PASD-5GC: A Process-Based Approach for Anomalous Signaling Detection in 5G Core Network

Cong Li[†‡], Yuhan Cao[†], Xingxing Liao[‡*], Zilong Wang[†‡], Wei You[¶], Xinsheng Ji[¶*]
[†] *School of Cyber Engineering, Xidian University, Xi'an, China*
[‡] *Purple Mountain Laboratories, China*
[¶] *Information Engineering University, Zhengzhou, China*
licong55@126.com, yhcao5819@163.com, liaoxingxing@pmlabs.com.cn
zlwang@xidian.edu.cn, youwei1102@163.com, jixs@pmlabs.com.cn
[*]Corresponding Author: liaoxingxing@pmlabs.com.cn, jixs@pmlabs.com.cn

***Abstract*—The rapid evolution of 5G technology has driven the expansion of user-plane services, with the N4 interface playing a crucial role in managing signaling interactions between the control plane and the user plane. However, the architectural openness of the 5G Core Network (5GC) and the N4 interface's dependency on the Packet Forwarding Control Protocol (PFCP) expand anomalous signaling attack surfaces. Existing anomaly detection approaches for 5GC N4 interfaces focus on packet-level features while overlooking contextual process information, resulting in constrained detection effectiveness. This paper proposes a Process-based Anomalous Signaling Detection approach (PASD-5GC) that integrates PFCP business logic with behavioral patterns. The core model of PASD-5GC, termed DM-Net, is designed to capture both local and global features of signaling sequences. Extensive experiments demonstrated that, compared to existing methods, PASD-5GC achieves up to a 34% improvement in abnormal signaling detection accuracy, validating the effectiveness and superiority of the proposed approach.**

***Index Terms*—5G Core Network, N4 Interface, Anomaly Detection, PFCP Session Process**

I. Introduction

With the rapid advancement of Fifth Generation Mobile Communication Technology (5G), the growing demand for massive data access and large-scale connectivity among users, machines, and devices imposes increasingly stringent requirements on network performance. As the data plane of the 5G core network, the User Plane Function (UPF) is strategically deployed at the network edge, in closer proximity to end-users. This deployment facilitates rapid data forwarding, efficient traffic scheduling, and robust user-plane session management, thereby delivering a high-performance, low-latency, and high-bandwidth telecommunications-grade service environment to users.

The N4 interface, the signaling transmission channel for the User Plane Function (UPF), handles a substantial volume of service data. Its inherent openness renders it vulnerable to illicit signaling attacks. In the data plane, signaling acts as the primary data carrier, facilitating the conveyance of control information, including resource allocation, data transmission, connection management, and session management. In the context of the N4 interface, the Packet Forwarding Control Protocol (PFCP) is employed to enable signaling interactions among various network elements associated with the UPF. PFCP operates over the User Datagram Protocol (UDP), which lacks built-in mechanisms for connection establishment, flow control, and error correction. This UDP-based transport mechanism makes PFCP signaling packets susceptible to forgery, as attackers can exploit the absence of authentication by simply guessing the correct Session Endpoint Identifier (SEID), as illustrated in Fig. 1. By transmitting a falsified PFCP session deletion or modification request, the attacker can induce the UPF to erroneously delete or alter the PFCP session linked to a specific User Equipment (UE). Such attacks can lead to large-scale service disruptions or information leakage, severely impacting UE communication and threatening the stability and security of 5G networks.

Researchers have proposed various solutions to mitigate the risk of anomalous signaling attacks on core network service interfaces. Prominent approaches include enhancing the architecture of the 5G core network, implementing robust authentication mechanisms, and developing advanced anomaly detection systems. For instance, Manan et al. [1] advocated for integrating additional Network Functions (NFs) into the 5G core network to facilitate zero-trust access control, thereby enhancing the security of 5G network interfaces. Haddad

This work is supported by the National Key Research and Development Program of China under Grant No. 2022YFB2902204 and Grant No. 2022YFB2902205.

ISBN 978-3-903176-72-0 © 2025 IFIP

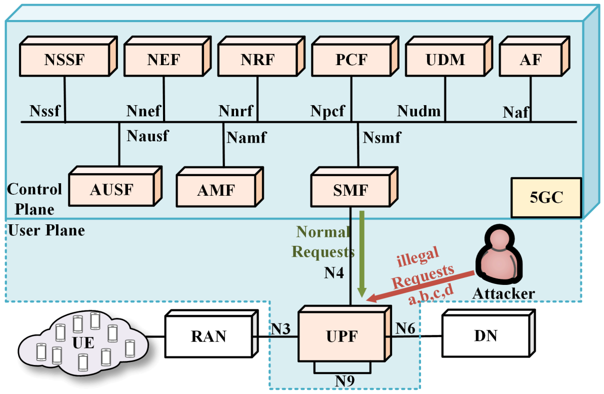


Fig. 1: PFCP signaling attack scenario, where *a* denotes PFCP Session Deletion Attack, *b* denotes PFCP Session Establishment Flooding Attack, *c* denotes PFCP Session Modification Attack (DROP), and *d* denotes PFCP Session Modification Attack (DUPL).

et al. [2] introduced a blockchain-based authentication scheme to ensure secure interface connections within 5G networks. However, these solutions often involve substantial deployment costs and complex network management requirements, potentially leading to compatibility issues and service disruptions, particularly in large-scale 5G deployments. In contrast, Radoglou-Grammatikis et al. [3] proposed a 5G core network intrusion detection system, 5GCIDS, which employs machine learning and deep learning techniques to detect anomalous signaling attacks at the N4 interface. This flow-based anomaly detection system effectively characterizes signaling behavior patterns and identifies anomalies, representing a significant advancement in N4 interface security. Nevertheless, further research is required to evaluate the system's adaptability and effectiveness in detecting anomalous signaling attacks, specifically within the 5G core network user plane.

