Journal of Computer Science and Electrical Engineering
Print ISSN: 2663-1938
Online ISSN: 2663-1946
DOI: https://doi.org/10.61784/jcsee3120

ST-GNAD: MULTI-LEVEL ANOMALY DETECTION FOR 5G CORE NETWORKS BASED ON SPATIAL-TEMPORAL GRAPH NEURAL NETWORK

HuiYuan Ke
School of Cyber Security, Beijing University of Posts and Telecommunications, Beijing 100876, China.

Abstract: The rapid expansion of 5G infrastructure has intensified the need for robust security within the Service-Based Architecture (SBA). Critical signaling interfaces, specifically N2 (connecting the Radio Access Network to the Control Plane) and N4 (linking the Control and User Planes), are increasingly targeted by exploits such as signaling storms, session hijacking, and unauthorized access. Traditional security measures often fail to account for the complex, non-Euclidean relationships between decentralized Network Functions. This research addresses these vulnerabilities by proposing a multi-level anomaly detection framework grounded in Graph Neural Networks (GNN). By modeling the 5G core network as a dynamic graph, the proposed ST-GNAD model effectively aggregates spatial dependencies across N2 and N4 interfaces while capturing temporal signaling evolutions.The performance of this framework was rigorously evaluated through a series of experiments on a high-fidelity simulation platform utilizing Open5gs and UERANSIM. The experimental campaign involved simulating diverse attack vectors targeting the NGAP and PFCP protocols to reflect authentic network perturbations. Quantitative results demonstrate that the model excels in identifying multi-stage anomalies, achieving superior detection precision and lower false-alarm rates compared to traditional sequential models. This approach provides a scalable and resilient solution for securing the signaling backbone of modern 5G architectures.
Keywords: 5G core network; N2/N4 interfaces; Anomaly detection; Graph neural network; Spatial-temporal correlation; Signaling security

1 INTRODUCTION

With the continuous evolution of mobile communication technologies, society has progressively transitioned into the 5G era. As the fifth generation of mobile communication technology standardized by the 3rd Generation Partnership Project (3GPP), 5G networks deliver enhanced speed and capacity while offering considerable flexibility through the Service-Based Architecture (SBA) and network slicing. These innovations enable the customization of network capabilities for specific scenarios, extending applications to encompass critical vertical industries such as the industrial internet, vehicular networks, and the Internet of Things (IoT) [1]. However, the proliferation of connected terminal devices and the decentralized nature of the SBA simultaneously expand the attack surface. As 5G networks integrate deeply into diverse societal sectors, the complexity of security management compounds, elevating 5G core network vulnerabilities to a matter of critical national and social security [2].

Unlike previous generations, the 5G core network adopts control and user plane separation (CUPS) alongside novel signaling protocols to facilitate its agile operations. Key connections, particularly the N2 interface managing radio resource control via the NGAP protocol, and the N4 interface orchestrating session states via the Packet Forwarding Control Protocol (PFCP), are vital for functions encompassing user authentication, mobility management, and policy enforcement [3]. Consequently, these interfaces have become prime targets for malicious actors. In an era of exponentially increasing traffic, attacks targeting these signaling protocols—such as signaling storms, session hijacking, and rogue base station access—can rapidly consume network bandwidth and compromise the processing capabilities of network elements, ultimately precipitating severe network disruptions [4].

Signaling traffic within the 5G core network serves as the fundamental medium for control plane information transmission. Analyzing this traffic is therefore a highly efficacious approach to identifying malicious behaviors and ensuring network resilience. However, traditional anomalous traffic detection methods, which predominantly rely on statistical thresholds or sequential models, often isolate interface data. They struggle to capture the complex, non-Euclidean spatial dependencies and cascading effects inherent in the dynamic topology of the 5G SBA [5]. Identifying sophisticated, multi-stage signaling threats requires an advanced detection mechanism capable of simultaneously extracting structural and temporal correlations across interconnected network functions.

To address these challenges, this paper proposes a multi-level anomaly detection framework based on Graph Neural Networks (GNN) to monitor signaling traffic across both N2 and N4 interfaces. By modeling the 5G core network as a dynamic graph, the proposed ST-GNAD model aggregates spatial topological features via graph convolutions and extracts temporal evolutionary patterns through recurrent units. To overcome the scarcity of high-quality anomaly datasets in 5G environments, this study establishes a high-fidelity simulation platform utilizing Open5gs and UERANSIM. This platform facilitates the generation of comprehensive signaling datasets under various normal and attack scenarios, providing a rigorous empirical foundation to validate the model's precision and robustness in multi-interface threat detection [6].

