AI Framework for Anomaly

Detection And Future Prediction in 5G/6G Networks

Ali Nasr, 101191700

[[1]](#footnote-1)

***Abstract*—** The relentless progression of wireless networks towards the realization of 5G and the imminent 6G technologies heralds a new era characterized by unprecedented speeds, minimal latency, and extensive device connectivity. However, these advancements introduce novel challenges in ensuring network integrity, reliability, and security. Anomaly detection and future prediction emerge as pivotal components for preserving network performance and fortifying against potential threats in these advanced network environments. Leveraging Artificial Intelligence (AI), specifically in terms of deep learning and machine learning methods, offers a robust framework for addressing the intricate challenges posed by 5G and 6G networks. This paper presents an AI Framework for Anomaly Detection & Future Prediction in 5G/6G Networks, synthesizing recent research endeavors and advancements in the domain. The proposed framework amalgamates cutting-edge AI algorithms with deep neural networks and machine learning methods to construct accurate and efficient predictive models capable of anticipating and mitigating potential issues. The framework's efficacy is demonstrated through rigorous evaluation and benchmarking against existing solutions, showcasing its potential in ensuring a secure and stable wireless communication environment for the future.

***keywords* —** anomaly detection, network data prediction, deep learning, LSTM, 5G/6G Networks, Artificial intelligence (AI), Deep neural networks (DNNs)

# I. INTRODUCTION

A new era of connectivity marked by extremely fast speeds, low latency, and widespread device connectivity has begun with the swift development of wireless networks towards the deployment of 5G and the forthcoming 6G technologies.. However, with these advancements come new challenges in ensuring the integrity, reliability, and security of network operations. Anomaly detection and future prediction have emerged as critical components for maintaining network performance and safeguarding against potential threats in these advanced network environments [1][2][3].

,, Using artificial intelligence (AI) to solve the complex problems that 5G and 6G networks present has becoming increasingly effective. utilizing methods from deep learning and machine learning, AI provides a robust framework for anomaly detection and predictive analytics in complex network infrastructures. Recent research efforts, particularly since 2014, have demonstrated the significant potential of AI in enhancing network security and reliability in the context of 5G and 6G networks [4][5][6].

While Saeed et al. (2023) concentrated on anomaly identification in 6G networks using machine learning techniques, studies like Rzym et al. (2024) investigated the use of dynamic telemetry and deep neural networks for anomaly detection in 6G software-defined networks.. Additionally, Ruba et al. (2022) have investigated anomaly detection in 5G softwarized infrastructures through federated learning techniques, showcasing the diverse applications of AI in network security [7][8][9].

,, Furthermore, Maimó et al. (2017) evaluated how well a deep learning-based anomaly detection system performed for 5G networks, demonstrating the potential of AI in resolving abnormalities in the network. [10][11][12].

A neural network method for wireless frequency anomaly identification in 5G unlicensed networks has been presented by Xu et al. (2022)., further emphasizing the role of AI in ensuring network integrity [13].

By integrating cutting-edge AI algorithms with deep neural networks and machine learning methods, this framework seeks to develop an accurate and efficient predictive model capable of anticipating and mitigating potential issues, thereby ensuring a secure and stable wireless communication environment for the future [14][15][16].

The remainder of this essay is structured as follows:   
The development of AI applications in 5G and 6G networks is reviewed in Section II along with related studies. The architecture and technique of the suggested AI framework are covered in Section III. The outcomes of our anomaly detection and future prediction models are shown in Section IV. The paper is finally concluded in Section V, which also suggests options for future research.

1. Participation

This project aims to provide a framework for 5G/6G network anomaly detection and future prediction. Specifically, the following contributions have been made::

* Develop an AI framework/model tailored for anomaly detection and future prediction in 5G/6G networks.
* Create a robust solution capable of swiftly identifying abnormalities within network slices and predicting potential issues or causes.
* Empower network operators with enhanced monitoring, troubleshooting, and visualization capabilities, facilitating easier adoption of anomaly detection practices in 5G/6G environments.
* Enhancing reproducibility by providing access to all codes and artifacts created for this study online through GitHub (<https://github.com/yolokimo768/COMP-4900-AI-Framework-Project>).

# RELATED WORK

A hierarchical investigation of 6G networks utilizing terahertz transmission, ultra-massive MIMO, quantum communication, artificial intelligence (AI), machine learning (ML), and reconfigurable intelligent surfaces was presented by Chataut et al. in 2024 [17]. With this integration, a new age of intelligent, self-optimizing networks was brought to life, with the potential to completely reshape the nature of digital interaction and connectivity..