The N4 interface is integral to the forwarding and processing of large-scale user-facing services, necessitating strict compliance with standardized business process protocols. Existing anomaly detection methods primarily focus on identifying anomalies at the packet level or as isolated events, often neglecting the contextual information embedded within business processes and standardized signaling interactions. This limitation leads to missed detections and false positives, particularly when addressing complex temporal anomalies and disguised anomalous behaviors, ultimately reducing detection accuracy. Consequently, effectively integrating business process information into anomaly detection frameworks remains a critical challenge. Addressing this issue is essential for enhancing the security of the N4 interface within the 5G core network and ensuring robust anomaly detection in an increasingly complex 5G environment.

The anomaly detection mechanism based on PFCP process features effectively captures complex data correlations and causal relationships that are challenging to detect using conventional methods. As process information inherently represents global contextual data, its modeling must adhere strictly to 3GPP standards to ensure the accuracy and consistency of signaling interactions. By comprehensively modeling PFCP signaling flows at the N4 interface, the behavioral patterns of session management can be fully characterized. Consequently, the mechanism identifies anomalies within individual packets. It detects inconsistencies in multi-step signaling interactions, such as logical conflicts induced by masquerade attacks or abnormal deviations in signaling execution sequences. These capabilities enhance the accuracy and reliability of anomaly detection, ensuring adaptability to the complex signaling dynamics of evolving network environments.

The main contributions of this paper are summarized as follows:

1) A novel anomaly detection mechanism for the N4 interface was proposed, integrating PFCP protocol processes with behavioral patterns, significantly enhancing detection accuracy over existing frameworks.
2) Proposed the DM-Net model, which integrates dilated convolution and a multi-head attention mechanism. This model effectively captures local and global features of sequential data, enabling precise identification of anomalous signaling and improving overall network anomaly detection accuracy.
3) The proposed approach was evaluated on the N4 interface PFCP intrusion dataset. Extensive experiments and comparative analyses showed that the process-based anomalous signaling detection mechanism outperformed conventional methods, achieving superior detection performance.

II. Related Works

Numerous studies have investigated anomaly signaling detection in the 5G core network environment. Some of these studies collect packet capture (pcap) traffic data between ports in the 5G core network and address various anomaly detection challenges using machine learning (ML) and deep learning (DL) techniques.

For instance, Kim et al. [4] proposed an intrusion detection mechanism based on feature selection and ML to identify potential cyberattacks in the 5G Core Network. This study specifically focused on the General Packet Radio Service (GPRS) Tunneling Protocol (GTP) and employs four AI models—Decision Tree, Random Forest, K-Nearest Neighbors (KNN), and Stacked Autoencoder—for anomaly detection, with the Random Forest model achieving the highest detection accuracy. Hu et al. [5] addressed the issue of an expanded attack surface in the 5G core network due to the massive connectivity of IoT devices and proposed an intrusion detection mechanism utilizing a multiple-kernel clustering (MKC) algorithm, which enhances clustering accuracy for incompletely sampled data and mitigates the sensitivity of anomaly detection model to feature selection.

Additionally, Radivilova et al. [6] explored several methods, including Decision Tree, DBSCAN (Density-Based Spatial Clustering of Applications with Noise), entropy, and time series analysis, to detect anomalies such as DDoS attacks, UDP flooding, TCP SYN attacks, ARP spoofing, and HTTP flooding. The results indicated that the Decision Tree method is highly effective in anomaly detection. Furthermore, Zhang et al. [7] focused on behavioral analysis and characterized network functional behavioral patterns through behavioral portraits. This approach integrated learning algorithms, such as RFECV (Recursive Feature Elimination with Cross-Validation) for attribute feature selection and graph modeling based on network function interactions, transforming the anomaly detection problem into a graph node classification task. Experimental results demonstrated that this method outperforms traditional ML models based on attribute feature analysis, graph embedding models based on structural feature analysis, and several existing 5G core network anomaly detection models.

Despite the significant contributions of the aforementioned studies in identifying and mitigating various security threats to the 5G core network architecture, they largely overlook anomaly detection related to the N4 interface and the Packet Forwarding Control Protocol (PFCP). Makondo et al. [8] highlighted that deploying the UPF as an independent node at the network edge exposes the PFCP protocol to cybersecurity threats. The study categorized various attack types targeting PFCP and provided recommendations and future research directions to mitigate these risks.

To facilitate further research on PFCP protocol attacks, Amponis et al. [9] introduced a labeled dataset, the 5GC PFCP Intrusion Detection Dataset, designed to support anomaly detection efforts in the 5G core network. Expanding upon this dataset, Radoglou-Grammatikis et al. [3] employed artificial intelligence (AI) techniques to detect multiple cyber-attacks against the PFCP protocol. However, this study only explored the fundamental design of an anomaly detection architecture and conducted preliminary ML and DL model evaluations, with the Decision Tree model achieving the highest detection accuracy of 64.1%. Furthermore, Pell et al. [10] employed a Long Short-Term Memory (LSTM) model to predict traffic patterns and detect PFCP-related attacks. The model was trained on a benign dataset and tested on a dataset containing PFCP signaling attacks. Experimental results demonstrated that the LSTM model successfully identifies anomalous packets associated with PFCP session modification attacks with an accuracy of 95%.

