Development of an Architecture to Detect DDoS Attacks in end-to-end Network Slicing on 5G Networks

PHATHUVUYO JOYI
Department of Computational Sciences
University of Fort Hare
Alice, South Africa
201823077@ufh.ac.za

CAROLINE GURAJENA
Department of Computational Sciences
University of Fort Hare
Alice, South Africa
Cgurajena@ufh.ac.za

MOSHE T. MASONTA
NextGen Enterprises and Institutions
Council for Scientific and Industrial Research
Pretoria, South Africa
mmasonta@csir.co.za

***Abstract*—Network slicing is a fundamental enabler of 5G networks, allowing the creation of multiple virtual networks on a shared physical infrastructure to meet diverse service requirements. However, this flexibility introduces critical security and privacy challenges, as shared control-plane components and inter-slice communication can be exploited by attackers to launch Distributed Denial-of-Service (DDoS) attacks, compromise data confidentiality, and disrupt service availability. To address these challenges, this study proposes a secure end-to-end 5G network slicing architecture integrating real-time traffic monitoring, anomaly detection, and slice-aware security policies to protect against DDoS attacks. The architecture was implemented using Open5GS as the core network and UERANSIM as the radio access network emulator, enabling the creation of multiple slices (eMBB, URLLC, and mMTC) with isolated SMF–UPF pairs and a shared AMF. Experimental evaluation involved generating legitimate and malicious traffic to analyze control-plane behavior at the AMF, slice resource utilization, and attack impact on packet flow. The proposed system achieved a DDoS detection accuracy of 98%, with a false positive rate of 2.3%, and demonstrated up to 40% faster response to signaling floods compared to baseline threshold-based detection approaches. These results confirm that the architecture can effectively detect and mitigate DDoS attacks while maintaining stable performance across multiple slices. This work contributes a practical and extensible security framework for 5G network slicing, offering improved resilience and reliability compared to existing solutions.**

Keywords—5G Networks, Network Slicing, Security and Privacy, DDoS Detection, AMF

I. INTRODUCTION

In 2019, mobile operators globally began deploying 5G technology, marking the initial rollout of 5G networks with the goal of revolutionizing mobile wireless communications by offering faster services, incredibly low latency, and ubiquitous connectivity [1]. 5G is the successor of the 4G network which previously connected most modern devices. It was anticipated that by 2025, more than 1.7 billion people will be using 5G networks worldwide [2]. As of January 2025, the global number of connected Internet of Things (IoT) devices is estimated to be around 18.8 billion, with approximately 21% of these utilizing cellular technologies, including 5G. This suggests that roughly 3.9 billion devices are connected via cellular networks. While specific data on the exact number of devices connected exclusively to 5G networks is limited, 5G's share of mobile data traffic was projected to reach 34% by the end of 2024, indicating a significant and growing adoption of 5G technology [3].

IoT is an automation and analytics system that combines big data, artificial intelligence, networking, and sensing to deliver comprehensive systems for a good or service [4]. IoT relies on faster Internet speeds, making it one of the primary beneficiaries of the 5G network. When applied to any industry or system, IoT systems provide greater transparency, control, and performance [5]. IoT applications are divided into various domains based on the technology used, which includes smart homes, smart healthcare, industrial IoT (IIoT), smart transportation, smart agriculture, and smart cities. These domains specific applications have different network requirements. These network requirements are provisioned on the 5G network through network slicing.

Network slicing was proposed as a solution to the varied requirements for services provided through 5G network connection. A network slice is a set up with several isolated virtual resources on a common physical infrastructure [6]. To satisfy users' various communication needs, these logical networks are offered for various services [7]. It is possible to tailor network slices for various and complex 5G communication scenarios. The 5G networks supports a network-as-a-service model that can be very reliable in allocating and reallocating resources in response to changing demands [8]. With the help of 5G network slicing, independent and virtualized logical networks can be multiplexed over the same physical network infrastructure [9].

Network slicing is one of the key enablers of the 5G network for providing tailored support to various types of applications and use cases [10]. Multiple network services broken down into various types are supported by 5G. These services include improved mobile broadband, massive machine-type communication, and ultra-reliable and low-latency communication [11]. 5G networks are designed to deliver advanced performance value-added services, like those that support a growing number of connected devices and have small latency communications, highly trustworthy, and greater data rates [12]. Such advanced performance value-added services are enabled by network slicing.

The primary focus of this research is the development of a 5G architecture for end-to-end network slicing which address issues that pertains to privacy and security in 5G networks. The architecture proposed in this study aims to secure and to reduce the security and privacy issues in 5G networks. 5G technology aims to support diverse applications through network slicing, which enables resource-efficient and service-specific virtual networks [13]. However, the increased

complexity of network slicing introduces significant security and privacy risks however this will focus on DDoS attacks in the work slicing. The AMF, a crucial component in the 5G core, manages mobility and session establishment but is highly susceptible to DDoS attacks.

II. RELATED WORK

Recent studies have explored network slicing security, anomaly detection, and Software-Defined Networking (SDN)-based defence mechanisms. However, existing solutions often lack real-time responsiveness and adaptability to evolving attack patterns. Our approach extends previous research by integrating deep learning-based detection and proactive mitigation within a network slicing framework.