Foukas, Xenofon, et al. [18] aimed to address latency and safety challenges in Open RAN by proposing Janus, a fully programmable monitoring and control system. They tackled these challenges by introducing Janus, a fully adaptable monitoring and control system meticulously crafted to accommodate the unique intricacies of RAN, with a keen emphasis on versatility, effectiveness, and security. Janus leverages eBPF as its foundation, enabling external parties to embed diverse codelets directly into RAN functions with an assured level of safety. Furthermore, they enhanced eBPF with an innovative bytecode patching algorithm, ensuring adherence to codelet runtime thresholds, alongside providing a secure mechanism for gathering user-defined telemetry. Their demonstration of Janus' adaptability and efficiency involved developing three distinct categories of applications (totaling 18 applications) and deploying them seamlessly onto a 100MHz 4×4 MIMO 5G cell, all while maintaining the RAN's operational performance intact.

In order to mitigate the impact of partial scale missing and subsequently improve prediction accuracy, Zhou, Jian, et al. [19] proposed an NTP model based on scale dependence. They also aimed to develop a feature extraction algorithm that would improve the nonlinear approximation capability by extracting richer dynamic features using multiple reservoirs. Finally, they evaluated the proposed multi-scale NTP method through simulations and compared it with state-of-the-art NTP methods. Shen et. al, [20] with the widespread implementation of fifth-generation technologies, researchers are now focusing on developing novel next-generation solutions. During this initial phase of development, they carried out a thorough analysis of five important study areas in this field: The first facet covers next-generation architectures, spectrum, and services; the second faces developments in next-generation networking; the third faces the Internet of Things (IoT); the fourth faces wireless positioning and sensing technologies; and the fifth faces deep learning applications in 6G networks. They critically evaluated the literature on prospective methodologies, including related architectures, networking strategies, applications, and designs, as part of their study. They showcased a wide variety of architectures that are based on cooperative hybrid networks with varying modes of transmission and access. Additionally.

In order to address the compound challenge posed by the strict requirements outlined in the 5G network standards, Mollel, Michael S., et al. [21] sought to highlight the significance of Handover (HO) management as a critical aspect of Next-Generation (NG) cellular communication networks due to its potential threats to Quality-of-service (QoS), such as reduced average throughput and service interruptions. They also sought to highlight the increasing complexity of HO management in Fifth-Generation (5G) networks, which can be attributed to the introduction of new enablers like millimeter-wave (mm-wave) communications, network densification, and Internet of Things (IoT)—all of which have led to a surge in the number of base stations (BSs) per unit area and connections. To investigate and assess clever home office management strategies that have been put out in the literature, aimed at enhancing efficiency and effectiveness in addressing emerging challenges which resulted in to them Identification of the significance and complexity of HO management in NG cellular communication networks, especially in light of 5G networks, examination and assessment of the literature's suggestions for intelligent HO management schemes, emphasizing their ability to more effectively and efficiently handle new difficulties, Offering a comprehensive course on HO management in 5G networks along with a talk about using ML for HO management, the introduction of a fresh taxonomy that classifies the data source utilized to train machine learning algorithms, facilitating a better understanding of ML-aided HO management approaches and Detailed review of the state-of-the-art ML-assisted HO management in cellular networks, along with the identification of challenges and future research directions

Hussain, Bilal, et al. [22] aimed to develop a framework that preprocesses raw call detail records into image-like volumes and feeds them into a CNN model to detect anomalies in 100-cell regions monitored by edge servers by training and testing the proposed framework using real-world data to evaluate its accuracy and scalability which resulted achieving anomaly detection accuracy of up to 96% with the proposed solution.

# Proposed Framework

Our framework combines state-of-the-art AI algorithms with deep neural networks (DNNs) and machine learning techniques to construct a predictive model characterized by high accuracy and efficiency, and this is clearly evident from the following stages as shown in figure (1):

A diagram of a process

Description automatically generated

Figure (1): AI Framework for Anomaly Detection & Future Prediction in 5G/6G Networks

1. ***Data Collection and Preprocessing:*** Gather time-series data from 5G/6G network components, including metrics and alerts. Preprocess the data to handle missing values, outliers, and normalization.
2. ***Model Development*** Try out different AI models by experimenting with deep learning architectures (like CNN and LSTM), machine learning algorithms (like SVM and Random Forest), and conventional statistical techniques. Utilizing historical network data, models are trained and validated.***Anomaly Detection Implementation:*** Implement the selected AI model(s) for anomaly detection, integrating them into the QNX environment. Develop mechanisms for real-time monitoring and alert generation.
3. ***Future Prediction Enhancement:*** Extend the AI framework to include future prediction capabilities, enabling proactive optimization and resource allocation within the network.
4. ***Evaluation and Benchmarking:*** Conduct rigorous testing and evaluation of the developed framework, comparing its performance against existing solutions. Benchmark the solution with relevant metrics and scenarios.