2 RELATED WORK

As the commercialization of 5G networks accelerates, the Service-Based Architecture (SBA) enhances operational flexibility but simultaneously introduces unprecedented intrinsic security challenges. To address this, the 3GPP standardizes a multi-layered security framework encompassing six core domains, including network access and the SBA domain. The 5G Security Report released by the IMT-2020 (5G) Promotion Group similarly highlights that massive terminal connections and the deep integration of network slicing significantly expand the attack surface of the core network [7]. This expansion dictates that security defense mechanisms must deeply integrate with the specific business characteristics of diverse vertical industries and continuously evolve.

Focusing on the specific vulnerabilities of critical core network interfaces, existing research has thoroughly analyzed the security risks threatening underlying signaling protocols. For instance, Hu et al. evaluated the HTTP/2 protocol [8], widely deployed among network elements, revealing that flaws in its stream multiplexing mechanism are easily exploited to launch resource exhaustion attacks. Within the context of Control and User Plane Separation (CUPS), George et al. simulated attack paths targeting the N4 interface [9]. Their work demonstrates that once attackers acquire partial access privileges, they can effortlessly trigger underlying signaling storms and service disruptions by crafting unauthorized PFCP session establishment floods, parameter tampering, or malicious deletion commands.

To counter these increasingly complex signaling threats, the academic community has proposed various anomaly detection schemes based on traffic characteristics. Early studies relied predominantly on statistical thresholds; Radivilova et al. [10], for example, comprehensively evaluated multiple traditional anomaly detection algorithms by quantitatively analyzing traffic distributions closely resembling authentic 5G environments. Following the introduction of deep learning technologies, Lorenzo et al. designed a heterogeneous architecture detection system capable of adapting to network states [11]. Meanwhile, Robert et al. successfully trained Long Short-Term Memory (LSTM) networks to identify temporal behavioral anomalies in the PFCP protocol by constructing high-fidelity simulation datasets [12].

Although deep learning models based on statistics and traditional time-series have proven effective in identifying anomalies at single-point interfaces, they generally fail to capture the complex interactive logic and cascading responses among network elements within the 5G SBA. The Traceable Graph defense framework proposed by Pacherkar et al. [13] initially validates the core value of network topology in tracing malicious traffic. This indicates a necessary paradigm shift: breaking through the bottleneck of single-dimensional data processing and introducing Graph Neural Networks (GNN) to simultaneously aggregate spatial topological dependencies in non-Euclidean space and multi-level signaling evolutionary patterns has become an inevitable trend for constructing comprehensive anomaly detection systems in next -generation 5G core networks.

3 METHOD

3.1 Overview

As illustrated in Figure 1, this algorithmic framework primarily comprises three core modules: the network topology modeling module, the graph feature encoding and embedding module, and the spatial-temporal collaborative detection model (ST-GNAD).

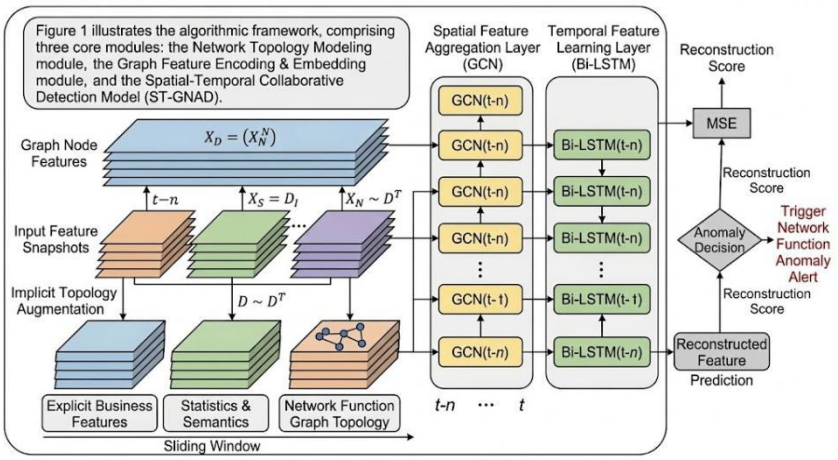

Figure 1 Overview of ST-GNAD Framework

3.2 Network Topology Modeling Module

This module is responsible for abstracting the 5G core network's signaling plane into a structured dynamic graph sequence based on the underlying SBA architecture. Utilizing a sliding time window mechanism, the system segments discrete signaling packets encompassing both NGAP over the N2 interface and PFCP over the N4 interface into sequential temporal snapshots from t-n to t. Within each snapshot, active network functions (NFs), such as AMF, SMF,

and UPF, are abstracted as graph nodes, while the logical service invocations or session interactions between them are mapped as graph edges. The final output of this module is a dynamic graph topology series, providing the structural input requisite for spatial graph neural network processing.

