AI and Data Science Journal
ISSN: 3078-7394
DOI: https://doi.org/10.61784/adsj3009

5G ABNORMAL SIGNALING DETECTION BASED ON AUTO-ENCODER

YaDi Fu
School of Cyber Security, Beijing University of Posts and Telecommunications, Beijing 100876, China.
Corresponding Email: 2022111026@bupt.cn

Abstract: With the proliferation of 5G networks, increasing attention has been directed toward associated security risks. The N4 interface, serving as the interface between the user plane and control plane in 5G architecture, encompasses functionalities including session management and policy enforcement, and is susceptible to risks such as session hijacking. PFCP, as the application layer protocol of the N4 interface, can be effectively monitored through anomaly detection to identify abnormal behaviors within the N4 interface. Consequently, this paper proposes an autoencoder algorithm model implemented with Transformer neural networks. During the training process, the model learns the sequential characteristics of normal PFCP bidirectional flows. In the detection phase, data is processed through the encoder and decoder, and the model computes the Euclidean distance between the reconstructed data and the original data to derive an anomaly score. Additionally, this paper employs publicly available datasets to experimentally validate the efficacy of the algorithmic model in detecting PFCP traffic anomalies.
Keywords: 5G security; Signaling detection; N4 interface; PFCP

1 INTRODUCTION

With the evolution of mobile communication technologies, society has progressively transitioned into the 5G era. 5G represents the fifth generation of mobile communication technology, standardized by the 3GPP (3rd Generation Partnership Project) and endorsed by the ITU (International Telecommunications Union). In comparison to 4G networks, 5G mobile communication networks deliver enhanced speed and capacity for inter-device communications, while offering considerable flexibility through network slicing functionality that enables customization of network capabilities according to specific service scenarios. The scope of 5G extends beyond traditional human-to-human communications to encompass human-to-machine and machine-to-machine interactions, thereby significantly broadening its application domains. Critical services and vertical industries supported by 5G technology include industrial internet, vehicular networks, Internet of Things (IoT), and intelligent healthcare, all of which impose stringent requirements on network reliability and security[1]. The proliferation of terminal devices connecting to networks and the substantial integration of IoT devices simultaneously expands the attack surface and compounds the complexity of security management. As 5G networks progressively integrate with diverse societal sectors, their implications for national and social security become increasingly profound, resulting in heightened attention to 5G security vulnerabilities[2].

5G networks not only introduce novel technologies but also adopt new signaling protocols, such as PFCP protocols. The PFCP protocol functions as the application protocol for the N4 interface between Session Management Function (SMF) and User Plane Function (UPF). In wireless communication networks, signaling protocols facilitate fundamental network management and mobility management functionalities, specifically encompassing user authentication, authorization, billing, terminal state transitions, and terminal handovers. In an era of exponentially increasing mobile communication users, attacks targeting signaling protocols have proliferated, including the prevalent signaling storm attacks, which consume substantial network bandwidth resources, compromise network equipment processing capabilities, and in severe cases, precipitate network disruptions. Additionally, attackers exploit protocol vulnerabilities to execute session hijacking, eavesdropping, and other malicious activities; these security risks similarly extend to 5G's novel signaling protocols.

Signaling traffic in 5G networks, as well as in broader mobile communication networks, serves the critical function of information transmission. Consequently, the analysis and detection of signaling traffic enable the identification of certain behaviors within 5G networks. In high-volume traffic environments, anomalous traffic detection is extensively employed in security domains such as intrusion detection and attack identification. The detection of anomalous signaling traffic to identify security threats constitutes a common and efficacious security approach in mobile communication networks.

This paper proposes an autoencoder-based algorithm for detecting abnormal PFCP signaling traffic. This algorithm can train a model capable of detecting anomalous PFCP signaling behaviors even when only normal datasets are available. The performance of the model is validated using the public PFCP intrusion dataset provided by George. To address the issue of incomplete normal PFCP signaling data in this dataset, this paper establishes a 5G simulation environment based on OAI to simulate a more comprehensive and diverse range of normal PFCP signaling traffic.

