

Performance comparison of NWDAF-based security analytics techniques in 5G/B5G networks

Apostolis Garos, Nikos Alabasis, Victoria Katsarou, Georgios Gardikis
R&D Department
Space Hellas S.A.
Athens, Greece
{agaros; nalabasis; vkatsarou; ggar}@space.gr

Dimitris Santorinaios, Maria Christopoulou
Institute of Informatics and Telecommunications
NCSR “Demokritos”
Athens, Greece
{maria.christopoulou; dsantorinaios}@iit.demokritos.gr

Abstract—This paper evaluates the performance of NWDAF-based security analytics techniques in 5G/B5G networks, focusing on anomaly detection for network security incidents. Utilizing a 5G testbed, the study examines both statistical methods (Z-Score, MAD, Hampel Filter) and machine learning techniques (Isolation Forest, LOF, One-Class SVM) for the detection of control-plane and data-plane DoS/DDoS attacks. Results indicate a better performance of statistical methods over ML algorithms in such volume-based attacks and suggest a hybrid approach, combining statistical and ML methods, to enhance anomaly detection and adapt to diverse network conditions for improved 5G security.

Keywords—5G, security analytics, NWDAF, Machine Learning

I. INTRODUCTION

6G is expected to adopt and further expand the paradigm of a software-centric architecture, focusing on virtualization and cloud technologies, and implement a Service-based architecture (SBA) for scalable and modular Network Functions (NFs).

The Network Data Analytics Function (NWDAF), introduced in the 3rd Generation Partnership Project (3GPP) Release 15, marked a pivotal step towards data-driven and proactive network management. As defined in [1], NWDAF's main function is to collect and analyze data from across the 5G network, including performance metrics, user behavior, and network conditions, to optimize network performance, resource management, and user experience. Within the SBA of 5G, NWDAF interacts with other network functions through standardized interfaces, providing comprehensive data collection and analytics services.

NWDAF has a wide range of applications, improving network security, optimizing service quality, enabling network slicing for diverse service requirements, and supporting edge computing for low-latency applications. In Release 18, the NWDAF features an Analytics logical function (AnLF), focused on inference, and a Model Training logical function (MTLF), focusing on training. In this paper, we focus on analytics mechanisms that can be used by NWDAF to detect anomalies in network operations, which are often associated with security incidents[2]. More specifically, we examine and evaluate on a full-stack 5G testbed different analytics algorithms -covering both ML and statistical methods- in an attempt to detect such incidents from NWDAF metrics.

II. RELATED WORK

Various works have explored the use of machine learning (ML) and artificial intelligence (AI) to secure 5G networks and infrastructures. Reference [3] discusses AI and ML-driven applications for 5G network security and their potential impacts. In [4], the authors introduce a Convolutional Neural Network (CNN) for detecting malicious network traffic. Unlike approaches examining network traffic, our work focuses on operational network metrics (time-series data) from various network functions. Reference [5] presents an NWDAF implementation and highlights its analytics potential but does not go deeper into benchmarking analytics approaches. The authors in [6] compare different algorithms for using NWDAF data, focusing on prediction rather than outlier detection and security. In [7], three ML models are applied to investigate the estimation of behavior information and network load prediction capabilities of NWDAF. Similarly, the focus is on prediction, and the comparison is limited to ML models.

III. METHODOLOGY AND APPROACH

A. Testbed and pipeline

The development and testing was conducted in our lab “5G-in-a-box” platform (Fig.1), which implements a full-stack 5G system, integrating core, edge and access. The platform is built around the Amarisoft Callbox Classic solution. We operated the platform in 5G SA mode in n78, using COTS UEs (Realme 7, Samsung A52 and Waveshare 5G Hat).



Fig. 1. “5G-in-a-box” used for development and evaluation

The platform offers remote WebSocket APIs accessible via different URLs, facilitating interaction with these components. These APIs allow for the sending and receiving of JSON-formatted messages to perform tasks such as querying network statistics and managing UE data. We have developed a pipeline to digest these metrics in real-time. At regular intervals, requests are made for selected metrics such as downlink and uplink bitrates, transmission and error counts as well as detailed information about connected UEs. Metrics also include attach and tracking area updates, session management statistics, and comprehensive UE registration records.

