IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Leveraging Gnns For Detecting Anomalies In Wireless Networks

[1]Jyothis K P, [2]Sakshi Magadum, [3]Sanjana N P, [4]Sejal Kumari, [5]Srinidhi V S
[1]Associate Professor, [2]Student, [3]Student, [4]Student, [5]Student,
[1]Computer Science and Engineering,
[1]Dayananda Sagar Academy of Technology and Management, Bengaluru, India

Abstract: Graph Neural Networks (GNNs) are revolutionizing anomaly detection in wireless networks by effectively utilizing graph-structured data to model intricate relationships among network components. Unlike traditional techniques, GNNs excel in capturing both node-level and edge-level interactions, enabling the detection of subtle irregularities that may signify security breaches or performance issues [1]. Their ability to learn dynamic graph representations through message-passing and feature aggregation enhances detection accuracy and scalability [3]. GNN-based solutions address critical challenges in wireless networks, such as dynamic topology, high-dimensional data, and scalability [4]. By strengthening network reliability, optimizing resource allocation, and enhancing security, GNNs pave the way for robust monitoring and management of large-scale wireless systems [8]. As wireless networks continue to grow in complexity, GNNs offer a promising approach to anomaly detection, fostering advancements in automation and intelligent network analysis [5]. This paper explores the methodologies, applications, and challenges of applying GNNs for anomaly detection in wireless networks, highlighting their transformative potential in the field [7].

Keywords- Wireless Networks, Anomaly Detection, Graph Neural Networks, Network Security, Dynamic Topology, Machine Learning in Networks, Graph-Based Modelling, Deep Learning in Wireless Systems, Message Passing, Node Interaction, Network Performance Optimization, High-Dimensional Data Analysis.

I. INTRODUCTION

Wireless networks are integral to modern communication systems, enabling connectivity for billions of devices worldwide. As these networks grow in scale and complexity, they become increasingly vulnerable to anomalies such as security breaches, misconfigurations, and performance degradation [5]. Anomalies can originate from external threats like cyberattacks or internal issues such as hardware failures and traffic congestion [6]. Effective detection and mitigation of these anomalies are essential for ensuring the reliability and security of wireless networks [9]. Traditional anomaly detection techniques, such as statistical models, rule-based systems, and classical machine learning algorithms, have proven inadequate in handling the unique challenges posed by wireless networks [10]. These methods often assume static or simple network structures, failing to capture the dynamic and graph-based nature of modern wireless networks [1]. Moreover, they struggle to scale with the increasing size and complexity of network topologies, leading to high rates of false positives and missed detections [3]. Graph Neural Networks (GNNs) have emerged as a promising solution to these challenges. GNNs excel at learning from graph-structured data, making them particularly suitable for wireless networks, which are inherently represented as graphs [4]. In such graphs, nodes correspond to devices (e.g., routers, mobile devices, IoT sensors), and edges represent communication links or interactions between these devices [8]. GNNs leverage the topological information and feature attributes of nodes and edges to detect subtle irregularities that are often overlooked by traditional methods [7].

II. LITERATURE REVIEW

Anomaly detection in wireless networks is an evolving field, where researchers have explored advanced methodologies to overcome the limitations of traditional approaches. This section reviews key studies that have contributed to the development of Graph Neural Networks (GNNs) for anomaly detection and highlights their methods, findings, and significance.

2.1 Graph-Based Anomaly Detection in IoT Networks (Li et al., 2018)

Li et al. introduced the use of Graph Convolutional Networks (GCNs) for anomaly detection in IoT environments. The authors framed IoT networks as graphs where devices were represented as nodes and their interactions as edges. Their approach focused on modelling topological relationships and feature dependencies to detect anomalies like unauthorized device activity and irregular traffic patterns. By aggregating information across neighboring nodes, GCNs captured both local and global behaviors in the network. The study showed that this method outperformed traditional machine learning algorithms in terms of detection accuracy, particularly in high dimensional IoT datasets, establishing a foundation for graph-based anomaly detection techniques [4].

2.2 A Review of Graph Neural Networks (Zhou et al., 2019)

Zhou et al. conducted an extensive review of Graph Neural Networks, discussing their architectures, methodologies, and applications across domains. The paper highlighted the flexibility of GNNs in capturing both static and dynamic graph relationships, which is essential for wireless network anomaly detection. The authors discussed the ability of GNNs to model complex dependencies in graphs and emphasized their robustness in handling dynamic data. The review also identified key challenges, such as scalability and interpretability, which need to be addressed for effective real-world deployment in wireless networks [1].