2 RELATED WORK

With the advancement of 5G networks, the entire telecommunications industry is endeavoring to address the security challenges inherent in 5G architecture, technology, and services. The security architecture defined by the 3GPP committee encompasses three security layers and six security domains. The three security layers comprise the Transport Layer, Home Service Layer, and Application Layer. The six security domains consist of Network Access Security, Network Domain Security, User Domain Security, Application Domain Security, Service-Based Architecture (SBA) Domain Security, and Security Visibility and Configurability.

In February 2020, China's IMT-2020 (5G) Promotion Group compiled and published the "5G Security Report," which systematically analyzed 5G security challenges from two perspectives: key technologies and typical scenarios. The report elucidated that new 5G technologies introduce novel security challenges, necessitating the refinement of security measures in accordance with the specific characteristics of various 5G vertical domains.

Regarding the specifics of 5G signaling security, Hu[3] conducted an analysis of the HTTP/2 signaling protocol utilized between core network elements, identifying potential attacks facilitated by HTTP/2, including stream multiplexing attacks and header compression attacks. Inspired by DDoS attacks, George[4] investigated PFCP protocol-based attacks under the assumption that attackers had obtained N4 interface access. Their research encompassed unauthorized PFCP session deletion requests, unauthorized PFCP session modification requests, and unauthorized PFCP session establishment flooding attacks.

Numerous security solutions predicated on 5G traffic detection have emerged. Radivilova T[5] synthesized and experimentally evaluated existing anomalous traffic detection methodologies, conducting tests on authentic data sets with numerical characteristics approximating 5G traffic, subsequently comparing experimental outcomes and analyzing their distinctive features and appropriate application scenarios. LORENZO[6] proposed an adaptive deep learning-based anomaly detection system for 5G networks after comprehensive consideration of 5G network architecture. Pacherkar[7] introduced a security framework featuring a traceable graph for malicious flow detection, primarily targeting three attacks: SMS storm attacks, PFCP attacks, and network slicing attacks. Robert[8] simulated PFCP signaling attacks to generate normal and anomalous PFCP protocol datasets, subsequently employing LSTM neural networks for the detection of anomalous PFCP signaling.

3 METHOD

3.1 Overview

As illustrated in Figure 1, the algorithmic framework comprises three core modules: the PFCP Traffic Parsing Module, the PFCP Traffic Aggregation Module, and the Transformer-AE Model.

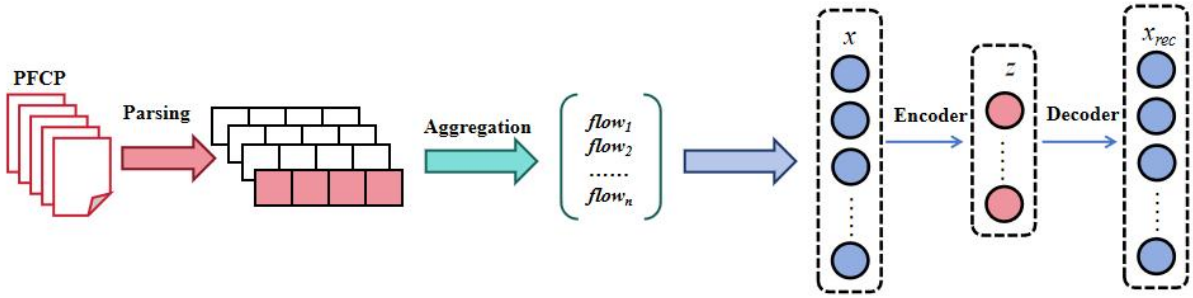

Figure 1 Overview of Anomaly Detection Framework

3.2 PFCP Traffic Parsing Module

This module is responsible for multi-level parsing of PFCP traffic. At the data link layer (MAC layer), timestamp information is parsed, establishing the foundation for subsequent temporal information learning. At the network layer (IP layer), source IP address and destination IP address parameters are extracted. At the transport layer, the source port and destination port fields are parsed. The packet parsing results from the network and transport layers will be utilized for subsequent traffic aggregation processing. At the application layer, the system parses PFCP signaling information and extracts PFCP message type fields. The final output format can be represented as: packet = [$feature_1$, $feature_2$, ..., $feature_n$], where n denotes the number of parsed fields for each packet.

3.3 Traffic Aggregation Module

In this phase, the input is packets = [$packet_1$, $packet_2$, ..., $packet_m$], i.e., m packets, with each packet containing n parsed fields. Based on source IP address, destination IP address, source port, and destination port parameters, the system aggregates packets into multiple bidirectional flows. Each flow is represented as flow = [$packet_1$, $packet_2$, ..., $packet_N$], where $N \leq 100$. The final output of this module is a collection of multiple flows, represented as flows = [$flow_1$, $flow_2$, ..., $flow_M$].

3.3 Transformer AE Module

In the model implementation process, both the encoder and decoder employ Transformer neural network architecture. As an emerging neural network structure, the Transformer[9] encompasses both encoder and decoder components. The encoder consists of a stack of identical layers, with each layer containing two sub-layers: a multi-head attention mechanism and a feed-forward network. Residual connections are applied around each sub-layer, followed by layer normalization. The decoder's structure is similar to the encoder's, also comprising multiple stacked layers, but each layer contains three sub-layers, namely, an additional multi-head attention mechanism that operates on the encoder's output is inserted between the encoder's two sub-layers.

In the Transformer AE[10] algorithm, the first layer of the encoder is a linear layer responsible for mapping the original input dimensions to the model's internal dimensions, ensuring input data compatibility with Transformer processing dimensions. Given that the Transformer neural network structure inherently lacks positional information, sequential positional encoding is necessary. This research employs sinusoidal and cosine functions to generate fixed positional encodings. After positional encoding, the system applies a dual-layer Transformer encoding structure to encode the data. The decoder, conversely, utilizes a dual-layer Transformer decoding structure to generate data from the input latent space.

During the training process, Mean Squared Error (MSE) is adopted as the loss function. In the anomaly detection phase, the model calculates an anomaly score for the input data, The formula is expressed as: $\mathrm{A} = \| D(E(x)) - x \|_2$

For the anomaly scores output by the Transformer AE model, this research employs a validation set method, optimizing evaluation metrics within the validation set to determine a threshold. In practical anomaly detection processes, when the anomaly score output by Transformer AE exceeds this threshold, it is classified as anomalous; conversely, it is classified as normal.

4 EXPERIMENTS

4.1 DataSet

4.1.1 Introduction of PFCP intrusion dataset

This paper utilizes the publicly available PFCP intrusion dataset provided by George for validation. The dataset includes PFCP session establishment DoS attacks, PFCP session deletion DoS attacks, and PFCP session modification flooding attacks. The aim of PFCP Session Establishment DoS Attack is to exhaust the resources of the UPF by inundating it with genuine Session Establishment Requests and Heartbeat Requests. The goal of PFCP Session Deletion DoS Attack is to disconnect a specific UE from the DN. The purpose of PFCP session modification flooding attacks is to attempt to alter session flows through a large volume of packets, thereby achieving the attack objective. There are two specific methods for this type of attack. The one is to invalidate packet handling rules for a specific session, leading to the disassociation of a targeted UE from the DN. The other one is to utilise the DUPL flag in the Apply Action field to compel the UPF to replicate rules for the session, generating multiple paths for the same data from a single source.