Existing research on risk issues and anomaly detection for N4 interfaces remains limited in scope. [10] focused solely on a single attack scenario—the PFCP session modification attack, while [3] fails to incorporate standard business process information, which plays a critical role in anomaly detection modeling. Moreover, the detection performance of the proposed solutions still leaves room for improvement. Therefore, there is a pressing need to develop a novel anomaly signaling detection mechanism for the N4 interface threat model, integrating the standard operational process of the PFCP protocol.

III. Threat Model

Based on the PFCP protocol message information and the actual networking architecture between the SMF (Session Management Function) and UPF, this section presents a risk threat model for the PFCP protocol, including the following four typical risk scenarios, as illustrated in Fig. 1.

a) **PFCP Session Deletion Attack:** The attacker exploits the SEID (Session Endpoint Identifier) generation rules and range of PDU (Packet Data Unit) sessions to craft a large volume of forged PFCP session deletion requests, which are then transmitted to the target network element, the UPF. This attack aims to disrupt the PDU session connectivity between the targeted User Equipment (UE) and the Data Network (DN). By forcing the target UE to disconnect from the DN, the attacker induces widespread service disruptions, affecting multiple UEs served by the target UPF.

b) **PFCP Session Establishment Flooding Attack:** The attacker exploits an unauthorized and forged SMF to send a high volume of illegitimate PFCP session establishment requests to the target UPF. The primary objective is to overwhelm the UPF with excessive requests, thereby impeding legitimate session establishment attempts and depleting the UPF's resources. This disrupts normal PDU session establishment processes, leading to resource exhaustion at the target UPF and preventing legitimate user equipment from accessing the network.

c) **PFCP Session Modification Attack (DROP):** The attacker generates a large volume of PFCP session modification requests by manipulating Forwarding Action Rules (FARs) and configuring the Apply Action field to the DROP flag. The objective is to compel the target UPF to remove the Tunnel Endpoint Identifier (TEID) and IP address associated with the gNB (Next-Generation NodeB), thereby blocking access to the Data Network (DN). This disrupts network services for multiple user devices connected to the target UPF, leading to widespread service interruptions.

d) **PFCP Session Modification Attack (DUPL):** The attacker generates unauthorized PFCP session modification requests by modifying the DUPL (Duplicate) flag bit in the Apply Action field. The objective is to establish multiple packet forwarding paths for data originating from a single source, generating redundant duplicate packets at the DN. This uncontrolled packet duplication gradually depletes the UPF's packet-processing resources, ultimately leading to performance degradation and impaired network functionality.

IV. PASD-5GC Architecture

A. Overall architecture

As depicted in Fig. 2, the system architecture consists of two core modules: the Sequence Modeling Module and the Abnormal Signaling Detection Module. 1)Sequence Modeling Module: This module constructs signaling sequences, either normal or anomalous, based on the PFCP session flow management specifications and predefined behavioral patterns. 2)Abnormal Signaling Detection Module: Following the sequence modeling, this module evaluates the sequences to determine their normality or abnormality, ultimately generating the detection results.

To elaborate, consider the input data $X \in \mathbb{R}^{N \times m}$, where N denotes the total number of input instances, and m represents the dimensionality of the data features. The output of the sequence modeling process is given by $S \in \mathbb{R}^{n \times k \times m}$, where n denotes the number of sequences, k the sequence length, and m the feature dimension. These sequences are constructed by session management process specifications and subsequently fed into the abnormal signaling detection module. Within this module, sequence features are extracted at both local and global levels using techniques such as dilated convolution and the multi-head attention mechanism. The final output is expressed as $Y \in \mathbb{R}^{n \times l}$, where l represents the number of classification labels. The model is trained using a cross-entropy loss function to optimize detection accuracy. By integrating structured sequence modeling with advanced feature extraction, PASD-5GC provides a robust and effective framework for identifying signaling anomalies in 5G networks.

B. Sequence Modeling

The session management process within the N4 interface can be categorized into three primary phases: the session establishment phase, the session modification phase, and the session deletion phase. The coordinated execution of these phases forms the cornerstone of session management, ensuring both network flexibility and the efficient utilization of resources.

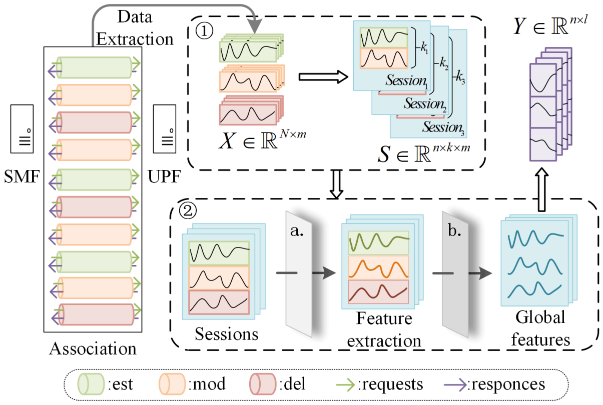


Fig. 2: Process-based Anomalous Signaling Detection System for 5G core network, where ① denotes Sequence Modeling Module, ② denotes Abnormal Signaling Detection Module, *a* denotes dilated convolution, and *b* denotes multi-head attention. N denotes the total number of input instances, n denotes the number of sequences, k the sequence length, and m the feature dimension.