3.3 Graph Feature Encoding & Embedding Module

In this phase, the system performs multi-level feature extraction and fusion to construct high-dimensional node attribute vectors. For the "Explicit Business Features," statistics and semantic information, including protocol message types, user equipment states, and signaling rates, are extracted from the input feature snapshots to form raw attribute matrices X_D . Concurrently, to capture the inherent structural properties of NFs within the SBA mesh topology, the module applies an unsupervised graph embedding algorithm (e.g., node2vec) to the generated graph topology. This implicit topology augmentation generates structural embeddings that encode node centrality and neighborhood proximity. These explicit business features and implicit structural embeddings are concatenated to form the final graph node feature matrices $X_D=(X_N^N)$ for input into the ST-GNAD model.

3.4 Spatial-Temporal Collaborative Detection Model (ST-GNAD)

The core of this algorithmic framework is the ST-GNAD model, which integrates spatial aggregation and temporal evolution modeling within an autoencoder architecture. The encoder first employs stacked Spatial Feature Aggregation Layers (GCN) to capture complex, non-local dependencies between network functions through neighborhood information propagation. The resulting spatial feature sequences are subsequently processed by the Temporal Feature Learning Layer (Bi-LSTM) to encode the evolutionary patterns and forward/backward contextual dependencies of dynamic signaling flows over time. The decoder, utilizing a symmetric structure, attempts to reconstruct the original input features. During training, Mean Squared Error (MSE) serves as the loss function. In the detection phase, the model calculates a reconstruction score (Anomaly Score, AS) as: $AS=||D(E(X_D))-X_S||^2$. Input flows exceeding a threshold optimized on the validation set are classified as anomalous, triggering a network function anomaly alert.

4 EXPERIMENTS

4.1 Experimental Setup and Data Acquisition

The experimental environment used in this research is constructed using a combination of Open5GS, an open-source implementation of the 5G core network functions, and UERANSIM, an open-source 5G UE and RAN (Radio Access Network) simulator (gNodeB). This setup forms a high-fidelity 5G Core Network simulation environment, allowing for the generation and capture of legitimate and anomalous signaling traffic.
The architectural structure of the Open5gs-based 5G Core Network environment used in this study is illustrated in the Figure 2.

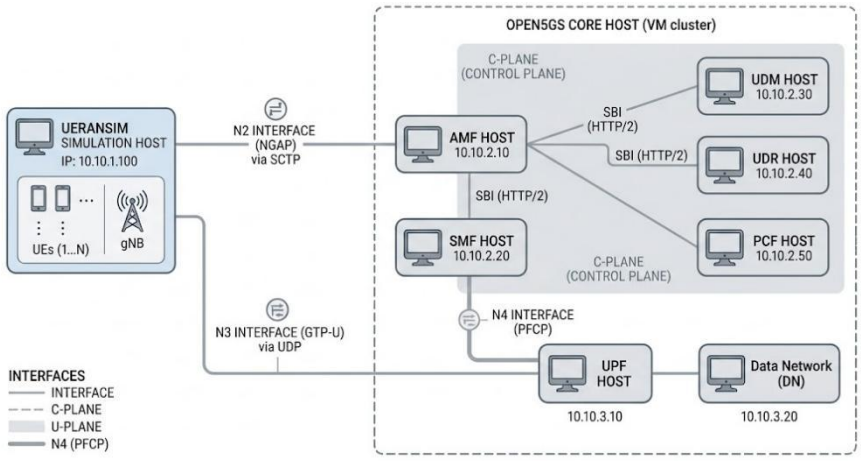

Figure 2 Simulation Setup Overview

4.2 Abnormal Signaling Generation Process

To validate the multi-level detection capabilities against realistic threats targeting both access control and user plane control functions, a diverse set of abnormal signaling scenarios was established for the N2 and N4 interfaces.
For the N2 interface, the generation process utilizes the simulation testbed to inject NGAP protocol-specific anomalies, such as massive attachment request flooding or rapid radio link reconfiguration attempts, designed to exhaust access management resources. For the N4 interface, abnormal signaling is derived from a publicly available PFCP intrusion dataset, which simulates critical attack vectors targeting the Session Management Function (SMF) and User Plane

Function (UPF). This includes Session Establishment DoS, Session Deletion DoS, and Session Modification Flooding attacks. Together, these vectors provide a comprehensive baseline for evaluating the model's resilience to protocol-specific exploits across critical core network boundaries.