4.1.2 Normal PFCP signaling dataset

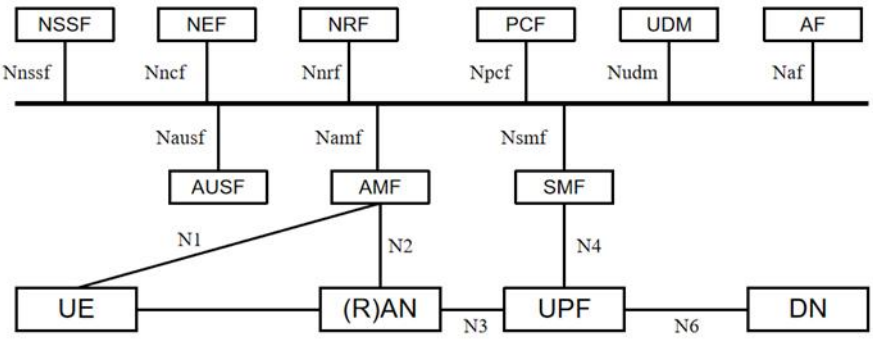

Figure 2 Overview of 5G Network Architecture

The 5G core network environment utilizes OAI simulation. The fundamental architecture of the 5G core network is illustrated in Figure 2. The network elements are constructed based on OAI network element packages. Multiple virtual machines are established in a Linux environment with appropriate network design and configuration. Each virtual machine functions as a distinct network element, interconnected within the server-provided network. The UE and base station are simulated using EXFO. These components collectively constitute the 5G core network, enabling the implementation of relevant communication functionalities.

The interface between the SMF (Session Management Function) and UPF (User Plane Function) network elements is designated as the N4 interface. At the application layer, the N4 interface employs the PFCP (Packet Forwarding Control Protocol). The primary functions of PFCP include data forwarding control, session management, separation of control

and user planes, QoS management, and others. Within the PFCP protocol stack, UDP serves as the transport layer protocol, while PFCP operates at the application layer. The PFCP protocol encompasses various signaling procedures, such as heartbeat procedures and session management procedures.

Following the establishment of the aforementioned simulated 5G core network environment, normal PFCP signaling traffic datasets were collected by capturing PFCP traffic on the N4 interface while executing normal activities in the UE access core network, including UE registration, PDU SESSION establishment, PDU SESSION termination, and UE deregistration. Through traffic parsing, aggregation, and data normalization processing, data with a length of 50 and a dimension of 4 can be obtained. The final dataset sizes available for training and testing are shown in Table 1.

Table 1 The Size of dataset

Type	Size
Normal	18431
PFCP session establishment DoS attack	7701
PFCP session deletion DoS attack	3432
PFCP session modification flooding attack	5375
All abnormal PFCP	16508

4.2 Result And Analysis

We used 60% of the normal data to train the model. 10% of normal data and 10% of abnormal data were used for threshold determination, with the remaining normal and abnormal data serving as the test set. First, this paper conducted experiments on datasets combining each type of anomaly with the normal test set, yielding the results shown in Table 2.

Table 2 Performance of anomaly detection methods

Data Type	Accuracy	Precision	Recall	F1-score
PFCP session establishment DoS attack	0.9930	0.9981	09893	0.9937
PFCP session deletion DoS attack	0.9937	0.9974	0.9851	0.9912
PFCP session modification flooding attack	0.9943	0.9985	0.9892	0.9939
All abnormal PFCP	0.9902	0.9981	0.9884	0.9932

To validate the advantages of the model, this paper selected three algorithms for comparison. The first applies Fourier transformation to the data, followed by clustering using the k-means[11] method. Training similarly used the normal dataset, resulting in multiple normal data cluster centers. When determining anomalies, the Euclidean distance between the data and the nearest cluster center is calculated; the greater the distance, the higher the degree of abnormality. The second replaces the Transformer neural network with an LSTM neural network, namely LSTM-AE[10], with data processing and training methods identical to those of the algorithm model in this paper. The third is a stacked encoder, with data processing and training methods identical to those of the algorithm model in this paper. The final results are shown in Table 3.