In accordance with the N4 interface session process specifications, this study employs a structured methodology to model and define the data flow exchanged between NFs as follows:

1) Session Message: The i^{th} session message, denoted as X_i, is defined as a unidirectionally transmitted message between the SMF and UPF over the N4 interface. It is formally expressed as:

$$X_i : NF_{ori} \overset{feature}{\longrightarrow} NF_{des}, \tag{1}$$

where NF_{ori} and NF_{des} denote the original and destination NFs of the message, respectively, and $feature$ denotes the session features, which contain information such as the SEID of the session message and the session phase stage. Each session message is represented as $X_i \in (NF_{ori}, NF_{des}, feature)$.

2) Session Sequence: The j^{th} sequence S_j is defined as an ordered collection of k consecutive session messages within the same session:

$$S_j = [X_1, X_2, \ldots, X_k], \tag{2}$$

where k denotes the length of the sequence, which can vary between different sessions. The session messages X_1 to X_k are arranged chronologically within the same session, and each sequence S_j describes a complete session process.

C. Abnormal Signaling Detection

To address the dual requirements of detecting both signaling timing anomalies and individual signaling anomalies, this paper proposes DM-Net (Dilated Convolution and Multi-Head Attention Improved Network). The proposed model integrates single signaling features with process context features by combining a dilated convolutional neural network with a multi-head attention mechanism, both of which are jointly optimized. Furthermore, DM-Net enables the classification of normal and anomalous sequences across different session stages, as represented by the abnormal signaling detection module in Fig. 2.

In sequence data processing, traditional convolution operations struggle to capture long-range dependencies due to the inherent limitations of receptive fields. To address this challenge, this paper employs dilated convolution to extract long-term dependency features across multiple phases efficiently. Additionally, a multi-head attention mechanism enhances sensitivity to local anomalies by dynamically emphasizing key features at different temporal scales. By integrating dilated convolution with multi-head attention, the proposed model significantly improves the ability to detect anomalous signaling.

A multilayer dilated convolution network is employed to extract long-range dependency features from input sequences. By capturing multi-scale features at varying dilation rates, dilated convolution allows the model to expand its receptive field while preserving computational efficiency. This effectively alleviates information loss in sequential data and improves the ability of the model to extract critical information on multiple scales. Specifically, for the input data $X^{(0)} = S \in \mathbb{R}^{n\times k\times m}$:

$$X^{(n)} = \sum_{m=0}^{M-1} X^{(n-1)}(i+m\cdot d_n)\cdot K_n(m), n = 1,2,3 \tag{3}$$

where $X^{(n)}$ denotes the output of the n^{th} layer convolution, i denotes the index position of the output sequence, K_n denotes the n^{th} convolution kernel weight, d_n denotes the dilation rate of the n^{th} layer convolution, and M denotes the convolution kernel size.

Beyond capturing long-range dependencies in sequences using dilated convolution, it is equally essential to establish correlations between local and global features within signaling sequences. To this end, this paper incorporates Multi-Head Attention, enabling the model to simultaneously focus on local and global features across multiple temporal scales. This facilitates a more comprehensive understanding of intricate patterns in signaling data, as expressed mathematically by:

$$X' = C\left(S\left(\frac{X^{(3)}W_1(X^{(3)}W_2)^T}{\sqrt{d}}\right)X^{(3)}W_3\right)W_O, \tag{4}$$

where W_1, W_2, W_3, W_O are the learnable transformation matrices, d is the attention dimension. C represents the concat operation and S represents the softmax operation. The formula performs adaptive transformation and feature combination on the input features $X^{(3)}$ to generate the fused feature representation X'.

Building upon this foundation, residual connections are introduced to retain the original information, while normalization is applied to ensure numerical stability. Subsequently, a feed-forward neural network (FFN) is employed to perform additional nonlinear transformations, further enhancing the representation of extracted features. This process is mathematically expressed as:

$$X^{final} = LN(FFN(LN(X' + X^{(3)})) + LN(X' + X^{(3)})), \tag{5}$$

where LN denotes the normalization operation, FFN denotes the Feed-Forward Neural Network, $X' + X^{(3)}$ denotes the Residual Connection.

Finally, the extracted feature vector X^{final} is input into a linear classification layer to perform multi-class prediction, thereby yielding the anomaly detection classification results $Y \in \mathbb{R}^{n\times l}$:

$$Y = Softmax(ReLU(X^{final}W + b)W_{out} + b_{out}) \tag{6}$$

By integrating the multi-scale feature extraction capability of dilated convolution with the global information modeling capacity of multi-head attention, the proposed model effectively captures both local features and global dependencies within sequence data. This makes it well-suited for classifying high-dimensional, non-uniform, and complex temporal data, particularly excelling in the communication data scenario involving PFCP packet sequences.

D. PASD-5GC training and testing process

According to the session management process specification, each phase of messages within a session follows a specific order constraint. In the anomaly detection process, each session message X_i in the sequence S_i is first examined independently to verify its compliance with the characteristic specifications of individual messages. Subsequently, the overall sequence S_i is analyzed to determine whether it adheres to the predefined process constraints. The sequence is classified as anomalous if the messages within sequence S_i deviate from these standard constraints. The detailed procedure is presented in **Algorithm 1**.

V. Experimental Evaluation and Result Analysis

A. Dataset Construction and Sequence Modeling

To evaluate the accuracy and effectiveness of the proposed PASD-5GC and DM-Net models in anomaly detection, this paper utilizes the PFCP Intrusion Detection Dataset collected at the UPF, as referenced in [9], for simulation experiments.

The publicly available dataset comprises four types of abnormal signaling and normal signaling recorded by Amponis at various time intervals (15s, 20s, 60s, 120s, and 240s) during simulated attacks over the N4 interface.

