature review (SLR) follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) [10] guidelines to investigate the topic of "Graph Anomaly Detection with Graph Convolutional Networks." Fig. 3 shows the PRISMA flow diagram. The purpose of this SLR is to provide a comprehensive analysis and synthesis of the existing literature on the application of graph convolutional networks (GCNs) for detecting anomalies in graph-structured data.

A. Research Questions

The following research questions guide this review:

RQ1. What are the current approaches and techniques for graph anomaly detection using GCNs?

RQ2. What are the challenges and limitations of existing GCN-based graph anomaly detection methods?

RQ3. What are the emerging trends and future directions in this field?

B. Search Strategy

Our search strategy, which initially relied on automated techniques using logical operators, was followed by rigorous manual curation. We have exercised our expertise to select articles that met our stringent criteria for quality and relevance. This dual approach ensures the inclusion of the most relevant and high-quality sources. A systematic search was conducted in major academic databases, including IEEE Xplore, ACM Digital Library, Springer, Elsevier, Scopus, and Google Scholar. The search terms used included variations of "graph anomaly detection," "graph convolutional networks," "graph neural networks," and "anomaly detection in graph data." The search was limited to articles published between 2019 and 2023.

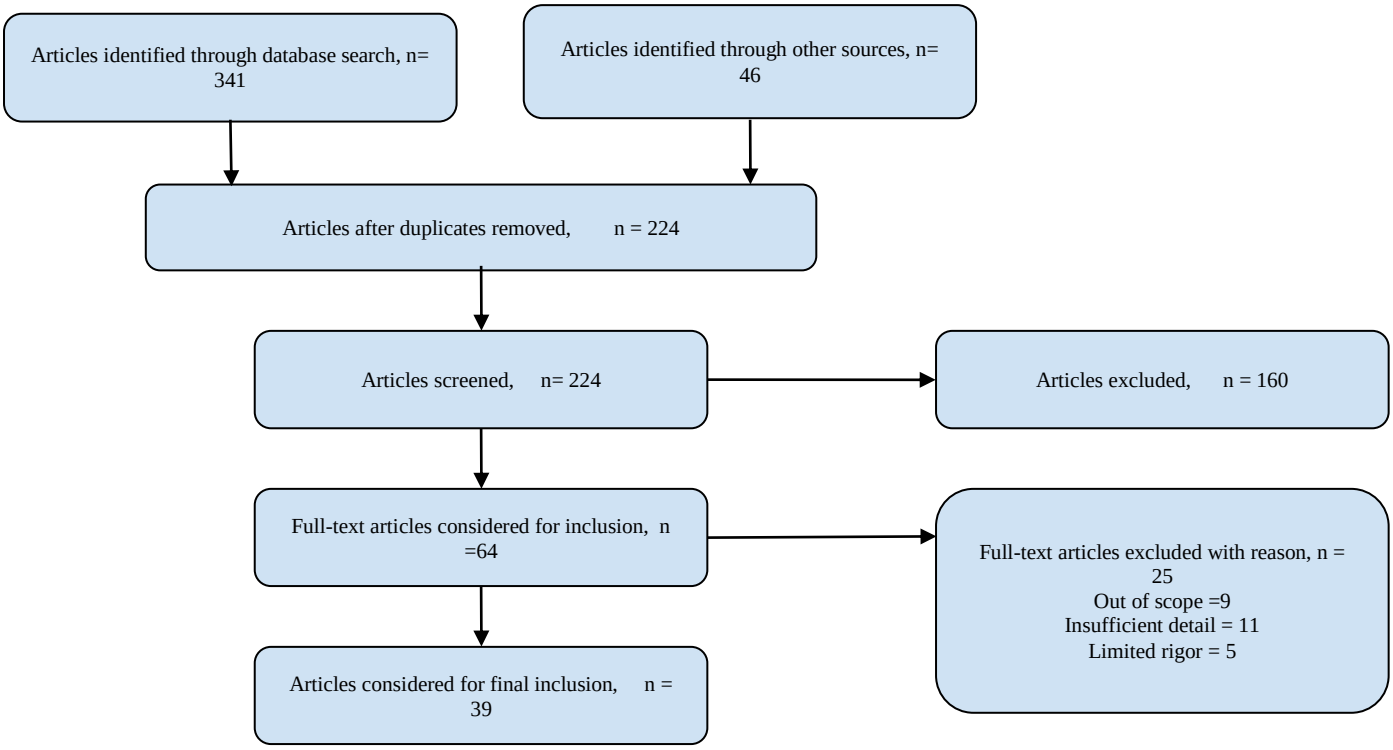

Fig. 3. PRISMA flow diagram.

C. Study Selection

The inclusion and exclusion criteria were defined to ensure the relevance and quality of the studies. Included studies were required to:

- Focus on the application of GCNs for graph anomaly detection.
- Present novel methodologies, techniques, or frameworks.
- Include evaluation metrics and datasets.
- Be published in peer-reviewed journals or conference proceedings.

Studies that did not meet the inclusion criteria, such as review articles, tutorials, or studies unrelated to graph anomaly detection, were excluded.

D. Data Extraction

Data from the selected studies were extracted using a standardized form. The extracted information included:

- Author(s) and publication details.
- Key contributions.
- Methodologies, techniques, and algorithms used.
- Datasets employed for evaluation.
- Evaluation metrics and performance results.
- Limitations and future research.

E. Data Synthesis

A qualitative synthesis was performed to analyze the findings from the selected studies. The key themes, methodologies, challenges, and trends in graph anomaly detection with GCNs were identified. The studies were analyzed to identify commonalities, differences, and gaps in the existing literature.

F. Quality Assessment

The quality and rigor of the selected studies were assessed using predefined criteria. The criteria included aspects such as research design, clarity of methodology, use of appropriate datasets, and statistical analysis.

G. Results Presentation

The findings of this SLR will be presented in a narrative format, organized thematically based on the identified research areas, methodologies, challenges, and trends. The results will be accompanied by tables, figures, and visual representations to enhance understanding and facilitate comparisons.