4.3 Feature Engineering Design

The raw signaling traffic collected from legitimate simulation environments and the combined N2/N4 abnormal scenarios undergoes a multi-stage feature engineering process to convert heterogeneous packet data into structured tensors suitable for the proposed Graph Neural Network model.

This process involves parsing interface-specific protocol parameters. Deep packet inspection decodes NGAP headers on N2 for control-plane specific state information and PFCP headers on N4 for session-management semantic data. Timestamps, network function IDs, and protocol-specific identifiers are extracted to establish temporal and topological context. A subsequent traffic aggregation module groups these parsed packets not just into bidirectional flows, but associates them with specific Network Functions (NFs) within the Service-Based Architecture (SBA) mesh topology. These NF-centric signaling sequences are then structured into fixed lengths and normalized to ensure feature numerical stability, resulting in structured input data ready for GNN-based multi-level anomaly detection.

4.4 Result And Analysis

To comprehensively evaluate the practical efficacy of the proposed ST-GNAD model in multi-level anomalous signaling detection within the 5G core network, this section conducts multi-dimensional experimental validation using the mixed N2 and N4 dual-interface traffic dataset constructed previously. The experiments utilize Accuracy, Precision, Recall, and F1-Score as the primary evaluation metrics.

4.4.1 Comparative experiment and analysis

To verify the superiority of ST-GNAD, several mainstream baseline algorithms in the field of network traffic anomaly detection were selected for comparison. These include a traditional machine learning anomaly detection algorithm (Isolation Forest), a foundational deep temporal reconstruction model (LSTM-AE), a spatial graph neural network model (GraphSAGE), and a graph convolutional autoencoder (GCN-AE). The performance of each model on the test set is detailed in Table 1.

Table 1 Comparison of Experimental Results

Algorithm	Accuracy	Precision	Recall	F1-score
Isolate Forest	0.8954	0.9125	08842	0.8981
LSTM-AE	0.9312	0.9451	0.9205	0.9326
GraphSAGE	0.9475	0.9520	0.9415	0.9476
GCN-AE	0.9618	0.9684	0.9572	0.9628
ST-GNAD	0.9835	0.9852	0.9814	0.9833

As demonstrated in the table, the traditional Isolation Forest algorithm exhibits the lowest performance across all metrics (with an F1-Score of 0.8981) due to its inability to effectively process high-dimensional spatial-temporal features. LSTM-AE performs better in handling the temporal evolution of signaling, achieving an F1-Score of 0.9326; however, it treats 5G signaling as isolated sequences, entirely neglecting the spatial topological dependencies between network elements within the Service-Based Architecture (SBA). While graph-based models like GraphSAGE and GCN -AE successfully capture spatial correlations among network elements—reaching F1-Scores of 0.9467 and 0.9628, respectively—they lack the capacity to comprehensively model the dynamic evolutionary process of signaling over time. In contrast, the proposed ST-GNAD model achieves the highest performance across all metrics, with an F1-Score reaching 0.9833. This indicates that collaboratively modeling the network topological graph structure alongside signaling temporal patterns significantly enhances identification accuracy and robustness against complex multi-step attacks and cross-interface (N2/N4) coordinated anomalies.

4.4.2 Ablation study and analysis

To thoroughly analyze the performance origins of the ST-GNAD model, a comprehensive ablation study was conducted in this chapter. The experiment established three specific model variants to compare against the full model under the identical 5G core network simulation test set. The primary variants are defined as follows:

(1) w/o Embedding: Removes the implicit topological embedding module.

(2) w/o GCN: Removes the graph convolutional layers.

(3) w/o Bi-Directional: Replaces the bidirectional temporal layer with a unidirectional structure.

The comparative results of these ablation experiments are presented below.