Algorithm 1 PASD-5GC

```
Input: Signaling data $\{X_1, X_2, \ldots, X_i\}_1^N$; Batch_size of model training and testing $b$; DM-Net parameters $model(\theta)$; Training epoch $E$; Number of sequence classification labels $l$.
Output: Abnormal detection results $\{Y_1, Y_2, \ldots, Y_i\}_1^n$
  /* Sequence Modeling */
  Model the signaling data $\{X_1, X_2, \ldots, X_N\}$ as sequence data $S = \{S_1, S_2, \ldots, S_{2n}\}$ and corresponding labels $\{y_1, y_2, \ldots, y_{2n}\}$
  Sample the modeling data 1:1 to form $S_{train}, S_{test}$
  /* Model Training */
  Initialize $model(\theta)$
  for $1 \leq i \leq E$ do
      Perform forward propagation to obtain predicted score $\{\hat{Y}^{(1)}, \hat{Y}^{(2)}, \ldots, \hat{Y}^{(b)}\}$
      Update $loss \leftarrow -\sum_{j=1}^{l} C_{train\_i} log(\hat{Y}_j^{(b)})$
      Optimize model parameters $model : \theta' \leftarrow \theta$ after backpropagation
  end for
  /* Model Test */
  for $1 \leq i \leq n$ do
      Obtain results $\{\hat{Y}^{(1)}, \hat{Y}^{(2)}, \ldots, \hat{Y}^{(n)}\}$ through the parameters $model(\theta)$
      Obtain the highest probability distribution as the predictive label $Y \leftarrow classification(\hat{Y}^{(1)}, \hat{Y}^{(2)}, \ldots, \hat{Y}^{(n)})$
  end for
  Return anomaly detection results $\{Y_1, Y_2, \ldots, Y_n\}$
```

The signaling data characteristics vary depending on the selected time intervals. Shorter time intervals allow for the capture of finer-grained signaling patterns, enhancing local feature prominence and strengthening the correlation of process context information. Conversely, in longer time windows, extended signaling intervals may result in "information loss" within the feature space, leading to more dispersed contextual information. Given these variations, it is essential to conduct experimental evaluations on datasets with different time intervals to ensure comprehensive model assessment.

The dataset comprises 35 features, including flow ID, source IP, destination IP, source port, destination port, protocol, duration, fwd_packets, bwd_packets, among others. Given that this study focuses on PFCP session attacks and flow modeling, user-level message features play a more significant role in the analysis. Consequently, it is necessary to filter the dataset accordingly. Specifically, feature information related to association establishment between the SMF and UPF operates at the NF level, whereas request/response messages pertaining to PFCP sessions correspond to the user level. Therefore, only session flow-related features are retained for subsequent sequence modeling and anomaly detection, as summarized in Table I.

TABLE I: SESSION FLOW-RELATED FEATURES OF THE DATASET

Feature	Description
flow ID	Flow identifier
duration	Length of time flow was active
Fwd_packets	Number of forward packets
Bwd_packets	Number of backward packets
PFCPHeartbeat Request_counter	Number of PFCP Heartbeat Request messages
PFCPHeartbeat Response_counter	Number of PFCP Heartbeat Response messages
PFCPSessionEstablishment Request_counter	Number of PFCP Session Establishment Request messages
PFCPSessionEstablishment Response_counter	Number of PFCP Session Establishment Response messages
PFCPSessionModification Request_counter	Number of PFCP Session Modification Request messages
PFCPSessionModification Response_counter	Number of PFCP Session Modification Response messages
PFCPSessionDeletion Request_counter	Number of PFCP Session Deletion Request messages
PFCPSessionDeletion Response_counter	Number of PFCP Session Deletion Response messages
Label	Flow label (e.g. benign or malicious)

In the session flow of the N4 interface, a predefined sequence specification exists, such as $\langle est \rightarrow mod \rightarrow del \rangle$ or $\langle est \rightarrow del \rangle$, which dictates the order of session establishment, modification, and deletion phases. Based on this specification, this study constructs different sequences by grouping individual data points according to normal and abnormal session flows. Additionally, abnormal signaling is deliberately introduced into certain sequences. The dataset is then partitioned into training and testing sets in a 1:1 ratio to evaluate the model's effectiveness in detecting individual signaling anomalies and process-related abnormalities.

TABLE II: SEQUENCE COMBINATION METHODS

S1	S2	S3	Label
Normal-est	Normal-mod	Normal-del	0
Normal-est	0xxx	Normal-del	0
Normal-est	Normal-mod	Abnormal-del	1
Normal-est	Normal-mod	Abnormal-mod	2
Normal-est	Normal-mod	Abnormal-est	3
Normal-est	Normal-mod	Normal-est	4
Normal-est	Normal-mod	Normal-mod	5
Normal-est	Normal-est	0xxx	6
Normal-est	Abnormal-est	0xxx	7
Normal-est	Abnormal-mod	0xxx	8
Normal-est	Abnormal-del	0xxx	9
Normal-mod	0xxx	0xxx	10
Normal-del	0xxx	0xxx	11
Abnormal-est	0xxx	0xxx	12
Abnormal-mod	0xxx	0xxx	13
Abnormal-del	0xxx	0xxx	14

The detailed composition of normal and abnormal sequences is presented in Table II, which includes two normal sequences (labeled 0) and fourteen abnormal sequences (labeled 1–14), where S_n represents the n^{th} packet in each sequence. 0xxx indicates that the sequence packet is empty, while est, mod, and del represent signaling for establishment, modification, and deletion, respectively.