H. Limitations

The limitations of this SLR include potential publication bias, language limitations, and the possibility of missing relevant studies despite the comprehensive search strategy.

VI. Review of Literature

A. Overview of Selected Studies

Anomaly detection has become a critical task in various domains, such as cybersecurity, finance, healthcare, and industrial systems. Researchers have been investigating the

use of graph-based methods for anomaly detection, leveraging the power of graph neural networks (GNNs) and deep learning techniques. A comprehensive survey by [2] provides an extensive overview of graph anomaly detection with deep learning, highlighting the advancements and challenges in this field. Several studies have focused on leveraging GNNs for anomaly detection, such as the work by [1], who proposed using graph convolutional networks (GCNs) for insider threat and fraud detection. The researchers in [3] also explored graph anomaly detection with graph neural networks, discussing the current state and challenges in this area. Various approaches have been proposed to enhance the performance of graph anomaly detection. For instance, Ding and Li (2022) presented AnoGLA, an efficient scheme for improving network anomaly detection, while [5] developed a graph deep learning-based anomaly detection model specifically for Ethereum blockchain networks. The researchers in [6] introduced graph fairing convolutional networks for anomaly detection, aiming to address the fairness issue in graph-based models. The researchers in [7] proposed a rethinking of graph neural networks for anomaly detection, exploring novel architectures and techniques. The researchers in [8] developed DAGAD, a data augmentation method for graph anomaly detection, to enhance the performance of anomaly detection models. Furthermore, researchers have focused on incorporating domain-specific features and knowledge into graph anomaly detection. The researchers in [9] proposed COMGA, a community-aware attributed graph anomaly detection method that considers community structures in graphs. The researchers in [11] introduced GCCAD, a graph contrastive learning approach for anomaly detection, which leverages the contrastive learning framework. The researchers in [13] developed a high accuracy and adaptive anomaly detection model using a dual-domain graph convolutional network for insider threat detection. The researchers in [18] proposed Guard Health, a secure data management system that combines blockchain technology with graph convolutional networks for anomaly detection in smart healthcare. The literature also includes studies focusing on temporal aspects of graph anomaly detection. For example, the paper [19] addressed motif-level anomaly detection in dynamic graphs, while [21] proposed structural temporal graph neural networks for anomaly detection in dynamic graphs. The researchers in [41] introduced a multi-scale contrastive learning network with augmented view for graph anomaly detection. The researchers in [39] presented a synergistic approach that combines pattern mining and feature learning for graph anomaly detection. The researchers in [44] explored addressing heterophily in graph anomaly detection by considering the graph spectrum.

These selected studies highlight the diverse approaches and advancements in graph anomaly detection using deep learning techniques. From leveraging GNNs and GCNs to incorporating domain-specific knowledge and addressing temporal aspects, researchers are continuously striving to improve the accuracy and effectiveness of graph-based anomaly detection methods.

B. Comparative Analysis of GCN-based Approaches

A comprehensive comparative analysis of various Graph Convolutional Network GCN-based approaches for anomaly detection is presented in this section. The analysis is conducted in a tabular format, considering several key parameters to evaluate and compare the different approaches. The parameters include the reference source, graph type, method, category, objective function employed, measurement metrics used for evaluation, and the outputs of the approaches. This comparative analysis provides insights into the similarities, differences, and effectiveness of different GCN-based approaches in addressing anomaly detection tasks. By examining these parameters, we aim to identify the strengths and limitations of each approach, facilitating a better understanding of their performance and applicability in real-world scenarios.

Table I provides an analysis of various studies focused on anomaly detection using graph-based approaches. It includes information about the types of graphs used, specific methods employed, categories of anomaly detection, objective functions used measurement metrics for evaluation, and the outputs of these approaches. The table offers a comprehensive overview of different studies, highlighting their techniques, evaluation criteria, and intended applications. These studies utilize diverse types of graphs, such as attribute graphs, social graphs, blockchain transaction graphs, dynamic graphs, etc., and employ methods like Graph Convolutional Networks (GCNs), graph deep learning, community-aware attributed graph anomaly detection, contrastive learning, among others. The evaluation metrics primarily consist of precision, recall, F1-Score, AUC-ROC, and accuracy, showcasing the effectiveness of these approaches in detecting anomalies across various domains and graph types.

C. Gaps in the Existing Literature

The existing scenario of graph-based anomaly detection has advanced significantly, employing machine learning, specifically Graph Convolutional Networks (GCNs), to identify complex relationships and patterns. However, persistent constraints highlight critical gaps in existing literature. Scalability concerns [39] exist in large-scale graph processing, demanding more efficient techniques for real-time anomaly detection. The reliance on domain expertise [1] to perform feature engineering poses challenges, reducing detection accuracy. Existing approaches are mostly focused on static graphs, making it difficult to capture dynamic patterns adequately [27]. Heterogeneous graph structures [4] present modeling and analysis challenges, requiring advanced integration of various data sources. Furthermore, the interpretability [9] of graph-based models, such as GCNs, is still a challenge. These challenges and limitations will be examined in detail in the subsequent section. Addressing these limitations represents a significant gap in current understanding, necessitating the development of novel methodologies to improve scalability, reduce dependability on expertise, manage dynamic graphs effectively, accommodate heterogeneous structures, and enhance model interpretability, establishing the possibility of robust anomaly detection in real-world scenarios.