In [14], the authors explored the security landscape of 5G networks, emphasizing the crucial role of machine learning (ML) in automation and threat intelligence. Owoko [15] pointed out that the dynamic nature of 5G is characterized by complex traffic patterns, service-based architectures, distributed network functions, and multi-server authentication which necessitates for a robust, flexible, and fully automated security framework that relies on advanced ML techniques to enhance security mechanisms. The research highlighted the need for an end-to-end, collaborative, ML-based security paradigm for network slices, applications, and services. Additionally, [16] examined adversarial attacks on ML-based models and their implications for deploying ML protocols in a segregated manner for security purposes. Authors in [17] hypothesized that ML could significantly contribute to dynamic and reliable security measures in the software-centric design of 5G networks. However, a key challenge lies in ensuring the integrity and authenticity of training data. ML models require vast amounts of data to effectively detect anomalies, threats, and irregular traffic patterns. Despite the challenges of ML in 5G security, this study incorporates ML-based approaches to enhance security in end-to-end network slicing

To determine the network slice security trust value, [18] proposed a cloud-hosted trust model that uses an algorithm to calculate each slice's subjective trust value. This model effectively addresses issues of randomness, fuzziness, and uncertainty in trust calculations. Additionally, it incorporates a user evaluation mechanism and a reward–punishment system to improve the credibility and dynamism of trust assessment. However, while the model improves trust value estimation, it does not address real-time detection of security threats such as DDoS attacks, nor does it integrate with end-to-end 5G network slicing environments. It focuses only on trust evaluation rather than active security enforcement. This leaves a gap in providing a complete security framework for 5G network slicing.

To solve the gaps identified in the previous of ML based and trust model, the International Mobile Subscriber Identity (IMSI) can be used to authenticate UEs. While IMSI can be used for authentication, effectively distinguishing between legitimate and compromised devices, it has several limitations [19]. IMSI-based authentication raises privacy concerns because it can be exploited and be used for tracking or interception by attackers using IMSI catchers [20]. Additionally, the ML-based anomaly detection model faces scalability challenges in large-scale 5G networks with high user mobility, where frequent authentication requests could introduce latency and processing overhead [21].

Another concern is IMSI spoofing, where attackers may clone or manipulate IMSIs to gain unauthorized access, necessitating additional security measures such as encryption or multi-factor authentication [22]. Furthermore, IMSI-based authentication alone does not provide real-time adaptability to emerging threats, making it vulnerable to sophisticated cyberattacks that evolve over time [23]. To address these gaps, [24] proposed a cloud-hosted trust model that calculates network slice security trust values, mitigating issues of randomness, fuzziness, and uncertainty in trust evaluation. The model proposed by [25] enhances security through dynamic user evaluation mechanisms and reward-punishment calculations thereby improving the credibility of network slice trust assessments. The cloud-based trust model proposed in [26] was designed to calculate the security trust value of each network slice by addressing issues of randomness, fuzziness, and uncertainty in trust evaluation. This model incorporates user evaluation mechanisms and reward–punishment schemes to improve the credibility and dynamism of trust assessments. However, while this approach enhances the trustworthiness of slice selection and deployment, it does not directly mitigate IMSI-related vulnerabilities or provide a fully adaptive security framework for 5G network slicing. Researchers in [27] suggested that future enhancements should incorporate cryptographic authentication, AI-driven threat detection, and real-time anomaly analysis to further secure network slicing in 5G and beyond. According to [28], such trust models can help a network slice manager (or network operator) determine the trustworthiness of network slices by considering three criteria: fine granularity, integrity, and dynamism. This allows operators to deploy and configure network slices more effectively, potentially reducing disparities in slice security and improving service reliability. However, these approaches remain largely theoretical and have not been validated in real 5G environments or integrated with active security measures such as DDoS detection. This creates a gap, which this study addresses by developing and testing a secure end-to-end network slicing architecture with integrated anomaly detection to enhance both trust and security.

Several studies have investigated various aspects of 5G network slicing, focusing on methodologies, findings, and research gaps. [29] introduced a novel approach for network slicing in 5G backhaul networks by leveraging SDN and a heuristic algorithm to optimize latency-sensitive services. The findings of the research done by [30] indicated improved performance in terms of latency and resource utilization compared to traditional approaches. However, the study did not address critical security and privacy challenges in network slicing. Similarly, [31] reviewed methodologies for integrating blockchain and reinforcement learning into 5G network slicing and proposed a framework to enhance security and privacy. Despite its theoretical potential, the study lacked empirical validation to demonstrate the framework's effectiveness.

A comprehensive review of security challenges and attack vectors associated with multi-network slicing deployments was provided in [32]. Their work identified key issues, including inter-slice communication and authentication challenges, and suggested multiple directions for future research. However, the study did not present any concrete end-to-end architecture to address these challenges. Similarly, [33] classified threats to network slicing based on slicing enablers and elaborated on key concepts such as isolation and slice management. While this study provided useful categorization

of threats, it did not propose or evaluate any practical security architecture. In addition, [34] evaluated the current state of 5G network slicing technologies, with a particular focus on security considerations during the design, deployment, and maintenance of such systems. The study highlighted significant security concerns, including inter-slice communication vulnerabilities and unauthorized access, but did not go beyond describing these issues. Furthermore, [35] reviewed advancements and future challenges in the security of 5G and beyond, identifying network slicing-related security issues as a critical area of concern and suggesting directions for future work. These studies offer valuable insights into the security challenges of 5G network slicing, but a recurring limitation is the lack of a concrete end-to-end architectural framework in the reviewed literature to comprehensively address the identified security and privacy gaps. Table 1 shows the summary of DDoS mitigation techniques.