B. Comparing baselines and evaluation indicators

1) Comparing baselines: To comprehensively evaluate the detection performance of PASD-5GC, this paper selects 5GCIDS [3] as a comparative benchmark to validate the effectiveness and accuracy of the proposed architecture. The 5GCIDS framework conducts anomaly detection without differentiating between anomalous signaling events within specific processes; instead, it directly performs overall feature learning and anomaly detection. In contrast, the proposed architecture first applies sequence modeling to transform isolated signaling data into structured sequence data before executing anomaly detection. Furthermore, to assess the effectiveness of the DM-Net model, this study also conducts comparative experiments against traditional machine learning and deep learning models utilized in [3]. The baseline models include Decision Tree(DT) [11], Random Forest(RF) [12], K-Nearest Neighbors (KNN) [13], Support Vector Machine (SVM) [14], AdaBoost [15], Gradient Boosting(GB) [11], Extra Tree(ET) [16], XGBoost [17], LightGBM [18], and Multilayer Perceptron (MLP) [19].

2) Evaluation indicators: To assess the experimental results quantitatively, this study employs five evaluation metrics: Accuracy, Recall, False Positive Rate (FPR), F1 Score, and Precision, as defined in Equation 7.

$$
\begin{aligned}
Accuracy &= \frac{TP+TN}{TP+TN+FP+FN} \\
Recall &= \frac{TP}{TP+FN} \\
FPR &= \frac{FP}{FP+TN} \\
F1 &= \frac{2\times TP}{2\times TP+FP+FN} \\
Pre &= \frac{TP}{TP+FP}
\end{aligned}
\tag{7}
$$

C. Experimental results and analysis

1) Comparison of PASD-5GC and 5GCIDS: To evaluate the effectiveness of the PASD-5GC architecture, this study selects the 5GCIDS architecture for comparative experiments using the 15s dataset, with the results presented in Fig. 3 and Table III. The experimental findings indicate a significant improvement in anomaly detection accuracy under the PASD-5GC architecture compared to the 5GCIDS architecture. Benefiting from sequence modeling, the Support Vector Machine (SVM) model, a conventional machine learning approach, achieves a 38% increase in accuracy relative to the 5GCIDS architecture. Similarly, the Multilayer Perceptron (MLP) model improves its accuracy from 54% to 88%, representing a 34% enhancement. Other models also exhibit substantial improvements in detection performance. The superiority of PASD-5GC over the traditional 5GCIDS architecture in detecting individual signaling packets stems from its explicit sequence modeling of the PFCP session management process and its behavioral patterns. By incorporating process context information and effectively integrating local signaling features with global sequence-level features, PASD-5GC achieves more robust anomaly detection.

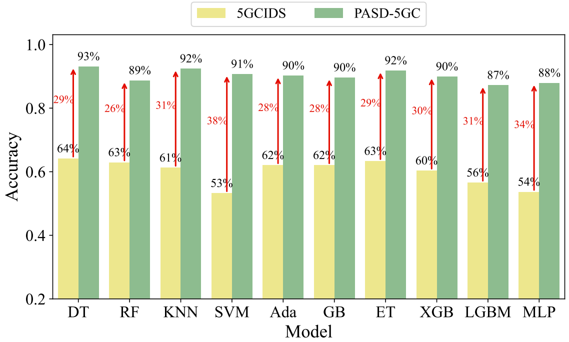


Fig. 3: Comparison of the Accuracy of PASD-5GC and 5GCIDS of Models in 15s-Timeout Dataset

TABLE III: Comparison of Recall, FPR, and F1-score for models in two architectures in the 15s-Timeout dataset

Models	PASD-5GC			5GCIDS		
	Recall	FPR	F1-Score	Recall	FPR	F1-Score
DT	**0.930**	**0.005**	**0.910**	0.639	0.090	0.642
RF	**0.887**	**0.008**	**0.865**	0.627	0.093	0.633
KNN	**0.924**	**0.005**	**0.898**	0.61	0.097	0.614
SVM	**0.907**	**0.007**	**0.897**	0.529	0.117	0.482
Ada	**0.902**	**0.007**	**0.871**	0.618	0.095	0.627
GB	**0.896**	**0.007**	**0.871**	0.618	0.095	0.629
ET	**0.917**	**0.006**	**0.911**	0.631	0.092	0.641
XGB	**0.899**	**0.007**	**0.899**	0.601	0.099	0.612
LGBM	**0.872**	**0.009**	**0.870**	0.563	0.108	0.579
MLP	**0.879**	**0.009**	**0.861**	0.533	0.116	0.486

2) Comparison of results between DM-Net model and other models in PASD-5GC: To validate the effectiveness of the proposed DM-Net model in accurately categorizing different anomaly types in the detection process, this study selects the four baseline models with the highest accuracy, along with Dilated Convolution(DC), Multi-Head Attention(MHA) and Long Short-Term Memory(LSTM) models, for comparison. The evaluation is conducted using Accuracy, Recall, FPR, and F1 Score metrics. The experimental results demonstrate that the DM-Net model effectively balances high detection completeness and accuracy, achieving significant improvements in accuracy and F1 Score compared to other models. As presented in Table IV, the DM-Net model exhibits superior performance. Specifically, compared to the decision tree model, the DM-Net model improves accuracy by 5.4%, while achieving a 7.4% increase in F1 Score over the extra tree model. Furthermore, compared to the DC model, DM-Net enhances accuracy by 12.8% and F1 Score by 14.6%. In comparison with the MHA model, DM-Net improves accuracy by 4.0% and F1 Score by 4.5%. In comparison with the LSTM model, DM-Net improves accuracy by 6.0% and F1 Score by 8.1%.