Through asynchronous operations, non-blocking data collection is utilized to process multiple network requests concurrently, thereby enhancing performance and efficiency. The received responses are in JSON format and are parsed and flattened to simplify the data structure. This transformation from nested JSON to a tabular format is essential for creating CSV files. Each entry is timestamped and includes identifiers for various network elements such as RAN UE IDs, cell IDs, and transmission-related statistics, providing a detailed view of the radio access network's performance and status.

The processed data is then merged and dynamically appended to CSV files, ensuring that new data is incorporated accurately without overwriting existing entries. The resulting data frames are easy to manipulate, store, and analyze. This structured approach ensures that the data pipeline is both efficient and scalable, allowing for seamless handling of large datasets.

B. Scenarios

DoS/DDoS attacks are seen as significant threats to telecom infrastructures, including 5G/B5G, directly impacting QoS and the availability of 5G core network functions [8]. (D)DoS is also one of the most prominent incident scenarios to be detected using NWDAF analytics, as also identified in [1]. In this work, we consider two threat scenarios involving control- and data-plane DoS/DDoS attacks from compromised UEs.

Scenario 1: Control plane DoS. In the first scenario, anomalous behavior was characterized by very quick and frequent association-deassociation of UEs, aiming to flood the network control plane. The training dataset consisted of 1 hour of traffic, incorporating periods of normal UE activity (streaming video content continuously) interspersed with 5 and 10-minute segments of anomalous behavior. The test dataset, intended to assess model performance, was a 20-minute segment including a critical 5-minute anomaly phase.

Scenario 2: Data plane DoS. The second scenario involved a data-plane DoS attack to an edge application, utilizing the hping tool deployed in the UE. This scenario also included background normal traffic, using the same approach as Scenario 1. The training data spanned 1 hour, with 5 and 10-minute durations of induced attack, while the corresponding test dataset included a 20-minute sample with a 5-minute attack segment.

C. Preprocessing

Effective anomaly detection necessitated comprehensive preprocessing steps tailored to both scenarios. These steps were crucial for data normalization, missing value handling,

and feature preparation for subsequent analytical processes. Key preprocessing actions included:

- *Numeric Focus:* Retention of only numeric data types to ensure datasets comprised strictly quantitative metrics.
- *Missing Data Management:* Application of forward-fill methods to address data continuity and integrity.
- *Data Transformation and Feature Engineering:* Conversion of data to floating-point format followed by differentiation of consecutive data points, with resultant features suffixed by '_diff'.
- *Normalization:* Utilization of MinMaxScaler to achieve uniform data scaling across features.

D. Feature selection

The feature selection step involved selecting the appropriate features for each type of attack. For Scenario 1, the selected features were metrics specific to RRC (Radio Resource Control) reconfigurations, DRB (Data Radio Bearer) counts, and NGAP (NG Application Protocol) messages. For Scenario 2, the selected features focused on uplink and downlink data usage and scheduling metrics. These features were specifically selected for their relevance to the anomaly types being studied in each scenario. This careful curation helps to emphasize the data characteristics that are most indicative of normal versus anomalous conditions, enhancing the predictive capabilities of the subsequent anomaly detection models. This approach, although incident-specific, yields a much better performance than a generic anomaly detection technique applied equally to all metrics. In an operational deployment, it is suggested that NWDAF employs a set of models, each corresponding to a different family of adversary techniques.

E. Techniques applied

We employed six different techniques, both statistical and ML-based, to analyse the data and detect the incidents. These are:

Statistical measures:

- *Z-Score:* The Z-score quantifies how many standard deviations an observation is from the mean. Observations with a Z-score greater than a threshold (commonly set at 3) are considered outliers. This method is particularly useful in scenarios where data is expected to conform to a Gaussian distribution, making it well-suited for metrics such as signal strength and message counts in 5G networks.
- *Median Absolute Deviation (MAD):* MAD offers robustness against outliers and is less sensitive to non-normal distributions of data. It is effective for analyzing data traffic where anomalies manifest as significant deviations from the median traffic volume, aiding in the detection of network abuses or malfunctions.
- *Hampel Filter:* The Hampel Filter is adept at smoothing out 'noise' and identifying outliers in time-series data by adjusting to the data's moving median and variability. This method is highly suitable for real-time anomaly detection in continuous data streams,

such as those encountered in 5G network monitoring, effectively identifying sudden, transient changes in network behavior.