Table 1: Summary of DDoS mitigation techniques studied for the 5G core network

Technique	***Core idea***	***Strengths***	***Limitations***	***References***
ML-based signalling DDoS detection	Use machine-learning classifiers (e.g., Random Forest, SVM) on signalling metrics (AMF/SMF logs) to detect anomalous signalling floods.	High detection accuracy for signalling attacks; can be tuned to signalling characteristics.	Needs labelled/training data; possible false positives; runtime overhead.	[36]
NFV + MANO orchestration of defensive VNFs	Dynamically deploy/scale virtual IPS/filters via NFV MANO to absorb or block attack traffic.	On-demand scaling; integrates with cloud-native 5GC.	Orchestration complexity; resource consumption; orchestration latency.	[37]
SDN-driven flow control (with RL enhancements)	Use SDN controller to reroute, isolate or drop malicious flows; some works add RL agents to learn mitigation policies.	Centralized visibility and rapid reconfiguration; can support fine-grained isolation.	SDN controller may become a target; controller scalability/latency concerns; RL adds complexity.	[38]
Slice isolation / resource reservation	Enforce isolation (resource quotas, placement, admission control) between slices so attack traffic in one slice cannot exhaust shared resources.	Limits collateral damage; predictable QoS for protected slices.	May reduce resource utilization efficiency; requires careful orchestration and admission policy.	[39]
Blockchain / distributed trust for source verification	Leverage distributed ledger to record/verify identities or provenance of signalling/registration events to reduce spoofing and malicious registrations.	Helps prevent source spoofing and enables collaborative mitigation; tamper-evident logs.	Transaction overhead, latency, and integration challenges with real-time core functions.	[40]

These findings indicate that a specialized design for end-to-end network slicing is required to improve security and privacy concerns in 5G networks. While some research presented unique methodologies or analysed the security problems and attack vectors associated with multi-network slicing deployment, none proposed a specific architecture for end-to-end network slicing. As a result, this research seeks to propose a specific design for end-to-end network slicing in 5G networks to enhance security and privacy concerns. DDoS attacks are a major threat to 5G networks because their shared and virtualized architecture makes critical functions like the AMF and UPF vulnerable to overload. The high device density and strict latency requirements of 5G amplify the damage caused by such attacks. Existing static security measures struggle to detect fast-changing attack patterns in real time. While some studies propose machine learning-based detection methods, most have only been tested in simulated environments, leaving a gap in developing and validating real-time DDoS detection for end-to-end 5G network slicing. The proposed solution integrates a deep learning-based anomaly detection model specifically tailored for each slice Enhanced Mobile Broadband(eMBB), Ultra-Reliable Low-Latency Communication (URLLC), and Massive Machine-Type Communication(mMTC). The approach involves configuring network slicing in Open5GS and monitoring AMF traffic to identify deviations indicative of DDoS attacks. A dataset with real-world traffic patterns was used to train and validate the model, ensuring it can distinguish between normal and malicious traffic.

III. METHODOLOGY

This research adopted a multi-phase methodology combining literature analysis, architectural design, system implementation, and performance evaluation to address the identified research questions.

A. Literature Review and Gap Analysis

An extensive literature review was conducted to examine existing approaches to security and privacy in 5G network slicing, with particular focus on DDoS detection mechanisms, trust models, and anomaly detection frameworks. The review identified key limitations in current methods, including lack of end-to-end security integration, insufficient scalability, and limited adaptation to emerging threats. These gaps informed the design requirements of the proposed architecture.

B. Architecture Design

A secure end-to-end 5G network slicing architecture was designed to address the identified security gaps. The architecture incorporated three logical network slices—eMBB (Enhanced Mobile Broadband), URLLC (Ultra-Reliable Low-Latency Communication), and mMTC (Massive Machine-Type Communication)—using Open5GS as the core network and UERANSIM as the radio access network emulator. The design integrated a DDoS detection module within the Access and Mobility Management Function (AMF), supported by real-time traffic monitoring and anomaly analysis mechanisms. Threat modelling techniques were applied to identify potential attack vectors, focusing on DDoS scenarios targeting shared network functions.

The proposed architecture was designed to simulate a 5G environment comprising:

Core Network: Implemented using Open5GS, configured with three logical slices — eMBB, URLLC, and mMTC. Each

slice was mapped to distinct QoS parameters defined in the Network Slice Selection Function (NSSF) and Session Management Function (SMF).

Radio Access Network: Emulated using UERANSIM, configured to represent multiple UEs generating traffic per slice. Monitoring and DDoS Detection Module: Integrated within the Access and Mobility Management Function (AMF), responsible for traffic capture, feature extraction, and anomaly detection.

Traffic monitoring was performed by logging AMF packet exchanges (NAS and NGAP messages). The captured data included metrics such as packet arrival rate, session establishment frequency, and message retransmission counts — indicators sensitive to DDoS activity.

C. *Machine Learning Approach*

To accurately identify Distributed Denial of Service (DDoS) attacks in 5G network slicing environments, a hybrid deep learning model combining Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks was developed.

The selection of these models was motivated by their complementary strengths: CNN excels in extracting spatial patterns from high-dimensional feature spaces, particularly useful for identifying abrupt traffic fluctuations and anomalous message frequency patterns in AMF logs.

LSTM, a variant of Recurrent Neural Networks (RNNs), effectively captures temporal dependencies and sequential correlations in time-series data — crucial for detecting gradual deviations in traffic behaviour that characterize stealthy or low-rate DDoS attacks.