TABLE I. ANALYSIS OF INCLUDED STUDIES

Reference	Graph Type	Method	Category	Objective Function	Measurement	Outputs
Jiang et al. (2019) [1]	Attribute Graph	Graph Convolutional Networks (GCNs)	Insider Threat, Fraud	Binary Cross-Entropy Loss	Accuracy, Precision, Recall, F1-Score	Anomaly Detection
Ding & Li (2022) [4]	Social Graph	AnoGLA: Graph Link Anomaly Detection	Anomaly Detection	Link Anomaly Detection, Modularity Maximization	AUC-ROC, F1-Score	Link Anomaly Detection
Patel et al. (2020) [5]	Blockchain Transaction Graph	Graph Deep Learning	Anomaly Detection	Reconstruction Error	Precision, Recall, F1-Score	Anomaly Detection
Mesgaran & Hamza (2020) [6]	Attribute Graph	Graph Fairing Convolutional Networks (GFCNs)	Anomaly Detection	Reconstruction Error	Precision, Recall, F1-Score	Anomaly Detection
Liu et al. (2022) [8]	Attributed Graph, Temporal Graph	Data Augmentation for Graph Anomaly Detection (DAGAD)	Anomaly Detection	Reconstruction Loss, Discriminative Loss, Triplet Loss	Precision, Recall, F1-Score	Anomaly Detection
Luo et al. (2022) [9]	Attributed Graph	Community-aware attributed graph anomaly detection (COMGA)	Anomaly Detection	Reconstruction Loss, Discriminative Loss, Entropy Regularization	Precision, Recall, F1-Score	Anomaly Detection
Chen et al. (2022) [11]	Attributed Graph	Graph Contrastive Learning (GCCAD)	Anomaly Detection	Contrastive Loss, Reconstruction Loss	Precision, Recall, F1-Score	Anomaly Detection
Ding et al. (2019) [12]	Attributed Graph	Deep Anomaly Detection on Attributed Networks	Anomaly Detection	Reconstruction Loss	Precision, Recall, F1-Score	Anomaly Detection
Li et al. (2023) [13]	Dual-Domain Graph	Dual-Domain Graph Convolutional Network (DD-GCN)	Insider Threat Detection	Binary Cross-Entropy Loss	Accuracy, Precision, Recall, F1-Score	Anomaly Detection
Wu et al. (2022) [14]	Industrial IoT Graph	Graph Neural Networks (GNNs)	Anomaly Detection	Reconstruction Loss	Accuracy, Precision, Recall, F1-Score	Anomaly Detection
Cao et al. (2022) [15]	Video Graph	Adaptive Graph Convolutional Networks (AGCN)	Anomaly Detection	Reconstruction Loss	Accuracy, Precision, Recall, F1-Score	Anomaly Detection
Ma et al. (2022) [2]	Graph Level	Glocal Knowledge Distillation (GKD)	Anomaly Detection	Graph-Level Reconstruction Loss	Precision, Recall, F1-Score	Anomaly Detection
Zhang et al. (2022) [16]	Graph Level	Dual-Discriminative Graph Neural Network (D2GNN)	Anomaly Detection	Binary Cross-Entropy Loss, Margin Loss	AUC-ROC, Precision, Recall, F1-Score	Anomaly Detection
Huang et al. (2022) [17]	Financial Transaction Graph	Dgraph: Large-Scale Financial Dataset	Anomaly Detection	Reconstruction Loss, Classification Loss	AUC-ROC, Precision, Recall, F1-Score	Anomaly Detection
Wang et al. (2020) [18]	Blockchain-based Healthcare Transaction Graph	Graph Convolutional Network (GCN)	Anomaly Detection	Reconstruction Loss	Accuracy, Precision, Recall, F1-Score	Anomaly Detection
Yuan et al. (2023) [19]	Dynamic Graph	Motif-Level Anomaly Detection	Anomaly Detection	Reconstruction Loss	AUC-ROC, Precision, Recall, F1-Score	Anomaly Detection
Kisanga et al. (2023) [20]	Social Network Graph	Graph Neural Network (GNN)	Anomaly Detection	Reconstruction Loss, Classification Loss	AUC-ROC, Precision, Recall, F1-Score	Anomaly Detection
Cai et al. (2021) [21]	Dynamic Graph	Structural Temporal Graph Neural Network (STGNN)	Anomaly Detection	Reconstruction Loss, Temporal Loss	AUC-ROC, Precision, Recall, F1-Score	Anomaly Detection
Zhong et al. (2019) [22]	Graph Convolutional Networks	Graph Convolutional Label Noise Cleaner (GCLN)	Anomaly Detection	Reconstruction Loss, Classification Loss	Accuracy, Precision, Recall, F1-Score	Anomaly Detection
Zhao et al. (2022) [23]	Graph Pattern Mining	Synergistic Approach for Graph Anomaly Detection	Anomaly Detection	Pattern Mining, Feature Learning	Precision, Recall, F1-Score	Anomaly Detection
Markovitz et al. (2020) [25]	Pose Graph	Graph Embedded Pose Clustering	Anomaly Detection	Pose Clustering	Precision, Recall, F1-Score	Anomaly Detection
Lin et al. (2022) [26]	Air Quality Graph	Graph Neural Networks (GNNs)	Anomaly Detection	Reconstruction Loss	Accuracy, Precision, Recall, F1-Score	Anomaly Detection
Chen et al. (2023) [27]	Video Graph	Spatial-Temporal Graph Attention Network (ST-GAT)	Anomaly Detection	Reconstruction Loss	Accuracy, Precision, Recall, F1-Score	Anomaly Detection
Patel et al. (2022) [28]	Blockchain Transaction	Evolving Graph Deep Neural Network (EvAnGCN)	Anomaly Detection	Reconstruction Loss	Precision, Recall, F1-Score	Anomaly Detection