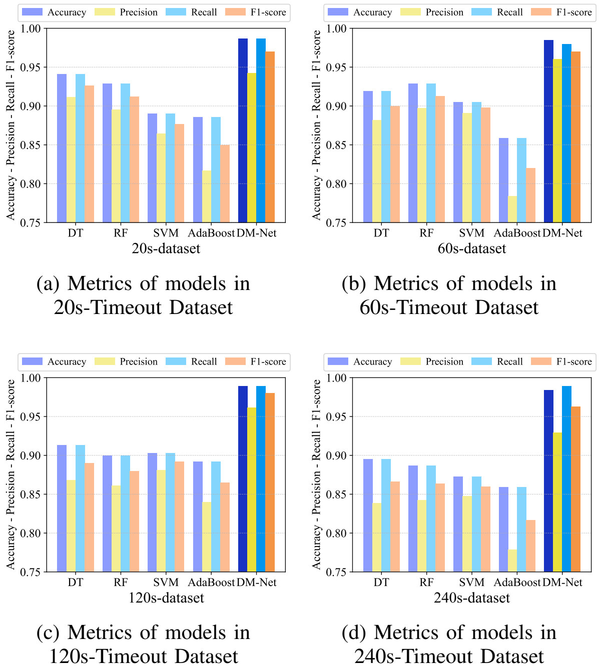
By integrating dilated convolution to extract key sequence information at multiple scales and employing the multi-head attention mechanism to focus concurrently on sequence patterns across different time scales, the DM-Net model demonstrates a more substantial capacity to adapt to complex data structures and enhance anomaly detection performance.

TABLE IV: Comparison of Accuracy, Recall, FPR, and F1 Score of Models in 15s-Timeout Dataset

Model	Accuracy	Recall	FPR	F1-Score
DT	0.931	0.930	0.005	0.910
KNN	0.924	0.924	0.005	0.898
ET	0.918	0.917	0.006	0.911
SVM	0.907	0.907	0.007	0.897
DC	0.857	0.857	0.010	0.839
MHA	0.945	0.945	0.004	0.940
LSTM	0.925	0.925	0.005	0.904
DM-Net	**0.985**	**0.985**	**0.001**	**0.985**

3) Comparison of results in the expanded datasets: To evaluate the generalization capability of the proposed DM-Net model in anomaly signaling detection across datasets with different time intervals, this study selects datasets with 20, 60, 120, and 240-second timeouts from the 5GC PFCP Intrusion Detection Dataset. Additionally, for comparison, the best-performing baseline models for each dataset, Decision Tree, Random Forest, SVM, and AdaBoost, are selected for experimentation.

The experimental results indicate that as the dataset time interval increases, the accuracy advantage of the DM-Net model over traditional machine learning models becomes more pronounced. As illustrated in Fig. 4, in the 20s-Timeout dataset, the DM-Net model achieved a 4.6% improvement in accuracy and recall, a 3.2% increase in precision, and a 4.4% enhancement in the F1-score compared to the Decision Tree model. In the 60s-Timeout dataset, the DM-Net model outperformed the Random Forest model with a 5.6% increase in accuracy, a 6.3% improvement in precision, a 5.1% enhancement in recall, and a 5.7% increase in the F1-score. In the 120s-Timeout dataset, the DM-Net model exhibited a 7.6% improvement in accuracy and recall, a 9.4% increase in precision, and a 9.0% enhancement in the F1-score compared to the Decision Tree model. In the 240s-Timeout dataset, the DM-Net model demonstrated an 8.9% improvement in accuracy, a 9.1% increase in precision, a 9.4% enhancement in recall, and a 9.7% improvement in the F1-score compared to the Decision Tree model.



(a) Metrics of models in 20s-Timeout Dataset

(b) Metrics of models in 60s-Timeout Dataset

(c) Metrics of models in 120s-Timeout Dataset

(d) Metrics of models in 240s-Timeout Dataset

Fig. 4: Anomaly Detection Metrics of models in Expanded Datasets of Different Time Intervals

This performance enhancement is attributed to the combination of dilated convolution and the multi-head attention mechanism, enabling the model to extract and learn local and global features effectively. As a result, the DM-Net model exhibits a superior understanding of complex temporal patterns. Even when the dataset contains dispersed sequence context information, the model can accurately capture signaling behavioral patterns, maintain high anomaly detection accuracy, and demonstrate strong robustness across varying data distributions and signaling scenarios. This adaptability allows the model to effectively accommodate the diverse traffic characteristics of the 5G core network.

VI. PASD-5GC deployment

To enable seamless integration of PASD-5GC for PFCP anomaly detection within the 5G core network, we propose its deployment as a functional component of the Network Data Analytics Function (NWDAF), as standardized by 3GPP. NWDAF is specifically designed to aggregate data from 5G network functions (NFs) to support machine learning-based analytics and decision-making. By embedding PASD-5GC within NWDAF, the model can leverage existing data pipelines without introducing additional monitoring burdens. This architectural integration facilitates real-time anomaly detection on the N4 interface while preserving system efficiency.

Furthermore, hosting PASD-5GC within NWDAF ensures model lifecycle manageability—enabling routine retraining, performance monitoring, and integration with NWDAF's mechanisms for accuracy assessment and model degradation mitigation.