Table 3 Performance of anomaly detection methods

Algorithm	Accuracy	Precision	Recall	F1-score
K-means	0.9453	0.9755	09488	0.9619
LSTM-AE	0.9818	0.9949	0.9801	0.9875
SAE	0.9741	0.9885	0.9759	0.9821
Transformer AE	0.9902	0.9981	0.9884	0.9932

The experimental results indicate that during the detection process of each type of PFCP anomalous traffic, the accuracy consistently exceeded 99%, demonstrating overall excellent performance. In comparative analyses with baseline algorithms, the Transformer AE continued to exhibit superior detection capabilities. The K-means algorithm demonstrated the least effective detection performance, attributable to the limited capacity of machine learning models to effectively learn from sequential data. Conversely, the LSTM-AE algorithm, which maintained the autoencoder structure while replacing the Transformer network with LSTM neural networks, yielded relatively favorable outcomes. The results suggest that while LSTM retains considerable advantages in learning temporal data, Transformers possess

enhanced dependency capture capabilities. Consequently, autoencoder models implemented with Transformer architecture demonstrate superior performance compared to those implemented with LSTM neural networks.

5 CONCLUSION

This paper primarily investigates PFCP anomalous signaling detection and proposes an autoencoder algorithm model based on Transformer architecture. Through learning the bidirectional flow sequence characteristics of normal PFCP traffic, we have implemented an anomaly detection model. We constructed a 5G core network simulation environment using OAI and generated a rich corpus of normal data. The model was trained using the generated data and subsequently employed to detect anomalies in public PFCP intrusion datasets, achieving favorable accuracy rates. Comparative experiments were conducted to further validate the algorithmic advantages of our approach.

COMPETING INTERESTS

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

REFERENCES

[1] Kim, H. 5g core network security issues and attack classification from network protocol perspective. Internet Serv. Inf. Secur., 2020, 10(2): 1-15.
[2] Eric Ruzomberka, David J, Love, Christopher G, Brinton, et al. Challenges and Opportunities for Beyond-5G Wireless Security. IEEE Secur. Priv., 2023, 21(5): 55-66.
[3] Xinxin Hu, Caixia Liu, Shuxin Liu, et al. Signalling Security Analysis: Is HTTP/2 Secure in 5G Core Network?. 10th International Conference on Wireless Communications and Signal Processing, IEEE, 2018: 1-6.
[4] George Amponis, Panagiotis, Radoglou-Grammatikis, Thomas Lagkas, et al. Threatening the 5G core via PFCP DoS attacks: the case of blocking UAV communications. EURASIP J. Wirel. Commun. Netw., 2022, 2022(1): 124-150.
[5] Radivilova T, Kirichenko L, Lemeshko O, et al. Analysis of Anomaly Detection and Identification Methods in 5G Traffic. 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), IEEE, 2021: 1108-1113.
[6] Maimo, L F, Gomez, Gómez, Ángel Luis Perales, Clemente, Félix J, García, et, al. A self-adaptive deep learning-based system for anomaly detection in 5g networks. IEEE Access, 2018, 6, 7700-7712. DOI: 10.1109/ACCESS.2018.2803446.
[7] Harsh Sanjay Pacherkar, Guanhua Yan. PROV5GC: Hardening 5G Core Network Security with Attack Detection and Attribution Based on Provenance Graphs. Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks, ACM, 2024, 254-264.
[8] Robert Pell, Mohammad Shojafar, Sotiris Moschoyiannis. LSTM-Based Anomaly Detection of PFCP Signaling Attacks in 5G Networks. IEEE Consumer Electron. Mag., 2025, 14(1): 56-64.
[9] Ashish Vaswani, Noam Shazeer, Niki Parmar, et al. Attention is all you nee. arXiv preprint arxXiv: 1706.03762, 2017.
[10] Yingfei Xu, Yong Tang, Qiang Yang. Deep Learning for IoT Intrusion Detection based on LSTMs-AE[C]. AIAM2020: 2nd International Conference on Artificial Intelligence and Advanced Manufacture, ACM, 2020, 64-68.
[11] Gousiya Begum, S, Zahoor Ul Huq, A P, Siva Kumar. Fuzzy K-Means with M-KMP: a security framework in pyspark environment for intrusion detection. Multim. Tools Appl., 2024, 80(30): 73841-73863.