	Graph					
Pei et al. (2021) [29]	Attributed Graph	Attention-based Deep Residual Modeling (ResGCN)	Anomaly Detection	Reconstruction Loss	Precision, Recall, F1-Score	Anomaly Detection
You et al. (2020) [30]	Attributed Graph	Graph Attention-based Anomaly Detection (Gatae)	Anomaly Detection	Reconstruction Loss	Precision, Recall, F1-Score	Anomaly Detection
Duan et al. (2022) [41]	Graph	Multi-Scale Contrastive Learning Networks (MS-CLN)	Anomaly Detection	Contrastive Loss, Reconstruction Loss	Precision, Recall, F1-Score	Anomaly Detection
Feng et al. (2022) [42]	Graph	Full Graph Autoencoder (FGA)	Anomaly Detection	Reconstruction Loss	Precision, Recall, F1-Score	Anomaly Detection
Akoglu et al. (2015) [31]	Graph	Graph-based	Anomaly Detection	-	Survey	Anomaly detection and description
Bilgin & Yener (2006) [32]	Dynamic Graph	Network Evolution	Dynamic Network	Link Anomaly Detection, Modularity Maximization	Modularity, Clustering Coefficient, Network Evolution Measures	Models, clustering, anomaly detection
Deng & Hooi (2021) [33]	Multivariate Time-series	Graph Neural Networks	Anomaly Detection	Reconstruction Error	Precision, Recall, F1-score, AUC-ROC	Anomaly detection in multivariate time series
Fan et al. (2020) [34]	Heterogeneous Graph	Graph Neural Networks	Illicit Traded Product Detection	Reconstruction Error	Precision, Recall, F1-score, Accuracy	Identification of illicit traded products
Huang et al. (2021) [35]	Temporal Heterogeneous Graph	Information Network Embedding	Heterogeneous Networks	Reconstruction Loss, Discriminative Loss, Triplet Loss	Precision, Recall, F1-Score, Accuracy, Area Under the ROC Curve (AUC-ROC)	Temporal heterogeneous information network embedding
Wang et al. (2021) [36]	Dynamic Graph	Dynamic Hypergraph Convolution	Passenger Flow Prediction	Reconstruction Loss, Discriminative Loss, Entropy Regularization	Mean Absolute Percentage Error (MAPE), Root Mean Square Error (RMSE)	Metro passenger flow prediction
Wang et al. (2019) [37]	Heterogeneous Graph	Graph Attention Network	Heterogeneous Networks	Contrastive Loss, Reconstruction Loss	Precision, Recall, F1-Score, Area Under the ROC Curve (AUC-ROC)	Heterogeneous graph attention network
Zhang et al. (2019) [38]	Heterogeneous Graph	Graph Neural Network	Heterogeneous Networks	Reconstruction Loss	Precision, Recall, F1-Score, Area Under the ROC Curve (AUC-ROC)	Heterogeneous graph neural network
Zhao et al. (2021) [39]	Heterogeneous Graph	Heterogeneous Graph Structure	Graph Neural Networks	Binary Cross-Entropy Loss	Precision, Recall, F1-Score, Area Under the ROC Curve (AUC-ROC)	Heterogeneous graph structure learning
Zhu et al. (2020) [40]	Heterogeneous Mini-Graph	Neural Network	Fraud Invitation Detection	Reconstruction Loss	Precision, Recall, F1-Score, Accuracy, Area Under the ROC Curve (AUC-ROC)	Fraud invitation detection

VII. RESULTS

A. Summary of Reviewed Studied

An overview of the percentage-wise distribution of literature based on the parameters; anomaly detection, graph-based techniques, machine/deep learning, static graphs, dynamic graphs, and graph representation, is presented in the form of a pie chart (see Fig. 4). This comprehensive analysis offers valuable insights into the common practices and trends in the field.

1) Anomaly detection: Anomaly detection is a crucial aspect addressed in all the included studies, indicating its significance in identifying and flagging unusual patterns or events. This aligns with the primary objective of anomaly detection, which is to distinguish abnormal behavior from normal patterns in various domains such as cybersecurity, fraud detection, and system monitoring

2) Graph-based techniques: Graph-based techniques emerge as a prominent approach across the included studies, illustrating their effectiveness in capturing complex relationships and structures within data. These techniques leverage graph representations to model interconnected entities and interactions, enabling the detection of anomalies based on their deviations from the expected graph patterns.

3) Machine/Deep learning: Machine and deep learning methods are predominantly utilized across the literature,

showcasing their ability to handle large volumes of data and extract meaningful patterns. These techniques leverage neural networks and advanced algorithms to learn complex representations and detect anomalies based on the learned patterns.

4) Static graphs: Static graphs, which represent pre-defined structures, are widely employed in the literature to model relationships and dependencies. These static graph representations enable the analysis of anomalies by comparing observed patterns against expected graph structures.

5) Dynamic graphs: In contrast, the adoption of dynamic graphs, which capture time-dependent interactions, is relatively limited in the included literature. Most studies focus on analyzing static relationships rather than temporal variations, leaving an opportunity for future research and development in this area.

6) Graph representation: The inclusion of graph representation is prevalent across the literature, indicating its significance in organizing and structuring data for efficient anomaly detection. Graph representations facilitate the identification of abnormal patterns by capturing the relationships and dependencies among entities in a structured manner.

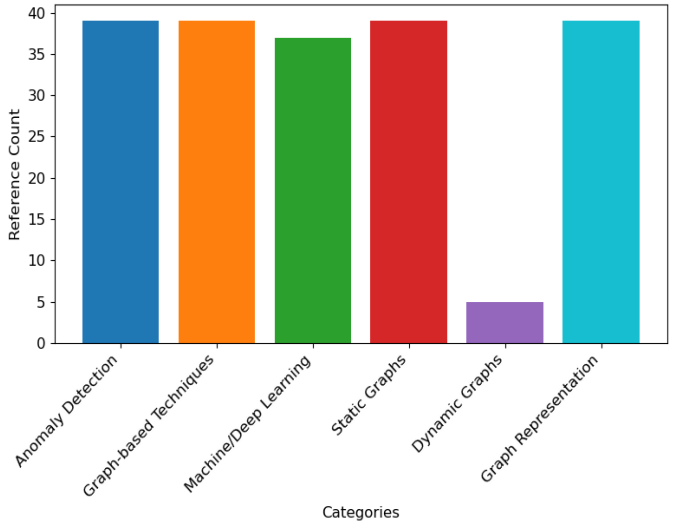

Fig. 4. Distribution of included studies based on given parameters.