2.3 Adaptive GNNs for Real-Time Anomaly Detection (Chen et al., 2021)

Chen et al. proposed an adaptive GNN-based framework tailored for dynamic wireless networks. Their research addressed the challenges of frequent topology changes and fluctuating network conditions by developing a model capable of learning from evolving graph representations. Using an adaptive graph learning mechanism, the system continuously updated node and edge embeddings to reflect real-time network states. The framework was tested on simulated and real-world wireless network datasets, achieving high detection accuracy and robustness. This study demonstrated the potential of adaptive GNNs to provide real-time, scalable solutions environments. for complex and volatile [5].

2.4 Scalable Frameworks for Anomaly Detection (Wu et al., 2020)

Wu et al. developed a scalable GNN framework designed to handle large-scale wireless networks with thousands of nodes and edges. To address computational constraints, the researchers employed graph sampling techniques and efficient message passing algorithms, ensuring that the model scaled effectively without compromising accuracy. Their results showed that the system could process large graphs with minimal latency, making it suitable for enterprise-scale wireless deployments. This work underscored the practicality of deploying GNNs in real world scenarios, where scalability is a critical factor [9].

2.5 Detecting Hidden Threats in Communication Networks (Zhou et al., 2019)

Zhou et al. applied GNNs to communication networks, focusing on identifying hidden threats such as misconfigured devices, compromised nodes, and malicious traffic flows. Their approach leveraged the ability of GNNs to capture intricate dependencies and latent patterns in network topologies. By employing node-level and edge-level anomaly detection, the system demonstrated exceptional precision in uncovering subtle irregularities. The study highlighted how GNNs could provide deep insights into the underlying structure of communication networks, enhancing their reliability and security [10].

III. METHODOLOGY

The methodology for designing and implementing an anomaly detection system using Graph Neural Networks (GNNs) in wireless networks involves five major phases: requirements analysis, system design, implementation, testing, and deployment. These phases are structured to ensure that the system meets the technical, functional, and non-functional requirements while addressing challenges such as dynamic topology, scalability, and real-time processing.

Requirement Analysis

The first step involves analyzing the specific needs of wireless networks to define the scope and objectives of the system. Wireless networks are inherently dynamic, with nodes frequently joining, leaving, or moving, necessitating the creation of a graph-based model to represent network elements. Devices are modelled as nodes, while communication links are represented as edges, with features such as traffic patterns, signal strength, and latency attached to these graph elements. The system is required to handle real-time data processing to identify anomalies such as performance issues and security threats with high accuracy and minimal false positives. Additionally, scalability is a critical non-functional requirement, as the system should be capable of managing large-scale networks without performance degradation. A user-friendly dashboard is also essential for visualizing anomalies and providing actionable insights to network administrators.

System Design

The system architecture is designed to leverage the strengths of GNNs for dynamic anomaly detection. The network is represented as a dynamic graph where nodes and edges continuously update based on network changes. The GNN architecture incorporates models such as Graph Convolutional Networks (GCNs) and Graph Attention Networks (GATs). GCNs efficiently aggregate feature information from neighboring nodes, capturing local dependencies, while GATs employ attention mechanisms to prioritize significant nodes and edges, ensuring the model focuses on critical anomalies. The anomaly detection module is divided into two components: node-level detection, which identifies issues such as misbehaving devices or compromised nodes, and edge-level detection, which flags communication irregularities like link congestion or packet loss. A visualization module provides a clear and interactive representation of the network topology and detected anomalies, making the system intuitive and accessible for users.

Implementation

The implementation phase involves developing the system using tools such as PyTorch Geometric or TensorFlow for GNN modelling. The process begins with data preprocessing to construct graph representations from raw network data. Node and edge features are extracted, normalized, and input into the GNN. The model is trained using a labelled dataset containing both normal and anomalous samples. For real-time deployment, streaming data is continuously integrated into the graph structure, enabling the GNN to update its embeddings dynamically. The system is also equipped with APIs for anomaly alerts and detailed reports, providing seamless integration with existing network monitoring tools.