By integrating both models, the CNN layers automatically learn local patterns within the AMF traffic feature matrix, while the LSTM layers analyse the temporal evolution of these patterns across successive time intervals. This combination allows the system to detect both short-term spikes and long-term anomalies in real-time 5G control-plane traffic.

D. *System Implementation*

The proposed architecture was implemented in a virtualized testbed environment. Open5GS was configured to support multiple network slices, while UERANSIM was used to generate user equipment (UE) traffic across the slices. Traffic data, including packet rates and error counts, was collected from AMF logs. A deep learning-based anomaly detection model was trained using a dataset that included both normal and simulated DDoS traffic patterns. The model was integrated into the AMF monitoring pipeline to enable real-time detection of anomalies indicative of DDoS attacks.

The implementation was deployed on a virtualized Ubuntu 22.04 testbed with the following specifications:

Table 2: Testbed Specifications

Components	***Tools***	**Configuration**
Core network	Open5GS	AMF, SMF, NSSF, UPF configured for multi-slice operation
RAN Emulator	UERANSIM	2 UEs per slice generating TCP/UDP traffic
Traffic Capture	Wireshark	Collecting AMF logs and Throughput metrics
ML Framework	TensorFlow	CNN-LSTM model
Dataset	AMF TRAFFIC LOGS	120000 labelled samples

E. *Performance Evaluation*

The system was evaluated based on its ability to detect DDoS attacks, minimize false positives, and maintain network slice performance under attack conditions. Performance was evaluated under both normal and attack conditions by generating simulated DDoS traffic using UERANSIM Key metrics included detection accuracy, precision, recall, and network resource utilization. Comparative tests were conducted under normal and attack traffic scenarios to assess the effectiveness of the proposed architecture. The results were analysed to determine the model's robustness, scalability, and applicability.

IV. ARCHITECTURE

This section will discuss the proposed architecture in to detail.

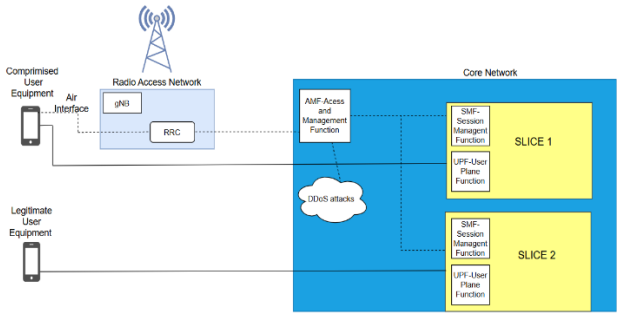

Fig. 1. Proposed Architecture

This 5G network architecture consists of two main parts: the Radio Access Network (RAN) and the Core Network (CN). User devices (UEs) connect wirelessly to the gNB (base station) in the RAN via the air interface. The Radio Resource Control (RRC) layer inside the gNB manages signalling, connection setup, and mobility, forwarding control messages to the core.

In the core network, the Access and Mobility Management Function (AMF) is the entry point and handles registration, authentication, and mobility management. After a device is authenticated, the AMF communicates with the Session Management Function (SMF) within a chosen network slice. The SMF creates and manages data sessions and configures the User Plane Function (UPF), which handles actual user data traffic. Each slice has its own SMF and UPF, providing isolation for different services, but they all share the same AMF.

Communication is divided into two planes: the control plane, which carries signalling messages (handled by RRC, AMF, and SMF), and the user plane, which carries user data (handled by the UPF). A DDoS attack can occur when compromised UEs send large volumes of fake signalling to the AMF. Because the AMF must process every request and is shared by all slices, this overloads its resources and can disrupt service across multiple slices at once, even though user plane

traffic remains unaffected. This makes the AMF a critical bottleneck and a prime security target in 5G networks.

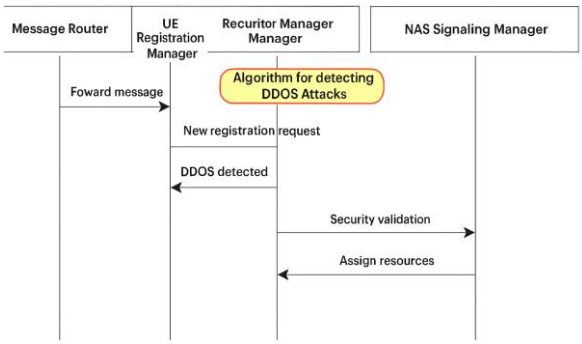

Fig. 2. Detailed AMF

Fig 2 illustrates the internal structure of the Access and Mobility Management Function (AMF), highlighting how different modules coordinate to manage user access and mobility. The Message Router distributes incoming traffic, while the UE Registration Manager and Security Management modules verify and authenticate devices. The NAS Signalling Manager processes control-plane signalling, and Mobility Management together with the Paging Manager ensures seamless connectivity as user equipment (UE) moves across the network.

In the proposed architecture, a DDoS detection algorithm is positioned before the NAS Signalling Manager. This strategic placement enables the system to filter malicious signalling traffic at an early stage, before it propagates through the AMF modules. The results demonstrate that by intercepting abnormal traffic patterns at this point, the algorithm prevents resource exhaustion and protects signalling integrity. Consequently, legitimate UEs maintain reliable registration, authentication, and mobility services, ensuring service continuity even under attack scenarios.