VII. Conclusion

In this paper, we propose a process-based anomalous signaling detection approach for 5GC N4 interfaces, called PASD-5GC, which accurately characterizes normal signaling behavior and identifies anomalies by sequentially modelling the signaling flow of the PFCP protocol while fully leveraging its global contextual information. Furthermore, we design a deep learning model that integrates dilated convolution and a multi-head attention mechanism, enabling the simultaneous extraction of local features and modelling of global dependencies. This approach enhances the ability to represent complex temporal patterns, thereby improving the accuracy and robustness of anomaly detection. Experimental results on the 5GC PFCP intrusion detection dataset demonstrate that the proposed approach significantly outperforms the existing method regarding accuracy and recall, validating its effectiveness. In Future research, we will focus on further optimizing the model architecture to accommodate more protocol interfaces and exploring its potential deployment in real-world 5G core network environments.

References

[1] A. Manan, Z. Min, C. Mahmoudi, and V. Formicola, "Extending 5g services with zero trust security pillars: a modular approach," in *2022 IEEE/ACS 19th International Conference on Computer Systems and Applications (AICCSA)*. IEEE, 2022, pp. 1–6.

[2] Z. Haddad, M. M. Fouda, M. Mahmoud, and M. Abdallah, "Blockchain-based authentication for 5g networks," in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*. IEEE, 2020, pp. 189–194.

[3] P. Radoglou-Grammatikis, G. Nakas, G. Amponis, S. Giannakidou, T. Lagkas, V. Argyriou, S. Goudos, and P. Sarigiannidis, "5gcids: An intrusion detection system for 5g core with ai and explainability mechanisms," in *2023 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2023, pp. 353–358.

[4] Y.-E. Kim, Y.-S. Kim, and H. Kim, "Effective feature selection methods to detect iot ddos attack in 5g core network," *Sensors*, vol. 22, no. 10, p. 3819, 2022.

[5] N. Hu, Z. Tian, H. Lu, X. Du, and M. Guizani, "A multiple-kernel clustering based intrusion detection scheme for 5g and iot networks," *International Journal of Machine Learning and Cybernetics*, pp. 1–16, 2021.

[6] T. Radivilova, L. Kirichenko, O. Lemeshko, D. Ageyev, O. Mulesa, and A. Ilkov, "Analysis of anomaly detection and identification methods in 5g traffic," in *2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, vol. 2. IEEE, 2021, pp. 1108–1113.

[7] W. Zhang, L. Ji, S. Liu, X. Li, P. Fei, and H. Xinxin, "Ibnad: An interaction-based model for anomaly detection of network function in 5g core network," *Journal of Cyber Security*, vol. 9, no. 3, pp. 94–112, 2024.

[8] N. Makondo, E. Baloyi, H. I. Kobo, and T. E. Mathonsi, "A review of pfcp cyber attacks in 5g standalone for robotic telesurgery services," in *2024 International Conference on Next Generation Computing Applications (NextComp)*. IEEE, 2024, pp. 1–7.

[9] G. Amponis, P. Radoglou-Grammatikis, G. Nakas, S. Goudos, V. Argyriou, T. Lagkas, and P. Sarigiannidis, "5g core pfcp intrusion detection dataset," in *2023 12th International Conference on Modern Circuits and Systems Technologies (MOCAST)*. IEEE, 2023, pp. 1–4.

[10] R. Pell, M. Shojafar, and S. Moschoyiannis, "Lstm-based anomaly detection of pfcp signaling attacks in 5g networks," *IEEE Consumer Electronics Magazine*, vol. 14, no. 1, pp. 56–64, 2024.

[11] M. Douiba, S. Benkirane, A. Guezzaz, and M. Azrour, "An improved anomaly detection model for iot security using decision tree and gradient boosting," *The Journal of Supercomputing*, vol. 79, no. 3, pp. 3392–3411, 2023.

[12] R. Primartha and B. A. Tama, "Anomaly detection using random forest: A performance revisited," in *2017 International conference on data and software engineering (ICoDSE)*. IEEE, 2017, pp. 1–6.

[13] J. Tian, M. H. Azarian, and M. Pecht, "Anomaly detection using self-organizing maps-based k-nearest neighbor algorithm," in *PHM society European conference*, vol. 2, no. 1, 2014.

[14] X. Zhang, C. Gu, and J. Lin, "Support vector machines for anomaly detection," in *2006 6th world congress on intelligent control and automation*, vol. 1. IEEE, 2006, pp. 2594–2598.

[15] Y. Yuan, G. Kaklamanos, and D. Hogrefe, "A novel semi-supervised adaboost technique for network anomaly detection," in *Proceedings of the 19th ACM international conference on modeling, analysis and simulation of wireless and mobile systems*, 2016, pp. 111–114.

[16] A. R. Kharwar and D. V. Thakor, "An ensemble approach for feature selection and classification in intrusion detection using extra-tree algorithm," *International Journal of Information Security and Privacy (IJISP)*, vol. 16, no. 1, pp. 1–21, 2022.

[17] S. T. Ikram, A. K. Cherukuri, B. Poorva, P. S. Ushasree, C. Zhang, X. Liu, and G. Li, "Anomaly detection using xgboost ensemble of deep neural network models," 2021.

[18] M. K. Islam, P. Hridi, M. S. Hossain, and H. S. Narman, "Network anomaly detection using lightgbm: A gradient boosting classifier," in *2020 30th international telecommunication networks and applications conference (ITNAC)*. IEEE, 2020, pp. 1–7.

[19] T. Teoh, G. Chiew, E. J. Franco, P. Ng, M. Benjamin, and Y. Goh, "Anomaly detection in cyber security attacks on networks using mlp deep learning," in *2018 international conference on smart computing and electronic enterprise (ICSCEE)*. IEEE, 2018, pp. 1–5.