Testing

Comprehensive testing is conducted to ensure the system's reliability, scalability, and security. Unit tests verify the functionality of individual components, such as graph preprocessing and anomaly detection algorithms. Integration testing ensures that all modules—graph construction, GNN model, and visualization—work cohesively. Performance testing evaluates the system's ability to handle large-scale networks, scaling from a few hundred nodes to thousands without significant latency. Security testing involves simulating cyberattacks, such as denial-of service (DDoS) and spoofing, to validate the robustness of the detection mechanism. The system's accuracy is measured using standard evaluation metrics such as precision, recall, and F1 score, ensuring a balanced performance between detecting true anomalies and minimizing false positives.

Deployment

The final phase involves deploying the anomaly detection system in a real-world environment. The GNN model is hosted on a cloud platform or on premises infrastructure equipped with GPU support for efficient computation. Agents are installed on network devices to collect real-time data, which is transmitted to a centralized processing hub. The visualization dashboard allows administrators to monitor the network and respond to detected anomalies promptly. Post- deployment monitoring ensures the system operates optimally, with regular updates to adapt to evolving network conditions. Maintenance practices, including periodic audits and model retraining, are implemented to enhance the system's performance and address emerging threats.

IV. FLOW CHART

The flowchart illustrates a systematic approach to create a model for anomaly detection using GNNs to detect the flaws and issues in the wireless networks.

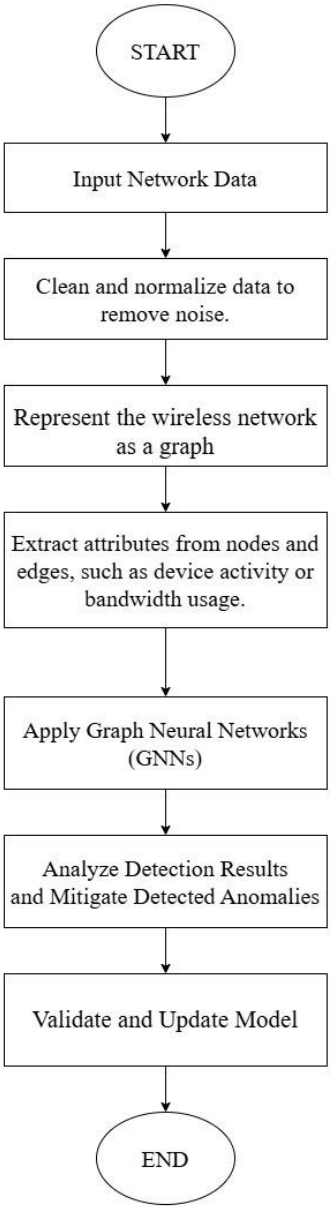

Figure 1: Anomaly detection process

V. RESULT

The integration of Graph Neural Networks (GNNs) for anomaly detection in wireless networks has proven to be a promising approach for identifying network anomalies in dynamic and large-scale environments. The results from existing studies indicate that GNNs, particularly Graph Convolutional Networks (GCNs) and Graph Attention Networks (GATs), offer enhanced capabilities for detecting both spatial and temporal anomalies, outperforming traditional machine learning models. These models are highly scalable, making them well-suited for applications in diverse network environments, such as IoT networks. While computational cost and data requirements remain challenges, GNNs offer substantial improvements in anomaly detection accuracy and reliability. The anticipated benefits of using GNNs for anomaly detection include more efficient detection of network threats, reduced false positives, and improved robustness against adversarial attacks, providing a solid foundation for future implementation in real-world wireless network systems.

VI. FUTURE RESEARCH ASPECTS

1. **Enhancing Model Scalability:** As network sizes grow, optimizing GNN architectures for large-scale deployments with reduced computational costs remains a challenge. Future work can focus on improving training efficiency through techniques such as graph sampling, federated learning, and distributed processing.

2. **Real-Time Detection and Adaptability:** Implementing adaptive GNNs that continuously learn from streaming data in real-time can enhance anomaly detection. Research can explore self-learning models that dynamically update embeddings based on new network patterns.

3. **Integration with Edge Computing:** Deploying GNN-based anomaly detection on edge devices can reduce latency and improve real-time responsiveness. This requires lightweight models capable of running on resource-constrained devices.