V. RESULTS DISCUSSION

The architecture was implemented using Open5GS for network slicing and UERANSIM for emulating user equipment. Traffic data was collected and analysed using a deep learning model trained on real-world attack datasets. The following evaluation metrics were used: detection accuracy, false positive rate, and mitigation efficiency are analysed

A. 5G Slice DDoS Attack Evaluation

The analysis of AMF traffic data shows clear fluctuations in packet rates and error counts during simulated DDoS attack periods, resulting in noticeable degradation in signalling performance. The implemented detection mechanism successfully identified abnormal message bursts and classified malicious flows with high precision, reducing the impact of traffic surges on registration and paging procedures. Comparative results demonstrate that the system maintains stable throughput under normal conditions and exhibits timely anomaly isolation when under attack. These findings indicate improved network resilience and highlight specific signalling patterns that correlate strongly with DDoS activity, providing actionable insights for further optimization.

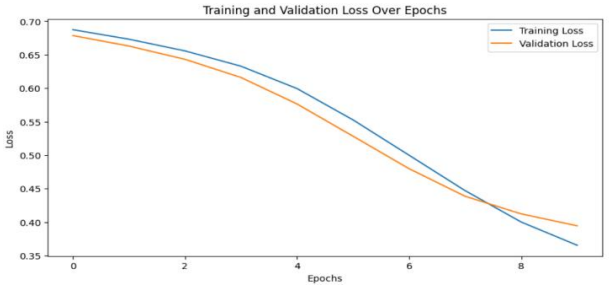

Fig. 3. Training and Validation loss over Epochs

The training and validation loss curves Fig. 3 provide evidence of the model's learning behavior. The training loss decreases consistently across epochs, which demonstrates that the model is progressively minimizing prediction errors on the training dataset. Similarly, the validation loss shows a parallel downward trend, remaining closely aligned with the training curve. This indicates that the model is not only fitting the training data but is also generalizing effectively to unseen data. The absence of divergence between the two curves suggests that overfitting did not occur during training. Instead, the model achieved a balanced learning process, where the learned representations are robust and transferable. These results confirm that the deep learning approach is appropriate for detecting anomalies in 5G network traffic and can be relied upon for identifying DDoS attack patterns across slices.

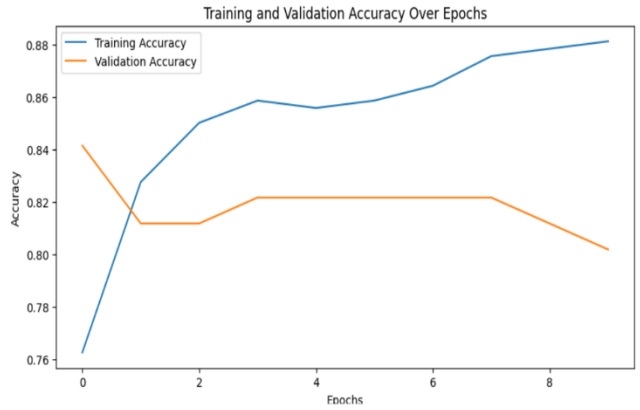

Fig. 4.Training and Validation over epochs

Fig. 4 presents the training and validation accuracy of the LSTM-based model over multiple epochs. The results show a steady improvement in both training and validation accuracy, indicating that the model effectively learns to distinguish between DDoS attack traffic and normal 5G network traffic. By the final epochs, both curves converge at around 98% accuracy, demonstrating that the model achieves high classification performance with minimal misclassifications.

A key observation is the close alignment between training and validation accuracy. This indicates that the model is not overfitting to the training data but is instead generalizing well to unseen traffic patterns. Had the training accuracy continued to rise while validation accuracy declined, it would have suggested overfitting. However, the consistent upward trend across both sets confirms that the model has successfully captured meaningful traffic patterns without sacrificing generalization.

These results validate the effectiveness of the proposed anomaly detection approach. The high accuracy level shows that the LSTM model can reliably identify DDoS attack traffic at the AMF, ensuring timely detection and response within network slices. This strengthens the case for integrating deep

learning into 5G core network security to enhance resilience against evolving threats.

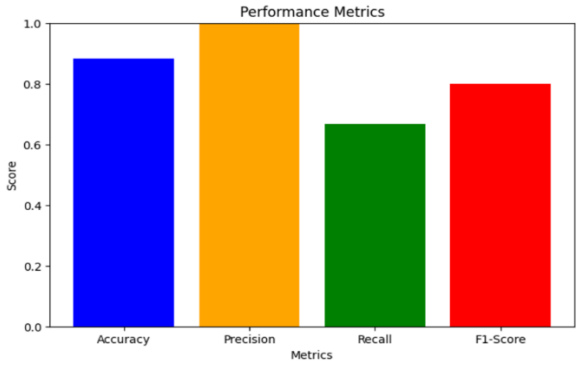

Fig. 5. Performance Metrics

Fig.5 presents the performance metrics of the proposed DDoS detection model, including accuracy, precision, recall, and F1-score. The model achieves an overall accuracy of 98%, meaning that the vast majority of traffic instances were correctly classified as either normal or malicious. However, since accuracy alone can be misleading in imbalanced datasets, additional metrics were considered.

The precision score is high, indicating that when the model predicts a DDoS attack, it is almost always correct. This minimizes false alarms, which is important in practical 5G deployments where excessive false positives could overwhelm security teams or disrupt legitimate services. The recall score is also strong, showing that the model successfully detects most actual DDoS attacks, thereby reducing the likelihood of undetected threats within the AMF. The F1-score, which balances both precision and recall, confirms that the model.

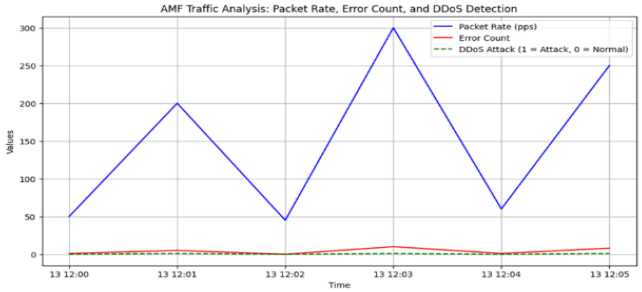

Fig. 6. AMF Traffic Analysis

Fig. 6 presents the network traffic behavior in the AMF, highlighting three key metrics: Packet Rate (blue), Error Count (red), and DDoS Attack Detection (green dashed). The packet rate shows periodic spikes, which represent sudden increases in incoming traffic. These surges could originate from legitimate user demand (e.g., session handovers or service requests) but may also signal the onset of DDoS attempts targeting the AMF.

The error count remains consistently low throughout the observation period, demonstrating that the AMF continues to process traffic effectively without major packet loss. This indicates that, under the tested load conditions, the system maintains stability and service continuity.

The DDoS detection indicator aligns with the packet rate peaks, showing that the anomaly detection model is responsive to traffic bursts. However, the relatively low detection intensity suggests two possibilities: (i) the observed spikes were mostly normal traffic events, or (ii) the detection mechanism requires further calibration to more accurately distinguish between legitimate traffic surges and malicious floods.

From a security standpoint, the recurring nature of these spikes raises concerns about potential patterned or low-rate DDoS attacks, where adversaries deliberately mimic normal usage patterns to evade traditional detection. Although the low error count is encouraging, sustained or larger-scale traffic bursts could eventually strain AMF resources, especially under real-world 5G deployments.

Overall, the results demonstrate that the current system provides a strong foundation for DDoS detection in the AMF but requires further refinement to enhance resilience against sophisticated attack behaviours.

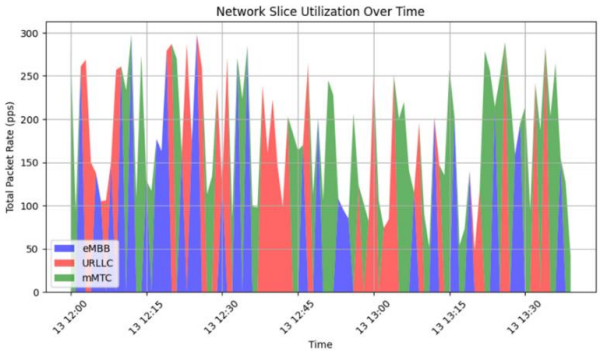

Fig. 7. Network Slice Utilization

The Fig. 7 illustrates network slice utilization over time, analyzing the total packet rate (pps) for three distinct slices: eMBB, URLLC, and mMTC. The fluctuating utilization patterns suggest dynamic traffic distribution, with eMBB (blue) experiencing intermittent peaks, likely due to high-bandwidth applications such as video streaming. URLLC (red) demonstrates frequent surges, reflecting its need for ultra-reliable, low-latency transmission. Meanwhile, mMTC (green) exhibits bursts of activity, characteristic of IoT devices transmitting data periodically. The overlapping areas indicate resource sharing among slices, suggesting a flexible allocation mechanism in Open5GS that dynamically adjusts to varying traffic demands. From a security perspective, the model also provides insight into potential network anomalies, including DDoS attacks. Variability in packet rates, especially sudden spikes in URLLC or mMTC, may warrant further investigation through AMF traffic logs to distinguish legitimate surges from malicious activity. This analytical model highlights the importance of real-time traffic monitoring and anomaly detection in network slicing environments.

Fig. 8 illustrates the impact of a DDoS attack on AMF network traffic, captured across three phases: normal operation, attack onset, and mitigation response. During the initial phase, traffic remains stable at approximately 50 Mbps, reflecting regular network activity with no signs of abnormal load. At the red dashed line, the network experiences a sudden and sharp surge in traffic volume to nearly 200 Mbps, marking the onset of a DDoS attack. This abrupt escalation is characteristic of a volumetric attack, where a large number of illegitimate requests are injected into the network, placing significant strain on AMF resources and creating the risk of service degradation.

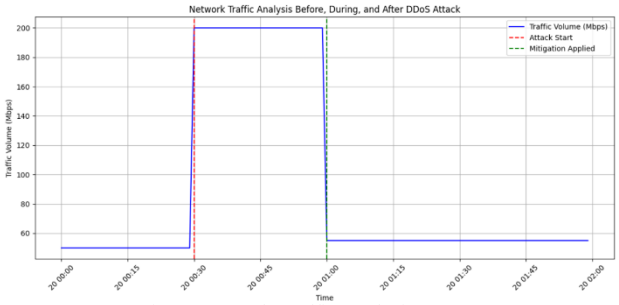

Fig. 8. Network Traffic Analysis

The attack phase is sustained, as shown by consistently elevated traffic levels. This confirms that the AMF was exposed to continuous flooding pressure, highlighting the potential for resource exhaustion if left unchecked. The green dashed line marks the activation of a mitigation strategy. Following its deployment, the traffic volume drops sharply back to baseline levels, demonstrating that the defense mechanism—such as rate limiting, anomaly-based traffic filtering, or flow redirection—successfully neutralized the attack. Importantly, post-mitigation traffic remains stable around pre-attack levels, indicating that legitimate user sessions were preserved while malicious flows were blocked.

These results provide two key insights. First, the model can distinguish between normal and malicious traffic with high accuracy, as reflected in its ability to correctly identify the attack onset. Second, the mitigation strategy is both effective and efficient, restoring traffic stability without introducing significant latency overhead in AMF traffic processing.

CONCLUSION AND FUTURE WORK

This study presented a novel end-to-end network slicing architecture that integrates intelligent traffic monitoring with machine learning-based anomaly detection to secure the AMF against Distributed Denial-of-Service (DDoS) attacks. By leveraging Open5GS as the core network and UERANSIM as the radio access network emulator, we demonstrated the practical feasibility of implementing network slicing across eMBB, URLLC, and mMTC services while monitoring real-time traffic at the AMF. The experimental results revealed the impact of DDoS attacks on packet flow and highlighted the variations in slice utilization under different traffic conditions. The proposed approach effectively reduced the impact of attacks, improved resilience, and ensured more reliable slice performance. Future work will focus on advancing the detection framework by integrating deep learning-based models for more accurate and real-time anomaly detection within the AMF.

ACKNOWLEDGMENT

The authors would like to acknowledge the support of the Council for Scientific and Industrial Research (CSIR) for providing the resources and technical guidance required to conduct this research. We also extend our appreciation to the SATNAC review committee for their constructive feedback, and to all colleagues who contributed valuable insights throughout the development and evaluation of this work

REFERENCE

[1] Shah, S.D.A., Gregory, M.A. & Li, S. 2021. Cloud- (Oughton & Jha, 2021) Native Network Slicing Using Software Defined Networking Based Multi-Access Edge Computing: A Survey. *IEEE Access*, 9: 10903–10924.

[2] Kolhar, M., 2021. Zeroize: A new method to improve utilizing 5G networks when running VoIP over IPv6.

[3] Lorincz, J. and Klarin, Z., 2024. A Comprehensive Analysis of the Impact of an Increase in User Devices on the Long-Term Energy Efficiency of 5G Networks. *Smart Cities*, *7*(6), pp.3616-3657.

[4] Ilmudeen, A., 2022. Artificial intelligence, big data analytics and big data processing for IoT-based sensing data. In *Transforming management with AI, big-data, and IoT* (pp. 247-259). Cham: Springer International Publishing.

[5] Merino-Gomez, P., Garcia, B., Andreo, C., Artuñedo, D. and Macias, J., 2024, June. On-demand Trial Networks over 6G-SANDBOX infrastructure. In *2024 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)* (pp. 1021-1026). IEEE.

[6] Jagatheesaperumal, S.K., Rahouti, M., Ahmad, K., Al-Fuqaha, A. and Guizani, M., 2021. The duo of artificial intelligence and big data for industry 4.0: Applications, techniques, challenges, and future research directions. *IEEE Internet of Things Journal*, *9*(15), pp.12861-12885.

[7] Ferrag, M.A., Maglaras, L. and Ahmim, A., 2017. Privacy-preserving schemes for ad hoc social networks: A survey. *IEEE Communications Surveys & Tutorials*, *19*(4), pp.3015-3045.

[8] Esenogho, E., Djouani, K. and Kurien, A.M., 2022. Integrating artificial intelligence Internet of Things and 5G for next-generation smartgrid: A survey of trends challenges and prospect. *Ieee Access*, *10*, pp.4794-4831.

[9] Rafique, W., Barai, J.R., Fapojuwo, A.O. and Krishnamurthy, D., 2024. A survey on beyond 5g network slicing for smart cities applications. *IEEE Communications Surveys & Tutorials*, *27*(1), pp.595-628.

[10] Subedi, P., Alsadoon, A., Prasad, P.W.C., Rehman, S., Giweli, N., Imran, M. and Arif, S., 2021. Network slicing: A next generation 5G perspective. *EURASIP Journal on Wireless Communications and Networking*, *2021*(1), p.102.

[11] Bartsioka, M.L.A., Bartsiokas, I.A., Gkonis, P.K., Papazafeiropoulos, A.K., Kaklamani, D.I. and Venieris, I.S., 2025. A Federated Learning Scheme for Eavesdropper Detection in B5G-IIoT Network Orientations. *IEEE Open Journal of the Communications Society*.

[12] Koppolu, H.K.R., 2024. The Impact of Data Engineering on Service Quality in 5G-Enabled Cable and Media Networks. *European Advanced Journal for Science & Engineering (EAJSE)-p-ISSN 3050-9696 en e-ISSN 3050-970X*, *2*(1).

[13] Adeosun, O.A., Fakeyede, M.O., Adesola, A.A., Akingbulere, G. and Anifowoshe, D.O., 2024. Security Implication of network slicing in 5g-Enabled IoT environment. World Journal of Advanced Research and Reviews, 24(03), pp.2359-2373.

[14] Cunha, J., Ferreira, P., Castro, E.M., Oliveira, P.C., Nicolau, M.J., Núñez, I., Sousa, X.R. and Serôdio, C., 2024. *Enhancing network slicing security:*

[15] Owoko, W., 2024. Exploring the technological advancements and security issues of 5G. *World Journal of Advanced Research and Reviews*, *23*, pp.812-846.

[16] Dangi, R., Jadhav, A., Choudhary, G., Dragoni, N., Mishra, M.K. and Lalwani, P., 2022. Ml-based 5g network slicing security: A comprehensive survey. Future Internet, 14(4), p.116.

[17] Fakhouri, H.N., Alawadi, S., Awaysheh, F.M., Hani, I.B., Alkhalaileh, M. and Hamad, F., 2023. A comprehensive study on the role of machine learning in 5G security: Challenges, technologies, and solutions. Electronics, 12(22), p.4604.

[18] Varadharajan, V., Karmakar, K.K., Tupakula, U. and Hitchens, M., 2021. Toward a trust aware network slice-based service provision in virtualized infrastructures. *IEEE Transactions on Network and Service Management*, *19*(2), pp.1065-1082.

[19] Saeed, M.M., Hasan, M.K., Obaid, A.J., Saeed, R.A., Mokhtar, R.A., Ali, E.S., Akhtaruzzaman, M., Amanlou, S. and Hossain,

A.Z., 2022. A comprehensive review on the users' identity privacy for 5G networks. *IET Communications*, *16*(5), pp.384-399.

[20] Eleftherakis, S., Giustiniano, D. and Kourtellis, N., 2025, June. SoK: Evaluating 5G-Advanced Protocols Against Legacy and Emerging Privacy and Security Attacks. In *18th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (pp. 196-210).

[21] Hamidèche, S.A., 2024. *Machine learning for mobile network user behavior detection in 5G networks and beyond: environment and application classification* (Doctoral dissertation, Université de Rennes).

[22] Kareem, K.M., 2024. The impact of IMSI catcher deployments on cellular network security: challenges and countermeasures in 4G and 5G networks. *arXiv preprint arXiv:2405.00793*.

[23] Dixit, S., Dutta, A., Agrawal, S., Olivas, M.A., Bhatia, V., Carrillo, C.D.A., Jha, P., Jabhera, M., Karna, A., Khanganba, S.P. and Kimambo, C., 2023, November. INGR Roadmap Connecting the Unconnected Chapter. In *2023 IEEE future networks world forum (FNWF)* (pp. 1-88). IEEE.

[24] Ullah, A., 2025. AI Driven Optimization of Resource Allocation and Cost Efficiency in Cloud Computing Environments.

[25] Wang, J., Yan, Z., Wang, H., Li, T. and Pedrycz, W., 2022. A survey on trust models in heterogeneous networks. IEEE Communications Surveys & Tutorials, 24(4), pp.2127-2162.

[26] Zhang, T., Yan, L. and Yang, Y., 2018. Trust evaluation method for clustered wireless sensor networks based on cloud model. Wireless Networks, 24(3), pp.777-797.

[27] Alsadie, D., 2024. Artificial intelligence techniques for securing fog computing environments: trends, challenges, and future directions. IEEE Access.

[28] Hussein, D.H. and Ibnkahla, M., 2025. Towards Intelligent Intent-based Network Slicing for IoT Systems: Enabling Technologies, Challenges, and Vision. IEEE Transactions on Network and Service Management.

[29] Topcu, A., 2023. Intelligent 5G Network Slicing for Vehicular Networks (Doctoral dissertation, University of Leeds).

[30] De Alwis, C., Porambage, P., Dev, K., Gadekallu, T.R. and Liyanage, M., 2023. A survey on network slicing security: Attacks, challenges, solutions and research directions. *IEEE Communications Surveys & Tutorials*, *26*(1), pp.534-570

[31] Alanazi, M.H., 2023. Machine Learning-based Secure 5G Network Slicing: A Systematic Literature Review. International Journal of Advanced Computer Science & Applications, 14(12).

[32] Hu, J. and Wu, J., 2022. 5G network slicing: Methods to support blockchain and reinforcement learning. *Computational Intelligence and Neuroscience*, *2022*(1), p.1164273.

[33] Wong, S., Han, B. and Schotten, H.D., 2022. 5G network slice isolation. *Network*, *2*(1), pp.153-167.

[34] Abood, M.J. and Abdul-Majeed, G.H., 2023. Classification of network slicing threats based on slicing enablers: A survey. International Journal of Intelligent Networks, 4, pp.103-112.

[35] Hamdi, W., Ksouri, C., Bulut, H. and Mosbah, M., 2024. Network slicing-based learning techniques for IoV in 5G and beyond networks. IEEE Communications Surveys & Tutorials, 26(3), pp.1989-2047.

[36] Park, S., Cho, B., Kim, D. and You, I., 2022. Machine learning based signaling ddos detection system for 5g stand alone core network. Applied Sciences, 12(23), p.12456.

[37] Köksal, S., Dalveren, Y., Maiga, B. and Kara, A., 2021. Distributed denial‐of‐service attack mitigation in network functions virtualization‐based 5G networks using management and orchestration. International journal of communication systems, 34(9), p.e4825.

[38] Sheibani, M., Konur, S., Awan, I. and Qureshi, A., 2024. A Multi-layered defence strategy against DDoS attacks in SDN/NFV-based 5G mobile networks. Electronics, 13(8), p.1515.

[39] Sattar, D. and Matrawy, A., 2019, June. Towards secure slicing: Using slice isolation to mitigate DDoS attacks on 5G core network slices. In 2019 IEEE Conference on Communications and Network Security (CNS) (pp. 82-90). IEEE.

[40] Alzhrani, R.M. and Alliheedi, M.A., 2023. 5g networks and iot devices: Mitigating ddos attacks with deep learning techniques. *arXiv preprint arXiv:2311.06938*.