Machine learning techniques:

- *Isolation Forest*: Isolation Forest is an ensemble method that isolates anomalies instead of modeling the normal behavior. It operates by randomly selecting features and then randomly selecting split values between the maximum and minimum values of these features. In our study, we applied the Isolation Forest to detect anomalies in network traffic by parameterizing the number of estimators and the sample size. Hyperparameter tuning was conducted using GridSearchCV to optimize parameters like `n_estimators`, `max_samples`, and contamination based on the F1 score, aiming for the best performance in differentiating between normal and anomalous traffic.
- *Local Outlier Factor (LOF)*: The LOF algorithm measures the local deviation of density of a given data point with respect to its neighbors. It is effective in identifying density-based anomalies, which are common in network traffic data. We tuned the LOF model to identify deviations in the dataset by experimenting with different contamination levels and `n_neighbors` to find the optimal setting for our data. Performance was assessed using the F1 score or silhouette score in absence of labeled data, enhancing our understanding of the model's ability to generalize.
- *One-Class SVM*: The One-Class SVM is tailored for unsupervised anomaly detection and works by identifying the smallest hypersphere in a high-dimensional space encompassing most of the data points. Utilizing a radial basis function (RBF) kernel, we optimized hyperparameters such as `nu` and `gamma` using GridSearchCV, focusing on the maximization of the custom F1 score for anomaly detection. The model was particularly evaluated for its ability to distinguish between the normal operations and potential security breaches within the network.

IV. RESULTS

The performance of statistical and machine learning anomaly detection methods against the two above-mentioned scenarios was measured. The effectiveness of each method is evaluated based on accuracy, precision, recall, and F1 score, providing insights into their suitability for different types of network anomalies.

Table I summarizes the performance of each method applied to the data of Scenario 1 (Control plane DoS).

TABLE I. PERFORMANCE OF METHODS FOR SCENARIO 1

Method	Accu- racy	Preci- sion	Recall	F1 Score
Z-Score	0.94	0.99	0.78	0.87
MAD	0.96	0.91	0.96	0.93
Hampel filter	0.97	0.91	0.99	0.95
Isolation Forest	0.96	0.91	0.96	0.93
Local Outlier Factor	0.84	0.83	0.46	0.59

Method	Accu- racy	Preci- sion	Recall	F1 Score
One-class SVM	0.96	0.91	0.95	0.93

Table II summarizes the performance of each method applied to the data of Scenario 2 (Data plane DoS).

TABLE II. PERFORMANCE OF METHODS FOR SCENARIO 2

Method	Accu- racy	Preci- sion	Recall	F1 Score
Z-Score	0.87	0.98	0.46	0.63
MAD	0.46	0.29	0.95	0.45
Hampel filter	0.57	0.25	0.46	0.33
Isolation Forest	0.74	0.45	0.55	0.49
Local Outlier Factor	0.66	0.31	0.40	0.35
One-class SVM	0.80	0.70	0.25	0.37

V. DISCUSSION

A. Interpretation of Results

The evaluation of various anomaly detection methods within a 5G network context highlighted significant performance disparities. Statistical methods particularly excelled in scenarios characterized by clear, repetitive patterns. Through the application of metrics such as Z-score, MAD, and the Hampel filter, these methods demonstrated notable effectiveness and computational efficiency in identifying deviations from typical network behaviors.

Conversely, the detection of complex anomalies like hping attacks presented considerable challenges. These types of attacks, which often lack distinctive statistical signatures and are less predictable, underscore the need for more sophisticated detection strategies. This variability in method performance across different anomaly types stresses the importance of a deep understanding of both the nature of network anomalies and the operational context. Such knowledge is crucial to select the most effective detection methods, ensuring not only high accuracy but also alignment with the specific security and operational demands of the network, thereby enhancing overall network reliability and security.