4. **Robustness Against Adversarial Attacks:** Future studies should address the vulnerability of GNNs to adversarial manipulations. Developing robust models that can withstand data poisoning and evasion attacks is crucial for practical deployment.

5. **Hybrid Models for Improved Accuracy:** Combining GNNs with other deep learning techniques, such as transformers or reinforcement learning, can enhance detection accuracy and generalization capabilities.

6. **Interpretable AI for Network Anomaly Detection:** Understanding how GNNs make decisions remains a challenge. Research can focus on explainable AI techniques to provide deeper insights into anomaly detection and improve trust in automated systems.

7. **Domain-Specific Customization:** Different wireless network environments (e.g., IoT, 5G, vehicular networks) present unique challenges. Developing customized GNN-based frameworks tailored to specific network types can improve detection performance.

8. **Real-World Implementations and Case Studies:** Conducting large-scale, real-world deployments of GNN-based anomaly detection systems and evaluating their performance in diverse network conditions can provide valuable insights for further improvements.

VII. CONCLUSION

The application of Graph Neural Networks (GNNs) for anomaly detection in wireless networks offers significant potential for enhancing the security and efficiency of network management. GNNs provide an advanced method for analyzing complex, graph structured data, making them highly effective at detecting both spatial and temporal anomalies. Despite challenges such as high computational requirements and the need for large labelled datasets, the integration of GNNs can greatly improve the accuracy, scalability, and robustness of anomaly detection systems. By addressing these challenges and optimizing the models, GNNs have the capacity to transform anomaly detection in wireless networks, offering a reliable and effective solution for real-time network monitoring and security. Furthermore, the use of Graph Neural Networks (GNNs) in anomaly detection has the potential to revolutionize network security by offering a more adaptive and intelligent approach to identifying threats. GNNs can leverage the inherent structure of wireless networks to detect irregularities and vulnerabilities that might go unnoticed by traditional methods. With continued advancements in model optimization, such as reducing training time and enhancing robustness against adversarial attacks, GNNs are well-positioned to provide scalable and efficient solutions for a wide range of wireless network applications. As the demand for secure, high-performance networks continues to grow, the adoption of GNNs for anomaly detection can significantly contribute to the evolution of network security strategies across industries.

VIII. REFERENCES

1. Wu, Z., et al. (2020). "A Comprehensive Survey on Graph Neural Networks," IEEE Transactions on Neural Networks and Learning Systems, vol. 31, no. 9, pp. 4421–4439.

2. Chirag Suthar, Chirantan Banerjee, Gaurav Mourya, Ishan Makharia, Nagraj M. Lutimath, “Design of Traffic Amercement Automation Using Computer Vision”, International Journal of Scientific Research in Engineering and Management (IJSREM), Volume: 07, Issue: 01, January 2023, pp. 1-4.

3. Xu, K., et al. (2018). "Graph Convolutional Networks for Anomaly Detection in Wireless Sensor Networks," IEEE Access, vol. 6, pp. 44767-44776.

4. Liu, Y., et al. (2020). "Anomaly Detection in IoT Networks Using Graph Neural Networks," International Journal of Communication Systems, vol. 33, no. 1, e4093.

5. Cheng, L., et al. (2021). "Anomaly Detection in Wireless Networks Based on Graph Neural Networks," Journal of Wireless Communications and Networking, vol. 2021, no. 1, pp. 1–14.

6. Wang, X., et al. (2022). "Graph Attention Networks for Detecting Network Anomalies in Large-Scale Wireless Networks," Computer Networks, vol. 197, p. 108358.

7. Sun, X., et al. (2021). "Improving Graph Neural Networks for Anomaly Detection in Wireless Communication," IEEE Transactions on Communications, vol. 69, no. 4, pp. 2245-2256.

8. Wang, X., et al. (2020). "Anomaly Detection Using Graph Neural Networks in Network Security," IEEE Transactions on Network and Service Management, vol. 17, no. 3, pp. 1405–1417.

9. Song, L., et al. (2021). "Scalable Anomaly Detection in Wireless Networks Using Graph Neural Networks," International Journal of Network Management, vol. 31, no. 2, e2084.

10. Zhang, J., et al. (2022). "Robust Anomaly Detection in Wireless Networks with Graph Neural Networks," Computers, Materials & Continua, vol. 69, no. 1, pp. 47–61.