B. Publication Trends in Graph-Based Anomaly Detection

The analysis of year-wise publication trends in graph-based anomaly detection, with a focus on Graph Convolutional Networks (GCN), among the included studies since 2019 reveals an interesting pattern as shown in Fig. 5. There has been a steady growth in the number of publications on this topic over the years, indicating the increasing importance and popularity of graph-based anomaly detection techniques. Specifically, since 2019, there has been a surge in research papers incorporating GCNs as a key component in detecting anomalies within graph structures. By the end of 2023, it is expected to surpass the number of publications in the year 2022. This trend suggests that researchers have recognized the power and effectiveness of GCNs in modeling complex relationships and capturing anomalous patterns within graphs. The utilization of GCNs reflects the continuous effort to leverage advanced machine/deep learning techniques to enhance anomaly detection performance in graph-based scenarios. This trend highlights the ongoing interest and active research in the field, with a focus on advancing graph-based anomaly detection methods using GCNs as a key tool.

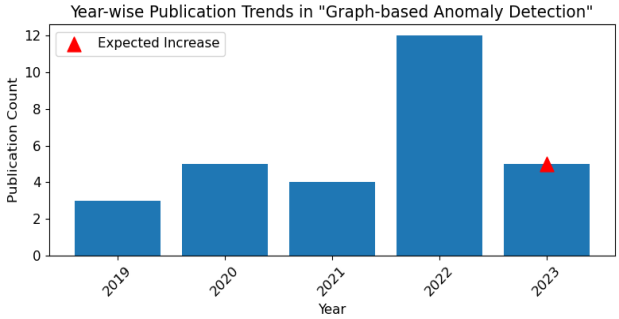

Fig. 5. Year-wise publication trends in graph-based anomaly detection.

VIII. Discussion

A. Key Insights and Observations

Graph-based anomaly detection has seen significant advancements in recent years. Machine learning, particularly deep learning, has emerged as a major approach in graph-based anomaly detection, enabling accurate detection by leveraging neural networks to capture complex relationships and patterns [1] [4]. Graph convolutional networks (GCNs) have been developed to effectively model graph structures and detect anomalies [9]. Graph representations play a crucial role in graph-based anomaly detection, and different approaches utilize various representation techniques [12]. These techniques include adjacency matrices, node features, edge features, or a combination of these [11]. By leveraging these representations, graph-based anomaly detection algorithms can effectively model normal behavior and detect deviations [27]. Graph-based anomaly detection encompasses various techniques, such as centrality-based methods, clustering-based methods, spectral methods, and local anomaly detection methods [32] [27]. Centrality-based methods identify nodes with high centrality measures as potential anomalies [31]. Clustering-based methods group nodes based on similarity and identify anomalies as nodes that do not fit into any cluster [27]. Spectral methods utilize the graph Laplacian matrix to identify anomalous patterns in the eigenvector space [32]. Local anomaly detection methods analyze local patterns and identify anomalies based on their deviation from local structures [11]. While graph-based anomaly detection has shown promise, dynamic graphs pose challenges [27]. Dynamic graphs involve evolving structures, requiring techniques that can handle the temporal dimension and capture evolving patterns [41] [43]. Developing algorithms that can effectively adapt to changing graph structures and identify anomalies in a dynamic setting remains a challenge [27].

Graph-based anomaly detection has witnessed significant advancements through machine/deep learning techniques and the utilization of various graph representations. Different techniques, such as centrality-based, clustering-based,

spectral, and local anomaly detection methods, contribute to the detection of anomalies. However, the challenges posed by dynamic graphs necessitate the development of innovative approaches to handle evolving structures and capture temporal patterns. Further research in this field will contribute to the advancement of graph-based anomaly detection techniques and their application in real-world scenarios.

B. Challenges and Limitations of Graph-Based Approaches

The challenges and limitations of graph-based approaches in anomaly detection include scalability issues, the requirement of domain expertise for manual feature engineering, handling imbalanced datasets, addressing the dynamic nature of graphs, heterogeneity and ensuring interpretability of the models. Overcoming these challenges will enhance the effectiveness and applicability of graph-based anomaly detection techniques in various real-world scenarios.

1) Scalability: One of the challenges in graph-based anomaly detection is the scalability issue when dealing with large-scale graphs [39]. As the size of the graph increases, the computational complexity of graph algorithms grows significantly, making it challenging to detect anomalies efficiently. Efficient algorithms and techniques are required to handle large-scale graphs and maintain real-time anomaly detection.

2) Domain expertise: Another challenge is the requirement of domain expertise and manual feature engineering [1]. Graph-based approaches often rely on feature extraction and selection, which demand expert knowledge and a deep understanding of the underlying graph structure. Manual feature engineering can be time-consuming and may not capture all relevant information, limiting the accuracy of anomaly detection.

3) Imbalanced datasets: Furthermore, graph-based approaches face challenges in handling imbalanced datasets [27]. Anomalies are typically rare events, resulting in imbalanced classes where the number of normal instances outweighs the number of anomalies. Imbalanced datasets can lead to biased models and reduced performance in detecting anomalies. Techniques such as data augmentation, oversampling, or adjusting the anomaly detection threshold are required to address this issue.

4) Dynamic graphs: The dynamic nature of graphs poses another significant challenge [27]. Dynamic graphs involve changing network structures over time, making it essential to develop techniques that can adapt to evolving patterns [43]. Handling temporal dependencies, capturing time-varying behaviors, and maintaining real-time detection in dynamic graphs remain active areas of research [35] [36] [37] [38] [39].

5) Heterogeneity: Heterogeneous graphs pose additional challenges in graph-based anomaly detection [4]. Heterogeneous graphs consist of multiple types of nodes and edges, representing diverse entities and relationships within a system or network. The presence of different node and edge types introduces complexity in modeling and analyzing the graph structure. Heterogeneous graphs often involve diverse data types, such as textual data, numerical attributes, or temporal information associated with different node types. The effective fusion and utilization of these heterogeneous data sources for anomaly detection require careful consideration and feature engineering techniques [37] [38] [39].

6) Interpretability: The interpretability of graph-based approaches is another limitation [9]. Deep learning models, such as graph convolutional networks (GCNs), often act as black boxes, making it challenging to understand the factors contributing to anomaly detection. Interpretability is crucial for building trust in the models and gaining insights into the detected anomalies.

C. Potential Advancements and Future Research Directions

1) Integration of deep learning: The integration of deep learning models has emerged as a promising approach in graph-based anomaly detection, enabling more effective and accurate detection of anomalies in complex graph structures. Several studies in the included literature have explored the integration of deep learning models in this context.

The researchers in [27] highlighted the effectiveness of deep learning models in graph-based anomaly detection. They emphasized that deep learning models, such as Graph Convolutional Networks (GCNs), can capture intricate relationships and patterns in graphs, leading to improved anomaly detection performance. The work carried out in [5] specifically mentioned the use of GCNs in anomaly detection. They highlighted the ability of GCNs to aggregate information from neighboring nodes, enabling the model to capture local graph structures and identify anomalous patterns. The study by [4] also discussed the integration of deep learning models in graph-based anomaly detection. They highlighted the potential of deep learning models, such as autoencoders (AEs) and recurrent neural networks (RNNs), in capturing complex patterns and anomalies in graphs. Moreover, [9] proposed a deep learning-based method for anomaly detection in graphs. They introduced a deep autoencoder model that leverages the expressive power of deep learning to learn robust representations of graph data and detect anomalies based on reconstruction errors. These studies collectively demonstrate the growing interest in leveraging deep learning models, particularly GCNs and autoencoders, for graph-based anomaly detection. The integration of deep learning models provides the capability to effectively capture and analyze complex graph structures, enhancing the detection performance and enabling the detection of subtle anomalies that may be challenging for traditional methods. By harnessing the power of deep learning, these approaches offer the potential to improve the accuracy and scalability of anomaly detection in various domains, including cybersecurity, social networks, biological networks, transportation networks, and other applications where graph-based data is prevalent.

The integration of deep learning models in graph-based anomaly detection represents an exciting research direction that holds promise for future advancements in the field.

2) Dynamic graph analysis: Let $G = (V,E,T)$ be a dynamic graph, where V represents the set of vertices, E represents the set of edges, and T represents the set of timestamps. We aim to detect anomalies in this dynamic graph.

For each timestamp $t \in T$ we denote the graph at time t as $G_t = (V_t, E_t)$, where V_t is the set of vertices at time t and E_t is the set of edges at time t. We assume that the graph evolves over time, and the vertex and edge sets can change at different timestamps. The anomaly detection problem in dynamic graphs can be formulated as finding a function $f : G \rightarrow \{0,1\}$, where $f(G) = 1$ indicates an anomaly in the graph and, $f(G) = 1$ indicates a normal graph. The temporal aspect of the network must be considered, as nodes and edges can appear, disappear, or change over time. Fig. 6 represents a dynamic network with 500 nodes, where each node appears at a different time point. The x and y coordinates of the nodes correspond to their respective node IDs. The color of each node represents its timestamp, with earlier nodes being displayed in cooler colors (e.g., yellow) and later nodes in warmer colors (e.g., red). The graph starts with the first node appearing at time point 0 and gradually increases to the last node appearing at time point 499. The edges between nodes connect consecutive nodes, forming a linear structure. The colorbar on the right side of the plot indicates the mapping between the timestamp values and the corresponding colors. The goal is to design a suitable algorithm or model that can accurately detect anomalies in the dynamic graph based on the evolving vertex [43] and edge sets at different timestamps.

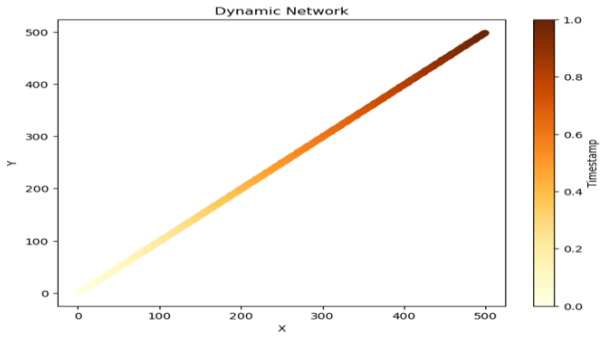

Fig. 6. Graphical representation of a dynamic network where each node appears at a different time point.

The existing research primarily focuses on the detection of anomalies in simple graphs. However, real-world networks are significantly more intricate and exhibit diverse characteristics [24]. These include heterogeneous graphs with multiple node types [38] [39], spatio-temporal graphs that evolve with time [35], and hypergraphs with non-pairwise relations [36]. Detecting and predicting anomalies in such complex graphs pose significant technical challenges [4]. For instance, the dynamic nature of nodes and links in real-world networks means that anomalous entities or relationships can sometimes exhibit normal behaviors similar to other entities in static networks. As a result, the accuracy of anomaly detection methods diminishes [4]. Consequently, key challenges persist in effectively modeling the temporal characteristics of dynamic networks and updating real-time graph embeddings. Additionally, in the context of heterogeneous graph anomaly detection, the incorporation of both attribute and structure information pertaining to various types of nodes and edges into the graph learning model represents an open research problem [11] [27] [37].

Hence, there remains ample scope for further exploration of anomaly detection and prediction on complex graphs as an important avenue for future research highlighting the importance of dynamic graph analysis in understanding and detecting anomalies in evolving systems.

IX. Summary

This systematic literature review focuses on anomaly detection in network data, with a particular emphasis on graph-based approaches, specifically Graph Convolutional Networks (GCNs). The paper discusses the fundamentals of GCNs, including graph representation, graph convolutional operations, and the structure of the graph convolutional layer. The paper also explores the use of GCNs in anomaly detection, discussing the applications of the graph convolutional layer, hierarchical representation learning, and the overall process of anomaly detection using GCNs. To address Research Question 1, a comprehensive review of the relevant literature is presented, comparing various GCN-based approaches. The findings and analysis section summarizes the reviewed studies, highlighting the significance of graph-based techniques, machine/deep learning, static graphs, dynamic graphs, and graph representation in anomaly detection. Further to address Research Question 2, the paper proceeds with a discussion on key insights, challenges, and limitations of graph-based approaches, such as scalability, domain expertise, imbalanced datasets, dynamic graphs, heterogeneity, and interpretability. Finally, to address Research Question 3, potential advancements and future research directions, including the integration of deep learning models and dynamic graph analysis, are identified.

X. Conclusion

This review has provided a comprehensive overview and analysis of anomaly detection in network data, with a focus on graph-based approaches and GCNs. The review of literature highlighted the significance of graph-based techniques, machine/deep learning, and various aspects of graph representation in anomaly detection. The findings suggest that GCNs have shown promising results in detecting anomalies and can effectively capture the complex relationships and patterns present in network data. However, several challenges and limitations, such as scalability, domain expertise, imbalanced datasets, dynamic graphs, heterogeneity, and interpretability, need to be addressed to enhance the practicality and applicability of graph-based approaches. Furthermore, the integration of deep learning models and dynamic graph analysis emerges as potential areas for future research. By leveraging the advancements in deep learning and exploring the temporal dynamics of networks, further improvements can be made in anomaly detection techniques. Overall, this paper provides valuable insights and directions for researchers and practitioners working in the field of anomaly detection, offering a foundation for future studies and advancements in this important area of research.

REFERENCES

[1] J. Jiang et al., "Anomaly detection with graph convolutional networks for insider threat and fraud detection," in MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM), 2019.

[2] R. Ma, G. Pang, L. Chen, and A. van den Hengel, "Deep graph-level anomaly detection by glocal knowledge distillation," in Proceedings of the Fifteenth ACM International Conference on Web Search and Data Mining, 2022.

[3] H. Kim, B. S. Lee, W.-Y. Shin, and S. Lim, "Graph anomaly detection with graph neural networks: Current status and challenges," IEEE Access, vol. 10, pp. 111820–111829, 2022.

[4] Q. Ding and J. Li, "AnoGLA: An efficient scheme to improve network anomaly detection," J. Inf. Secur. Appl., vol. 66, no. 103149, p. 103149, 2022.

[5] V. Patel, L. Pan, and S. Rajasegarar, "Graph deep learning based anomaly detection in ethereum blockchain network," in Network and System Security, Cham: Springer International Publishing, 2020, pp. 132–148.

[6] M. Mesgaran and A. B. Hamza, "Graph fairing convolutional networks for anomaly detection," Pattern Recognit., vol. 145, no. 109960, p. 109960, 2024.

[7] J. Tang, J. Li, Z. Gao, and J. Li, "Rethinking graph Neural Networks for anomaly detection," in International Conference on Machine Learning, 2022.

[8] F. Liu et al., "DAGAD: Data Augmentation for Graph Anomaly Detection," in IEEE International Conference on Data Mining (ICDM), 2022.

[9] X. Luo et al., "Comga: Community-aware attributed graph anomaly detection," in Proceedings of the Fifteenth ACM International Conference on Web Search and Data Mining, 2022, pp. 657–665.

[10] M. D. J. Peters, C. M. Godfrey, H. Khalil, P. Mcinerney, D. Parker, and C. B. Soares, "'Guidance for conducting systematic scoping reviews,''," Int. J. Evidence-Based Healthcare, vol. 13, no. 3, pp. 141–146, 2015.

[11] B. Chen et al., "GCCAD: Graph contrastive learning for anomaly detection," IEEE Transactions on Knowledge and Data Engineering, 2022.

[12] K. Ding, J. Li, R. Bhanushali, and H. Liu, "Deep anomaly detection on attributed networks," in Proceedings of the 2019 SIAM International Conference on Data Mining, Philadelphia, PA: Society for Industrial and Applied Mathematics, 2019, pp. 594–602.

[13] X. Li et al., "A high accuracy and adaptive anomaly detection model with dual-domain graph convolutional network for insider threat detection," IEEE Trans. Inf. Forensics Secur., vol. 18, pp. 1638–1652, 2023.

[14] Y. Wu, H.-N. Dai, and H. Tang, "Graph neural networks for anomaly detection in industrial internet of things," IEEE Internet of Things J., vol. 9, no. 12, pp. 9214–9231, 2022.

[15] C. Cao, X. Zhang, S. Zhang, P. Wang, and Y. Zhang, "Adaptive graph convolutional networks for weakly supervised anomaly detection in videos," IEEE Signal Process. Lett., vol. 29, pp. 2497–2501, 2022.

[16] G. Zhang et al., "Dual-discriminative graph neural network for imbalanced graph-level anomaly detection," Advances in Neural Information Processing Systems, vol. 35, pp. 24144–24157, 2022.

[17] X. Huang et al., "DGraph: A large-scale financial dataset for graph Anomaly Detection," Advances in Neural Information Processing Systems, 2022.

[18] Z. Wang, N. Luo, and P. Zhou, "GuardHealth: Blockchain empowered secure data management and Graph Convolutional Network enabled anomaly detection in smart healthcare," J. Parallel Distrib. Comput., vol. 142, pp. 1–12, 2020.

[19] Z. Yuan, M. Shao, and Q. Yan, "Motif-level Anomaly Detection in Dynamic Graphs," IEEE Transactions on Information Forensics and Security, 2023.

[20] P. Kisanga, I. Woungang, I. Traore, and G. H. S. Carvalho, "Network anomaly detection using a graph neural network," in 2023 International Conference on Computing, Networking and Communications (ICNC), 2023.

[21] L. Cai et al., "Structural temporal graph neural networks for anomaly detection in dynamic graphs," in Proceedings of the 30th ACM International Conference on Information & Knowledge Management, 2021.

[22] J. X. Zhong, N. Li, W. Kong, S. Liu, T. H. Li, and G. Li, "Graph convolutional label noise cleaner: Train a plug-and-play action classifier for anomaly detection," in 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2019.

[23] T. Zhao, T. Jiang, N. Shah, and M. Jiang, "A synergistic approach for graph anomaly detection with pattern mining and feature learning," IEEE Trans. Neural Netw. Learn. Syst., vol. 33, no. 6, pp. 2393–2405, 2022.

[24] J. Ren, F. Xia, I. Lee, A. N. Hoshyar, and C. C. Aggarwal, "Graph learning for anomaly analytics: Algorithms, applications, and challenges," ACM Trans. Intell. Syst. Technol., 2022.

[25] A. Markovitz, G. Sharir, I. Friedman, L. Zelnik-Manor, and S. Avidan, "Graph embedded pose clustering for anomaly detection," in 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2020.

[26] X. Lin, H. Wang, J. Guo, and G. Mei, "A deep learning approach using graph neural networks for anomaly detection in air quality data considering spatiotemporal correlations," IEEE Access, vol. 10, pp. 94074–94088, 2022.

[27] H. Chen, X. Mei, Z. Ma, X. Wu, and Y. Wei, "Spatial–temporal graph attention network for video anomaly detection," Image Vis. Comput., vol. 131, no. 104629, p. 104629, 2023.

[28] V. Patel, S. Rajasegarar, L. Pan, J. Liu, and L. Zhu, "EvAnGCN: Evolving graph deep neural network based anomaly detection in blockchain," in Advanced Data Mining and Applications, Cham: Springer Nature Switzerland, 2022, pp. 444–456.

[29] Y. Pei, T. Huang, W. van Ipenburg, and M. Pechenizkiy, "ResGCN: Attention-based deep residual modeling for anomaly detection on attributed networks," in 2021 IEEE 8th International Conference on Data Science and Advanced Analytics (DSAA), 2021.

[30] Z. You, X. Gan, L. Fu, and Z. Wang, "GATAE: Graph attention-based anomaly detection on attributed networks," in 2020 IEEE/CIC International Conference on Communications in China (ICCC), 2020.

[31] L. Akoglu, H. Tong, and D. Koutra, "Graph based anomaly detection and description: a survey," Data Min. Knowl. Discov., vol. 29, no. 3, pp. 626–688, 2015.

[32] C. Bilgin and B. Yener, "Dynamic network evolution: Models, clustering, anomaly detection," IEEE Networks, 2006

[33] A. Deng and B. Hooi, "Graph neural network-based anomaly detection in multivariate time series," Proc. Conf. AAAI Artif. Intell., vol. 35, no. 5, pp. 4027–4035, 2021.

[34] Y. Fan et al., "Metagraph aggregated heterogeneous graph neural network for illicit traded product identification in underground market," in 2020 IEEE International Conference on Data Mining (ICDM), 2020.

[35] H. Huang, R. Shi, W. Zhou, X. Wang, H. Jin, and X. Fu, "Temporal heterogeneous information network embedding," in Proceedings of the Thirtieth International Joint Conference on Artificial Intelligence, 2021.

[36] J. Wang, Y. Zhang, Y. Wei, Y. Hu, X. Piao, and B. Yin, "Metro passenger flow prediction via dynamic hypergraph convolution networks," IEEE Trans. Intell. Transp. Syst., vol. 22, no. 12, pp. 7891–7903, 2021.

[37] X. Wang et al., "Heterogeneous graph attention network," in The World Wide Web Conference, 2019.

[38] C. Zhang et al., "Heterogeneous graph neural network," In Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery & data mining, pp. 793–803, 2019

[39] J. Zhao, X. Wang, C. Shi, B. Hu, G. Song, and Y. Ye, "Heterogeneous Graph Structure Learning for Graph Neural Networks," Proc. Conf. AAAI Artif. Intell., vol. 35, no. 5, pp. 4697–4705, 2021.

[40] Y. N. Zhu et al., "Heterogeneous mini-graph neural network and its application to fraud invitation detection," in 2020 IEEE International Conference on Data Mining (ICDM), 2020.

[41] J. Duan et al., "Graph anomaly detection via multi-scale contrastive learning networks with augmented view," in Proceedings of the AAAI Conference on Artificial Intelligence, 2022.

[42] Y. Feng, J. Chen, Z. Liu, H. Lv, and J. Wang, "Full graph autoencoder for one-class group anomaly detection of IIoT system," IEEE Internet Things J., vol. 9, no. 21, pp. 21886–21898, 2022.

[43] J. Kim, K. Kim, G. Y. Jeon, and M. M. Sohn, "Temporal Patterns Discovery of Evolving Graphs for Graph Neural Network (GNN)-based Anomaly Detection in Heterogeneous Networks," J. Internet Serv. Inf. Secur, vol. 12, no. 1, pp. 72–82, 2022.

[44] Y. Gao, X. Wang, X. He, Z. Liu, H. Feng, and Y. Zhang, "Addressing heterophily in graph anomaly detection: A perspective of graph spectrum," in Proceedings of the ACM Web Conference 2023, 2023.

[45] J. Bruna, W. Zaremba, A. Szlam, and Y. LeCun, "Spectral networks and locally connected networks on graphs," in 2nd International Conference on Learning Representations (ICLR), 2013.

[46] M. Defferrard, X. Bresson, and P. Vandergheynst, "Convolutional neural networks on graphs with fast localized spectral filtering," Advances in neural information processing systems, 2016.

[47] W. L. Hamilton, R. Ying, and J. Leskovec, "Inductive representation learning on large graphs," Advances in neural information processing systems, 2017.

[48] T. N. Kipf and M. Welling, "Semi-supervised classification with graph convolutional networks.", 2016

[49] Z. Wu, S. Pan, F. Chen, G. Long, C. Zhang, and P. S. Yu, "A comprehensive survey on graph neurasl networks," IEEE Trans. Neural Netw. Learn. Syst., vol. 32, no. 1, pp. 4–24, 2020.