B. Optimizing Anomaly Detection Approaches: Balancing Performance and Precision in 5G Networks

The analysis confirmed the robust performance of statistical methods over machine learning techniques in anomaly detection for 5G networks, underscoring their suitability for predictable anomaly patterns. These methods are particularly effective in scenarios where anomalies can be distinctly identified through statistical metrics. For example, the Hampel Filter was highly effective in detecting rapid UE behaviors with minimal false negatives, whereas the Z-Score method proved optimal for identifying irregular hping attacks. ML methods are expected to be more appropriate for scenarios involving low-volume persistent attacks, not examined in this paper.

This study highlights the critical need for tailoring anomaly detection strategies to the specific characteristics of

network anomalies, as well as for combining ML methods with traditional statistical measures, towards optimizing performance. The choice of model involves a strategic balance between achieving high recall to avoid missing crucial anomalies and maintaining high precision to reduce false alarms. z

VI. CONCLUSIONS AND FUTURE WORK

This study benchmarked various statistical and ML techniques for NWDAF-based security analytics. For the selected attack scenarios, the results confirmed the superiority of statistical methods, which proved particularly effective against clear, predictable anomalies. As an overall recommendation, it can be proposed that an effective security analytics framework coupled with NWDAF should engage a variety of techniques, both statistical and ML, each targeting a specific set of adversary techniques.

Follow-on research will focus on refining these statistical models to enhance their precision and adaptability to diverse network behaviors. Investigating hybrid models that combine the interpretability and efficiency of statistical methods with the dynamic learning capabilities of machine learning can be seen to provide a robust framework for future anomaly detection systems. Further exploration is also needed to ensure these methods can scale effectively in real-world 5G environments. Such mechanisms can be used as components of a holistic approach to 5G security, such as the EU Cybersecurity Toolbox [9].

ACKNOWLEDGMENT

This work has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the project PRIVATEER (GA No. 101096110) and the project SAFE-6G (GA No. 101139031). Views and opinions expressed are, however, those of the authors only and do not necessarily reflect those of the EU or SNS JU.

REFERENCES

- [1] 3GPP TS 23.288 (V18.4.0), "Architecture enhancements for 5G System (5GS) to support network data analytics services (Release 18)," Dec. 2023.
- [2] P. Gkonis et al., "Leveraging Network Data Analytics Function and Machine Learning for Data Collection, Resource Optimization, Security and Privacy in 6G Networks," *IEEE Access*, pp. 1–1, 2024, doi: 10.1109/ACCESS.2024.3359992.
- [3] H. Zeeshan Baig, and M. Imran. "Artificial Intelligence and Machine Learning in 5G Network Security: Opportunities, advantages, and future research trends." *arXiv preprint arXiv:2007.04490* (2020).
- [4] J. Lam and R. Abbas. "Machine learning based anomaly detection for 5g networks." *arXiv preprint arXiv:2003.03474* (2020).
- [5] A. Chouman, D. M. Manias and A. Shami, "Towards Supporting Intelligence in 5G/6G Core Networks: NWDAF Implementation and Initial Analysis," 2022 International Wireless Communications and Mobile Computing (IWCMC), Dubrovnik, Croatia, 2022, pp. 324-329
- [6] D. Chen, Q. Song, Y. Zhang, L. Li, and Z. Yang, "Comparative Analysis of Time Series Prediction Algorithms on Multiple Network Function Data of NWDAF", *Int. J. of Distributed Sensor Networks*, January 2024, <https://doi.org/10.1155/2024/5525561>
- [7] S. Sevçican, M. Turan, K. Gokarşlan, H. Yılmaz, T. Tugcu, "Intelligent network data analytics function in 5G cellular networks using machine learning", *Journal of Communications and Networks*. (2020) 22, no. 3, 269–280, <https://doi.org/10.1109/jcn.2020.000019>.
- [8] R. Ettiane, A. Chaoub, and R. Elkouch, "Toward securing the control plane of 5G mobile networks against DoS threats: Attack scenarios and promising solutions," *Journal of Information Security and Applications*, vol. 61, p. 102943, Sep. 2021, doi: 10.1016/j.jisa.2021.102943.
- [9] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, <https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures>