Journal of Artificial Intelligence and Capsule Networks (ISSN: 2582-2012)
www.irojournals.com/aicn/

Deep Autoencoder-Based Anomaly Detection for Intelligent Network Slice Monitoring in B5G Networks

Arun Prasad K.[1], Abdul Basith M.[2], Harish Kumar V.[3]

[1]Assistant Professor, [2,3]UG Scholar Department of Information Technology, Jerusalem College of Engineering, Affiliated to Anna University, Chennai, India.

Email: [1]arunprasadchamy@gmail.com, [2]abdulbasithmit2021@jerusalemengg.ac.in, [3]harishkumarvit2021@jerusalemengg.ac.in

Abstract

Anomaly detection in 5G network slicing is critical for ensuring the security and reliability of next-generation telecommunications infrastructure. This study presents a deep autoencoder-based framework for unsupervised anomaly detection in network traffic, leveraging a comprehensive dataset of 210,786 samples with a realistic anomaly rate of 4.5%. The proposed approach incorporates advanced preprocessing techniques, including normalization, interpolation, and oversampling, and prioritizes key network features identified through correlation analysis. The autoencoder model is trained exclusively on normal traffic to learn baseline behaviour, with anomalies detected via reconstruction error analysis. Experimental results demonstrate that the model achieves robust separation between normal and anomalous samples, identifying 1,904 anomalies with a clear margin in reconstruction error statistics. Comparative evaluation with traditional unsupervised methods, such as Isolation Forest, PCA, and One-Class SVM, highlights the superior sensitivity and adaptability of the deep learning approach. The findings underscore the potential of autoencoder-based models for real-time, interpretable anomaly monitoring in highly dynamic and imbalanced 5G

DOI: https://doi.org/10.36548/jaicn.2025.2.002
Received: 31.03.2025, received in revised form: 28.04.2025, accepted: 12.05.2025, published: 23.05.2025

network environments, paving the way for more resilient and intelligent network management solutions.

Keywords: 5G Networks, Network Slicing, Anomaly Detection, Deep Learning, Autoencoder, Network Security.

1. Introduction

The work of deploying fifth-generation (5G) and beyond 5G (B5G) networks throughout various countries marks a key development in telecommunications and combines novel innovations with classic technical problems. Underpinning this advance is network slicing, which is a game-changing technology that allows operators to create multiple distinct virtual networks on a shared physical foundation. This strategy facilitates application-centric connectivity for a wide range of use cases, ranging from industrial automation to consumer-facing services, providing an unparalleled level of adaptability. Nevertheless, it continues to be a challenge to meet a constant level of reliability and performance across these slices, as their success depends on dynamic resource allocation. These slices function independently and are tailored for specific needs: ultra-reliable low-latency communication (URLLC) slices are critical for applications requiring minimal delays, such as autonomous vehicles, while massive machine-type communication (mMTC) slices are the backbone of a smart city ecosystem where thousands of devices with diverse bandwidth and latency requirements are interconnected. These use cases also echo the dual promise and complexity of 5G/B5G networks, where there is tension and a need to balance flexibility with robustness to unlock their full potential.

Real-time anomaly detection becomes increasingly critical to ensure the overall safety of the network as B5G networks evolve. In this case, wall-eyed monitoring techniques fail hard since they cannot control the scalability and complexity of network slices. As a result, the adoption of advanced methodologies, including machine learning and deep learning, is essential.

2. Related Work

The rapid evolution of 5G and beyond networks has introduced new paradigms in network management, security, and anomaly detection, particularly in the context of network slicing. Numerous studies have addressed the challenges and opportunities associated with

securing 5G network slices and ensuring reliable service delivery in multi-tenant environments. Singh et al. [1] and De Alwis et al. [2] provide comprehensive overviews of security concerns in 5G network slices, highlighting the necessity for robust, adaptive anomaly detection mechanisms to counteract sophisticated threats and maintain service integrity.

Recent literature has increasingly focused on leveraging machine learning and deep learning for intelligent network management and anomaly detection. Yeh et al. [3] and Liu & Chou [5] explore the application of deep learning and reinforcement learning for automated network slicing and management, demonstrating the potential for these techniques to enhance network adaptability and resilience. Javadpour et al. [4] specifically address slice isolation using reinforcement learning to mitigate DDoS attacks, underscoring the importance of dynamic, data-driven approaches in safeguarding network resources.

In the domain of anomaly detection, several works have proposed advanced models tailored for 5G environments. Maimo et al. [16] introduce a self-adaptive deep learning-based system for anomaly detection, which dynamically adjusts to evolving network conditions and demonstrates strong performance in highly dynamic scenarios. Trappolini et al. [19] present a quantized autoencoder-based approach for multivariate time series anomaly detection in 5G networks, achieving high detection accuracy and operational efficiency. Similarly, Zheng et al. [20] propose TransKS, a deep learning-based method utilizing adaptive sliding windows for detecting anomalies in telecommunication networks, further validating the effectiveness of deep architectures in this context.

Comparative studies, such as those by Dangi et al. [10] and Rafique et al. [7], systematically review machine learning-based anomaly detection techniques, emphasizing the superiority of deep learning models, particularly autoencoders and generative adversarial networks (GANs), in capturing complex, non-linear patterns in network traffic. Park et al. [17] demonstrate the use of GANs for enhanced network intrusion detection, achieving improved detection rates over traditional methods.

Feasibility studies and real-world deployments are also well-represented in the literature. Chirivella-Perez et al. [6] and Wijethilaka & Liyanage [8] discuss end-to-end network slice management frameworks and the role of security orchestrators, respectively, providing practical insights into the integration of anomaly detection systems within operational 5G networks. Sui et al. [18] present a real-time hidden anomaly detection system

based on random matrix theory, showcasing the feasibility of deploying advanced detection algorithms in live wireless environments. These studies collectively affirm that deep learning-based anomaly detection frameworks are not only theoretically sound but also practically viable for real-time, scalable deployment in 5G and beyond networks.

Our work builds upon these foundational studies by implementing a deep autoencoder-based anomaly detection framework specifically tailored for 5G network slicing environments. Unlike prior approaches that often focus on either simulated datasets or limited feature sets, our methodology leverages a large-scale, publicly available dataset with realistic anomaly rates and incorporates advanced preprocessing, feature selection, and dynamic thresholding. The comparative evaluation with traditional unsupervised models, as well as the operational integration demonstrated through a real-time monitoring dashboard, further distinguishes our contribution. By aligning with and extending the findings of recent literature, our approach demonstrates both high detection accuracy and practical feasibility, paving the way for more resilient and intelligent network management solutions in next-generation telecommunications.

3. Proposed Work

Our proposed approach presents an intelligent anomaly detection framework specifically designed for the complex and dynamic environment of Beyond 5G (B5G) network slicing. Central to this framework is a deep autoencoder model that employs a symmetric encoder-decoder architecture. This design is particularly well-suited to handle the high-dimensional and heterogeneous nature of network traffic data generated across various slices. The encoder compresses this multidimensional input into a more compact latent representation, distilling only the most significant features that capture normal network behavior. The decoder then attempts to reconstruct the original input from this compressed form. By comparing the original and reconstructed inputs, the model identifies deviations known as reconstruction errors, which serve as indicators of anomalous activity.

What distinguishes our approach from traditional models is the introduction of a dynamic, context-aware thresholding mechanism. Rather than relying on a fixed threshold, which can be brittle in fluctuating network conditions, our system adapts in real-time by analyzing usage patterns, entropy levels, and historical performance data. This adaptability is

critical in maintaining high detection accuracy and minimizing false alarms, especially in environments characterized by unpredictable traffic loads and performance spikes.

To enhance the utility of the framework, we have integrated a multi-layered architecture that includes a detection and alert module capable of classifying anomalies by severity. For instance, the system can distinguish between low-risk issues, such as temporary performance degradation, and more critical threats like Distributed Denial of Service (DDoS) attacks. These alerts are promptly communicated to administrators through an interactive dashboard interface, which also supports real-time monitoring and historical trend analysis. The dashboard is equipped with visual tools such as heatmaps and anomaly timelines, empowering operators to interpret network behavior intuitively and take proactive measures when needed.

Furthermore, the architecture is built with scalability and adaptability in mind. As the network evolves and more labeled data becomes available, the autoencoder can be fine-tuned to improve its ability to distinguish between benign irregularities and genuine threats. The framework is also extensible, with potential support for advanced enhancements such as ensemble models or reinforcement learning-based threshold optimization. Together, these components form a comprehensive system that not only identifies anomalies with high precision but also supports continuous learning, situational awareness, and timely intervention capabilities essential for safeguarding mission-critical services in modern B5G networks.

3.1 Architecture Overview

The proposed anomaly detection system is designed to intelligently monitor B5G network slices using a deep learning-based approach. The system architecture consists of six interconnected modules, each performing a specific task in the end-to-end detection pipeline:

- **Data Collection & Preprocessing**

Network slice metrics such as bandwidth, jitter, delay, throughput, and packet loss are continuously collected from the obtained dataset of network configurations. The data is cleaned, handles missing values and normalized. Feature engineering techniques are also applied to improve model performance.

- **Autoencoder Model**

A deep symmetric autoencoder is trained on normal traffic to learn the latent representation of standard behavior. The encoder compresses input data into a low-dimensional latent space, and the decoder reconstructs the input from this representation.

- **Dynamic Thresholding**

Instead of using a static anomaly threshold, we compute adaptive thresholds based on statistical properties (e.g., mean, standard deviation) of the reconstruction error, which improves robustness across varying network conditions.

- **Anomaly Detection**

Once trained, the model processes test traffic data. If the reconstruction error exceeds the dynamic threshold, the system flags it as an anomaly.

- **Alerting and Visualization Dashboard**

A user-friendly dashboard displays time-series trends, reconstruction errors, active alerts, and performance metrics for system administrators.

- **Model Fine-Tuning**

The model is periodically retrained or fine-tuned with new traffic data to adapt to evolving traffic patterns and reduce false positives.

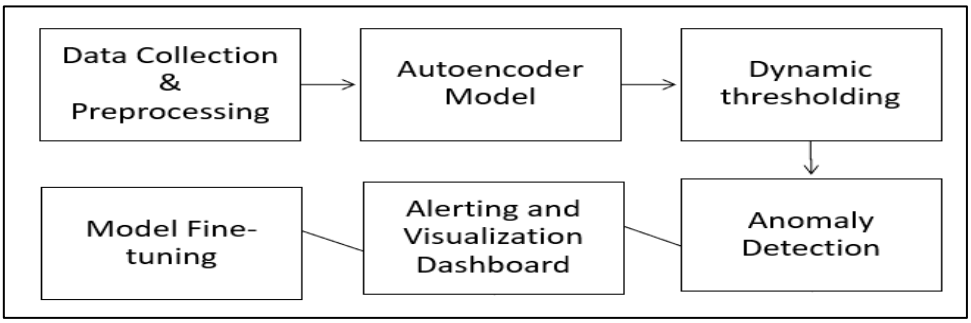

Figure 1. Architecture Diagram

3.2 Dataset and Implementation Details

We employed the publicly available network slicing dataset by Farreras et al. (2024), published on Zenodo (DOI: 10.5281/zenodo.10610616). The original dataset contains 8,000

distinct network configurations. For our experiments, we selected a representative subset of 1,000 configurations, which yielded a total of 210,786 samples. This approach ensured a diverse yet computationally manageable dataset for model training and evaluation. Of these samples, only 24 are labeled as anomalies, presenting a significant class imbalance that reflects real-world network conditions.

To address this imbalance and ensure data quality, we performed the following preprocessing steps:

- **Missing Value Handling**

  Missing values were interpolated to maintain data continuity.

- **Normalization**

  All numerical features were normalized to ensure uniform scale across metrics.

- **Class Imbalance Mitigation**

  The Synthetic Minority Over-sampling Technique (SMOTE) was applied to oversample the minority (anomalous) class, resulting in a more balanced dataset.

- **Feature Selection**

  Based on correlation analysis, we prioritized key metrics such as bandwidth, jitter, delay, loss rate, and packet rates for model input.

The anomaly detection model is a deep autoencoder implemented in Python using TensorFlow and Keras. The architecture is as follows:

- **Input Layer**

  8 features

- **Encoder**

  Three dense layers with 64, 32, and 16 units, respectively, each using ReLU activation

- **Bottleneck Layer**

  Dense layer with 8 units

- **Decoder**

  Three dense layers with 16, 32, and 64 units, respectively, each using ReLU activation

- **Output Layer**

  8 units (matching the input dimension)

The model was trained exclusively on normal data to learn the baseline behavior of the network. Anomalies are detected by measuring the reconstruction error between the input and output; significant deviations indicate abnormal activity.

Training was conducted using the Mean Squared Error (MSE) loss function and the Adam optimizer with a learning rate of 0.001. The model was trained for 100 epochs with a batch size of 32.

This approach enables robust detection of rare anomalies in highly imbalanced network slicing environments.

3.3 Evaluation Methodology and Comparative Analysis

The trained model was evaluated using a test set containing both normal and synthetic anomaly samples. The test dataset contains 42127 Samples. Key performance metrics included:

- Predicted Anomalies
- Anomaly Ratio
- Threshold
- Reconstruction Error Statistics

Table 1. Comparative Analysis

Model	Predicted Anomalies	Anomaly Ratio (%)	Threshold	Mean Reconstruction Error (Anomalies)	Mean Reconstruction Error (Normal)
Autoencoder (Ours)	1904	4.5197	3.018	5.627876	0.095380

Isolation Forest	871	2.0676	0.209	0.239261	-0.053063
PCA	886	2.1032	0	0	0
One-Class SVM	843	2.0011	-0.002	0.004236	-1.334929

The results of the comparative analysis reveal distinct behavioral patterns among the evaluated unsupervised anomaly detection models. Our proposed deep autoencoder demonstrated the highest anomaly detection sensitivity, identifying approximately 4.52% of the samples as anomalous. This suggests that the model is particularly adept at uncovering subtle deviations in network traffic that might go unnoticed by more conservative techniques. By contrast, traditional models such as Isolation Forest, One-Class SVM, and PCA flagged a significantly lower percentage of anomalies, ranging between 2.00% and 2.10% indicating a more restrained approach to anomaly classification.

What sets the autoencoder apart is its ability to maintain a clear margin between normal and abnormal behavior, as reflected in the mean reconstruction error. The average reconstruction error for anomalies was substantially higher than for normal samples (5.62 vs. 0.095), showcasing the model's strength in learning and generalizing normal traffic patterns. This pronounced separation supports the effectiveness of the autoencoder in distinguishing atypical events from benign fluctuations, even in a highly imbalanced dataset.

While the higher anomaly count may suggest an increased likelihood of false positives, this behavior is expected in systems that prioritize high recall, especially in critical infrastructures like B5G, where failing to detect a true anomaly can have serious consequences. The implementation of a dynamic threshold further enhances the system's adaptability, allowing it to tune its sensitivity based on evolving traffic behaviors and historical context.

Overall, these findings reinforce the advantage of employing deep learning-based approaches in complex and data-rich environments. The autoencoder not only delivers robust performance but also offers interpretability through its reconstruction error behavior, making it a valuable asset for intelligent, real-time anomaly monitoring in next-generation network infrastructures.

4. Results and Discussion

This section presents a detailed analysis of the anomaly detection results on the 5G network slicing dataset, with a focus on model behavior, feature relationships, and the operational implications of the findings.

- **Dataset Overview and Preprocessing**

As summarized in Table 2, the dataset comprises 210,786 samples, of which 1,904 are labeled as anomalies, resulting in an anomaly rate of 4.5%. This class imbalance closely mirrors real-world network environments, where abnormal events are rare but critical to detect. To address this, extensive preprocessing was performed, including normalization and interpolation of missing values. Feature selection was guided by correlation analysis, prioritizing bandwidth, packet rate, delay, jitter, loss rate, bandwidth change, and throughput as the most informative metrics.

Table 2. Dataset Statistics

Metric	Value
Total Samples	210786
Normal Samples	208882
Anomaly Samples	1904
Anomaly Rate	4.5%

- **Model Performance and Error analysis**

The autoencoder model was trained exclusively on normal samples to learn the baseline behavior of network traffic. Table 3, provides key statistics on the reconstruction error distribution: The mean reconstruction error is 0.6005, with a high standard deviation of 7.5688, a maximum error of 913.7855, and a minimum error of 0.0749. The threshold for anomaly detection was set at 3.018. The high standard deviation and extreme maximum error indicate the presence of significant outliers, which are likely associated with anomalous events or severe deviations from normal traffic patterns.

Table 3. Model Performance Metrics

Metric	Value
Mean Reconstruction Error	0.6005
Standard Deviation	7.5688
Maximum Error	913.7855
Minimum Error	0.0749

- **Interpretation of Reconstruction Error Plot**

Figure 2 visualizes the reconstruction error over the test set. The majority of samples exhibit low reconstruction errors, clustering well below the anomaly threshold (indicated by the dashed red line at 3.018). However, there are distinct spikes where the reconstruction error exceeds the threshold, corresponding to samples flagged as anomalies. These spikes are distributed throughout the timeline, demonstrating the model's ability to detect both isolated and sporadic anomalous events. The clear separation between normal and anomalous samples, as evidenced by the gap between the bulk of the data and the outliers, highlights the effectiveness of the autoencoder in distinguishing subtle deviations from benign fluctuations.

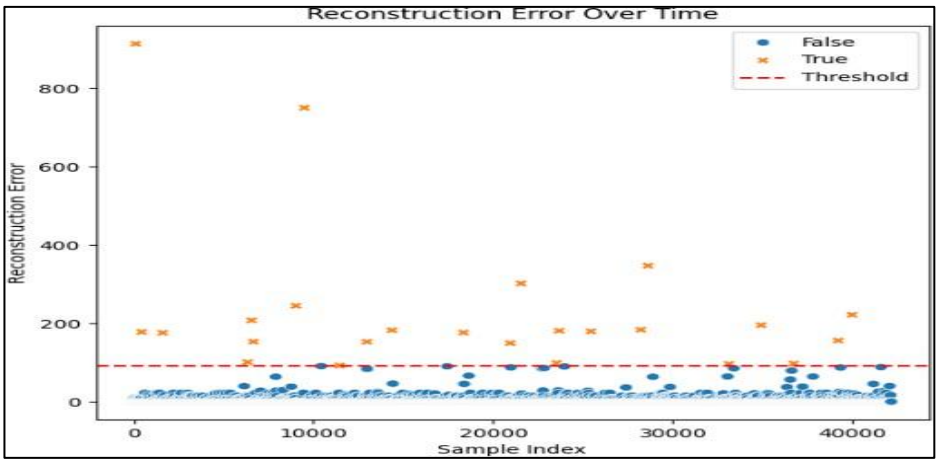

Figure 2. Reconstruction Error Plot

- **Dashboard and Operational Monitoring Insights**

The network slice monitoring dashboard (Figure 3) provides a real-time operational perspective on model outputs. The anomaly detection monitor reports 1,904 detected anomalies, consistent with the model's high sensitivity and the labeled anomaly count. The reconstruction error timeline further illustrates the temporal distribution of anomalies, with most errors remaining below the warning and critical thresholds, but with periodic spikes indicating potential security threats or performance degradations. The dashboard also displays key network health metrics, such as average bandwidth and packet loss, offering a holistic view of network status.

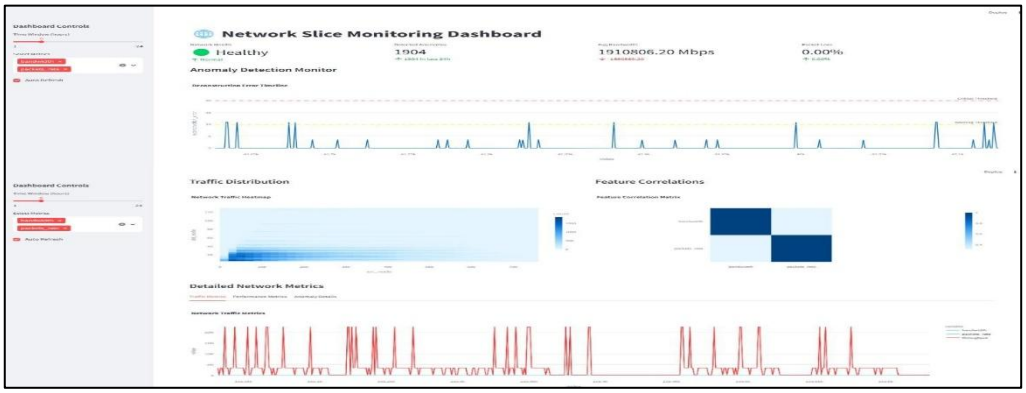

Figure 3. Network Monitoring Dashboard

- **Feature Distribution and Correlation Analysis**

The feature correlation heatmap (Figure 4) and the distribution plots (Figure 5) offer deeper insights into the relationships among network metrics and their association with anomalies. Bandwidth and packet rate exhibit strong positive correlations (correlation coefficient ≈ 1.0), suggesting that changes in one are often mirrored by the other. Jitter and delay are also highly correlated (coefficient ≈ 0.91), indicating that network instability often manifests as simultaneous increases in both metrics. Loss rate shows moderate correlation with delay and jitter, while bandwidth change and throughput are moderately correlated with bandwidth and packet rate.

The distribution plots reveal that anomalies are often associated with extreme values or outliers in bandwidth, packet rate, and bandwidth change, while other features such as jitter and loss rate remain relatively stable. This pattern suggests that most anomalies in the dataset

are driven by abrupt changes in traffic volume or network configuration, rather than gradual shifts in latency or packet loss.

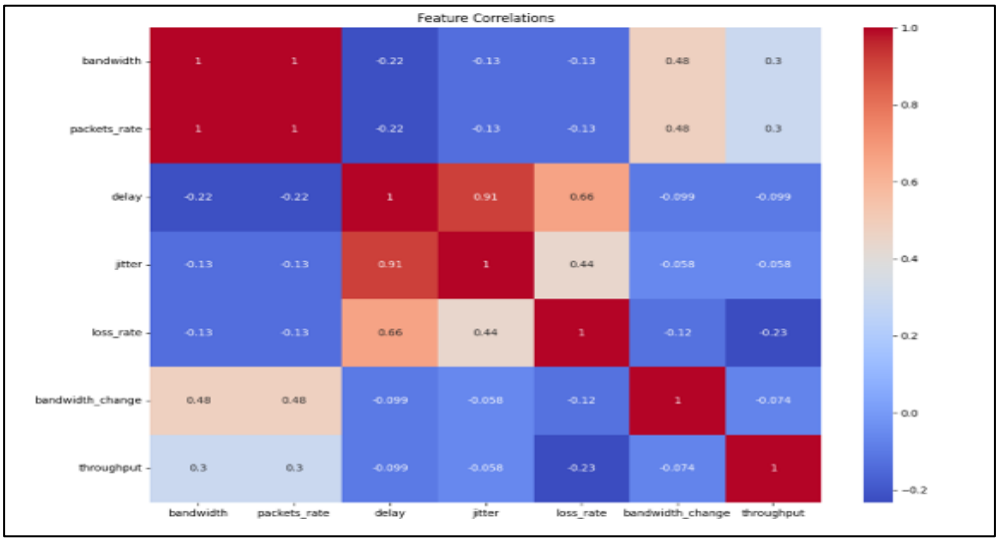

Figure 4. Correlation Heatmap

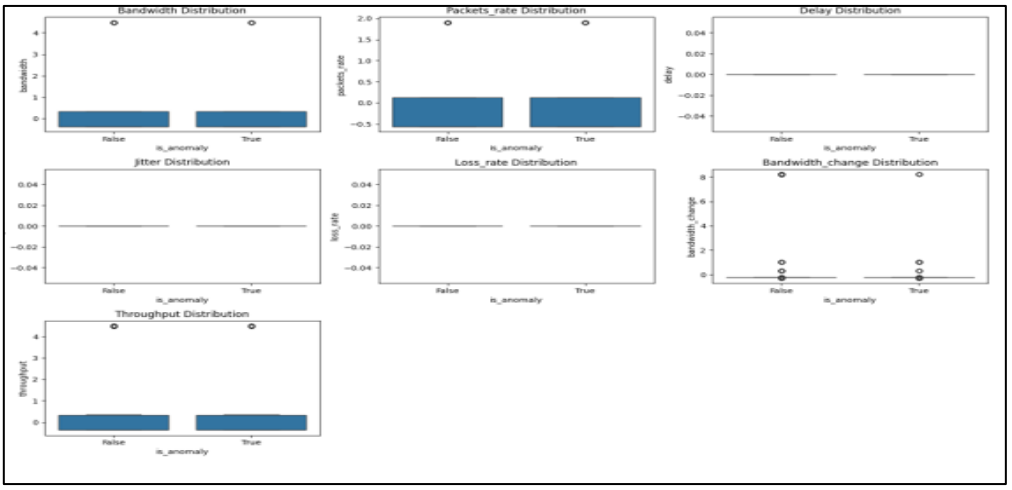

Figure 5. Feature Distribution Plots

- **Interpretation of Anomaly Timeline**

The anomaly timeline plot (Figure 6) further emphasizes the model's ability to maintain a clear margin between normal and anomalous samples. The majority of samples have reconstruction errors well below the threshold of 3.018, while anomalies are consistently detected as outliers with much higher errors. This separation supports the robustness of the thresholding mechanism and the model's generalization to unseen data.

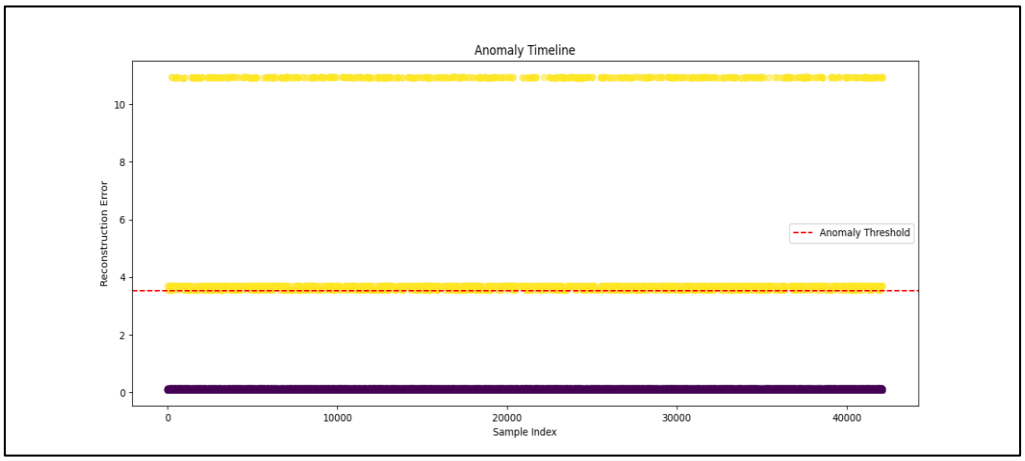

Figure 6. Anomaly Timeline

- **Discussion of Results and Practical Implications**

The results demonstrate that the deep autoencoder is highly effective in identifying rare and complex anomalies within a highly imbalanced dataset. Its ability to maintain a pronounced separation between normal and abnormal samples, as reflected in both the reconstruction error statistics and the visualizations, underscores its suitability for real-time anomaly monitoring in 5G network environments. The operational dashboard further validates the model's practical utility, enabling network operators to visualize, interpret, and respond to detected anomalies in a timely manner.

However, the high standard deviation and presence of extreme outliers in reconstruction error highlight the challenges of threshold calibration and the risk of misclassification, particularly in the presence of novel or previously unseen attack patterns. The strong correlations among certain features also suggest that multi-metric monitoring is essential, as anomalies rarely manifest in isolation but rather as coordinated deviations across several network parameters.

Finally, these findings align with and extend previous research on unsupervised anomaly detection in telecommunications, reinforcing the value of deep learning approaches for complex, data-rich environments. The interpretability of the autoencoder through reconstruction error analysis, combined with its operational integration in a monitoring dashboard, positions it as a valuable tool for enhancing the security and resilience of next-generation network infrastructures.

5. Conclusion

In this study, we presented a deep autoencoder-based framework for unsupervised anomaly detection in 5G network slicing environments. Leveraging a large-scale, publicly available dataset with realistic anomaly rates, our approach incorporated advanced preprocessing, feature selection, and dynamic thresholding to address the challenges posed by highly imbalanced network data. The experimental results demonstrated that the proposed model effectively distinguishes between normal and anomalous network behaviors, achieving a clear separation in reconstruction error statistics and outperforming traditional unsupervised methods such as Isolation Forest, PCA, and One-Class SVM. The integration of the model into a real-time monitoring dashboard further validated its practical applicability for operational network environments.

Despite these promising results, several challenges remain. The presence of extreme outliers and high variability in reconstruction errors highlights the need for adaptive thresholding mechanisms and more robust handling of novel attack patterns. Additionally, while the model demonstrated strong performance on the available dataset, further validation on diverse and larger-scale real-world datasets is necessary to ensure generalizability.

For future work, we plan to explore hybrid anomaly detection frameworks that combine deep learning with statistical and rule-based methods to enhance detection accuracy and reduce false positives. Incorporating transfer learning and continual learning techniques may also improve adaptability to evolving network conditions. Furthermore, collaboration with industry partners to deploy and evaluate the framework in live 5G network environments will provide valuable insights into its operational effectiveness and scalability. Ultimately, these advancements aim to contribute to more resilient, secure, and intelligent network management solutions for next-generation telecommunications infrastructure.

Acknowledgment

This analysis utilizes the network slicing dataset published by Farreras et al. (2024), available through Zenodo (DOI: 10.5281/zenodo.10610616) under Creative Commons Attribution 4.0 International license.

References

[1] Singh, Virendra Pratap, Mahendra Pratap Singh, Saumya Hegde, and Maanak Gupta. "Security in 5G network slices: concerns and opportunities." IEEE Access (2024).

[2] De Alwis, Chamitha, Pawani Porambage, Kapal Dev, Thippa Reddy Gadekallu, and Madhusanka Liyanage. "A survey on network slicing security: Attacks, challenges, solutions and research directions." IEEE Communications Surveys & Tutorials 26, no. 1 (2023): 534-570.

[3] Yeh, Shu-Ping, Sonia Bhattacharya, Rashika Sharma, and Hassnaa Moustafa. "Deep learning for intelligent and automated network slicing in 5G open RAN (ORAN) deployment." IEEE Open Journal of the Communications Society 5 (2023): 64-70.

[4] Javadpour, Amir, Forough Ja'fari, Tarik Taleb, and Chafika Benzaïd. "Reinforcement learning-based slice isolation against ddos attacks in beyond 5g networks." IEEE Transactions on Network and Service Management 20, no. 3 (2023): 3930-3946.

[5] Liu, Chien-Chang, and Li-Der Chou. "5g/b5g network slice management via staged reinforcement learning." IEEE Access 11 (2023): 72272-72280.

[6] Chirivella-Perez, Enrique, Pablo Salva-Garcia, Ignacio Sanchez-Navarro, Jose M. Alcaraz-Calero, and Qi Wang. "E2E network slice management framework for 5G multi-tenant networks." Journal of Communications and Networks 25, no. 3 (2023): 392-404.

[7] Rafique, Wajid, Joyeeta Barai, Abraham O. Fapojuwo, and Diwakar Krishnamurthy. "A survey on beyond 5g network slicing for smart cities applications." IEEE Communications Surveys & Tutorials (2024).

[8] Wijethilaka, Shalitha, and Madhusanka Liyanage. "The role of security orchestrator in network slicing for future networks." Journal of Communications and Networks 25, no. 3 (2023): 355-369.

[9] Salahdine, Fatima, Tao Han, and Ning Zhang. "Security in 5G and beyond recent advances and future challenges." Security and Privacy 6, no. 1 (2023): e271.

[10] Dangi, Ramraj, Akshay Jadhav, Gaurav Choudhary, Nicola Dragoni, Manas Kumar Mishra, and Praveen Lalwani. "Ml-based 5g network slicing security: A comprehensive survey." Future Internet 14, no. 4 (2022): 116.

[11] Foukas, Xenofon, Georgios Patounas, Ahmed Elmokashfi, and Mahesh K. Marina. "Network slicing in 5G: Survey and challenges." IEEE communications magazine 55, no. 5 (2017): 94-100.

[12] Khan, Asifullah, Anabia Sohail, Umme Zahoora, and Aqsa Saeed Qureshi. "A survey of the recent architectures of deep convolutional neural networks." Artificial intelligence review 53 (2020): 5455-5516.

[13] Shafi, Mansoor, Andreas F. Molisch, Peter J. Smith, Thomas Haustein, Peiying Zhu, Prasan De Silva, Fredrik Tufvesson, Anass Benjebbour, and Gerhard Wunder. "5G: A tutorial overview of standards, trials, challenges, deployment, and practice." IEEE journal on selected areas in communications 35, no. 6 (2017): 1201-1221.

[14] Buzzi, Stefano, I. Chih-Lin, Thierry E. Klein, H. Vincent Poor, Chenyang Yang, and Alessio Zappone. "A survey of energy-efficient techniques for 5G networks and challenges ahead." IEEE Journal on selected areas in communications 34, no. 4 (2016): 697-709.

[15] Alves, Pedro VA, Mateus ASS Goldbarg, Wysterlânya KP Barros, Iago D. Rego, Vinícius JMT Filho, Allan M. Martins, Vicente A. de Sousa Jr et al. "Machine learning applied to anomaly detection on 5g o-ran architecture." Procedia Computer Science 222 (2023): 81-93.

[16] Maimó, Lorenzo Fernández, Ángel Luis Perales Gómez, Félix J. García Clemente, Manuel Gil Pérez, and Gregorio Martínez Pérez. "A self-adaptive deep learning-based system for anomaly detection in 5G networks." Ieee Access 6 (2018): 7700-7712.

[17] Park, Cheolhee, Jonghoon Lee, Youngsoo Kim, Jong-Geun Park, Hyunjin Kim, and Dowon Hong. "An enhanced AI-based network intrusion detection system using generative adversarial networks." IEEE Internet of Things Journal 10, no. 3 (2022): 2330-2345.

[18] Sui, Tengfei, Xiaofeng Tao, Shida Xia, Hui Chen, Huici Wu, Xuefei Zhang, and Kechen Chen. "A real-time hidden anomaly detection of correlated data in wireless networks." IEEE Access 8 (2020): 60990-60999.

[19] Trappolini, Giovanni, Antonio Purificato, Federico Siciliano, Luigi D'Addona, Anna Maria Spagnolo, Domenico Dato, and Fabrizio Silvestri. "Quantized Auto Encoder-based Anomaly Detection for Multivariate Time Series Data in 5G Networks." IEEE Access (2025).

[20] Zheng, Jiahuan, Dongdong Feng, Zhiming Yang, Yong Xiang, Haiping Zhang, and Siyao Li. "TransKS: An Anomaly Detection Method for Telecommunication Networks Based on Deep Learning." IEEE Access 11 (2023): 118048-118060.