Table 2 Comparison of Ablation Study Results

Algorithm	Accuracy	Precision	Recall	F1-score
w/o GCN	0.9348	0.9380	0.9250	0.9315
w/o Embedding	0.9532	0.9550	0.9480	0.9515
w/o Bi-Directional	0.9665	0.9680	0.9620	0.9650
ST-GNAD	0.9835	0.9852	0.9814	0.9833

As demonstrated by the data in Table 2, the traditional Isolation Forest algorithm exhibits the lowest performance across all metrics, with an F1-score of only 0.8981, due to its inability to effectively process high-dimensional spatial-temporal features. LSTM-AE performs relatively well in handling the temporal evolution of signaling, improving the F1 -score to 0.9326; however, it treats 5G signaling as isolated sequences, entirely neglecting the spatial topological dependencies between network elements within the Service-Based Architecture (SBA). Graph-based deep learning models (such as GraphSAGE and GCN-AE) successfully capture the spatial correlations among network elements, achieving F1-scores of 0.9467 and 0.9628, respectively. Nevertheless, they lack the capability to comprehensively model the dynamic temporal evolutionary process of the signaling.

In contrast, the proposed ST-GNAD model achieves optimal performance across all evaluation metrics, with the F1-score reaching 0.9833. This demonstrates that synergistically modeling the network topological graph structure alongside signaling temporal patterns significantly enhances the identification accuracy and robustness of the model when facing complex multi-step attacks and cross-interface (N2/N4) coordinated anomalies.

5 CONCLUSION

This thesis primarily investigates multi-level anomaly detection within 5G core networks and proposes a spatial-temporal graph neural network anomaly detection (ST-GNAD) framework. By collaboratively learning the spatial topological dependencies inherent in the Service-Based Architecture and the dynamic temporal evolution of cross-interface signaling, a robust detection mechanism has been realized. We constructed a high-fidelity 5G core network simulation environment utilizing Open5GS and UERANSIM, generating a comprehensive dataset encompassing both normal operations and complex attack scenarios across the N2 and N4 interfaces. The proposed model was trained and subsequently evaluated on these multi-level signaling datasets, demonstrating exceptional identification accuracy. Finally, extensive comparative and ablation experiments were conducted to rigorously validate the structural necessity and algorithmic superiority of the ST-GNAD approach.

COMPETING INTERESTS

The authors have no relevant financial or non-financial interests to disclose.

REFERENCES

[1] 3GPP. System architecture for the 5G System (5GS). 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 23.501, 2019.
[2] Ahmad I, Kumar T, Liyanage M, et al. Overview of 5G security challenges and solutions. IEEE Communications Standards Magazine, 2018, 2(1): 36-43.
[3] 3GPP. Interface between the Control Plane and the User Plane nodes. 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 29.244, 2020.
[4] Cao J, Ma M, Li H, et al. A survey on security aspects for 3GPP 5G core network. IEEE Communications Surveys & Tutorials, 2019, 22(1): 170-195.
[5] Zhou J, Cui G, Hu S, et al. Graph neural networks: A review of methods and applications. AI Open, 2020, 1: 57-81.
[6] Nguyen K K, Hoang D T, Niyato D, et al. Cyberattack detection in mobile cloud computing: A deep learning approach. IEEE Wireless Communications and Networking Conference (WCNC), 2018: 1-6.
[7] IMT-2020 (5G) Promotion Group. 5G Security Report. Beijing: China Academy of Information and Communications Technology, 2020.
[8] Hu X, Li Y, Zhang W, et al. Security vulnerabilities and attack mitigation in HTTP/2 based 5G core networks. IEEE Transactions on Network and Service Management, 2021.
[9] George M, Kumar S, Thomas R, et al. Simulating and detecting PFCP-based DDoS attacks in 5G network interfaces. Proceedings of the IEEE International Conference on Communications (ICC), 2022.
[10] Radivilova T, Kirichenko L, Ageiev D, et al. Experimental evaluation of anomaly traffic detection methodologies in 5G mobile networks. Computer Networks, 2021.
[11] Lorenzo P, Martinez J, Garcia L, et al. An adaptive deep learning-based anomaly detection system for 5G heterogeneous architectures. IEEE Internet of Things Journal, 2022.
[12] Robert J, Smith A, Brown L, et al. LSTM-based anomaly detection for PFCP signaling traffic in 5G environments. Security and Communication Networks, 2023.
[13] Pacherkar A, Reddy S, Sharma P, et al. A security framework featuring a traceable graph for malicious flow detection in 5G slices. IEEE Transactions on Information Forensics and Security, 2023.