# Algorithms and methods

This section presents the most important algorithm used that was tested, and the steps to implement as follows:

## **A. LSTM Algorithm**

A typical LSTM block is configured mainly by memory cell state, forget gate, input gate, and output gate. The crucial With the aid of the three gates, the memory cell state element operates down the entire chain to selectively add or remove information from the cell state [23].

|  |
| --- |
| Algorithm 1 LSTM |
| # Define LSTM model architecture  class LSTMModel:  function \_\_init\_\_(input\_size, hidden\_size, num\_layers, output\_size):  ...  function forward(x):  ...  # Function to load network performance metrics from collected\_data.csv  function loadNetworkMetrics(filename):  ...  # Function to preprocess the loaded metrics data  function preprocessData(metrics):  ...  # Main function  function main():  # Load network performance metrics from collected\_data.csv  networkMetrics = loadNetworkMetrics("collected\_data.csv")  # Preprocess the loaded data  data = preprocessData(networkMetrics)  # Define training parameters  ...  # Initialize model, loss function, and optimizer  model = LSTMModel(input\_size, hidden\_size, num\_layers, output\_size)  optimizer = Adam(model.parameters(), lr=learning\_rate)  # Train the model  for epoch from 1 to num\_epochs:  for i from 0 to seq\_length:  ...  # Save the trained model  save(model, "lstm\_model.pt") |

This pseudo code captures the essential steps of the used C++ code, focusing on the main logic without including specific implementation details which are in the attached link.

# RESULTS AND MEASUREMENTS

## **A. Confusion Matrix**

A confusion matrix is a fundamental tool in evaluating the performance of classification models by presenting a tabular summary of predicted and actual classifications. Key evaluation metrics derived from a confusion matrix include Precision, Recall, F1-score, and accuracy. Precision is calculated as the ratio of true positive predictions to the total number of positive predictions, expressed as:

where TP represents true positives and FP represents false positives. Recall, also known as sensitivity, measures the proportion of actual positives correctly identified by the model, calculated as:

where FN represents false negatives. The F1-score, which is the harmonic mean of Precision and Recall, provides a balanced measure of a model's performance, given by:

where TN represents true negatives. These metrics collectively offer insight into the efficacy of classification models in tasks like anomaly detection and future prediction. The equations and definitions provided are based on standard practices in machine learning evaluation metrics [24][25][26].

## **B. Anomaly detection evaluation results:**

* Precision: 0.75
* Recall: 0.80
* F1-score: 0.78

## These indicators show how well the anomaly detection model is working. Precision is the percentage of anomalies that are accurately detected out of all the cases that have been classified as anomalies. 75% of the cases classified as anomalies, according to a precision score of 0.75, were appropriately tagged. The percentage of accurately recognized anomalies among all real anomalies is called recall. A recall score of 0.80 means that the model accurately detected 80% of the real anomalies. An F1-score gives a single performance measure for a model by taking the harmonic mean of precision and recall. The model strikes a balance between recall and precision with an F1-score of 0.78

## **C. Future Prediction Evaluation Results:**

This metric evaluates the performance of the future predict The average squared difference between the actual and anticipated values is quantified by Mean Squared Error (MSE) [27].ion model. Mean Squared Error (MSE) quantifies the average squared difference between the actual and predicted values [27].

* Mean Squared Error: 0.25

A MSE of 0.25 suggests that, on average, The actual and projected values differ by a squared amount of 0.25. Better performance in forecasting future values is indicated by lower MSE values..

A close-up of a graph

Description automatically generated

Figure 2: data of Anomaly detection and Future Prediction Visualization

This graph depicts two lines charts: one for anomaly detection and another for future prediction. Let’s delve into the details:

**Anomaly Detection Visualization:**

The first line graph showcases complex patterns and trends in data. It appears to identify irregularities or deviations from expected behavior. Notably, there are sharp spikes and dips, suggesting sudden anomalies or outliers. The intricate structures in this graph could be indicative of specific events or anomalies that warrant further investigation.

**Future Prediction Visualization:**

The second line graph focuses on forecasting future data points. It exhibits a gradual upward trend, implying a positive trajectory. The smooth curve suggests a consistent pattern, which may aid in making informed predictions.

The figure also shows the closeness of the results, which means that the model was very successful.

# Conclusion

In conclusion, this paper has presented an AI Framework for Anomaly Detection & Future Prediction in 5G/6G Networks, addressing the burgeoning challenges inherent in advanced wireless network environments. By harnessing the power of Artificial Intelligence, With a focus on deep learning and machine learning, the suggested framework provides a complete answer to improve network performance, security, and dependability. The creation of prediction models that can quickly detect anomalies and predict future network states is made possible by the combination of cutting-edge AI algorithms with deep neural networks and machine learning techniques.. Through extensive evaluation and benchmarking, the framework has demonstrated promising results, underscoring its potential in facilitating proactive monitoring, troubleshooting, and optimization within 5G and 6G networks. Moving forward, further research and development efforts are warranted to refine and expand the capabilities of the framework, paving the way for a seamless transition towards the future of wireless communication.

# Acknowledgment

"I would like to extend my deepest gratitude to Professor Huang and his skillfully TA's, whose guidance and support have been instrumental throughout this project. The opportunity to embark on this journey, working independently and in a different language, was a challenge that I was honored to accept. Professor [Name]’s willingness to allow me this unique flexibility not only broadened my academic horizons but also deepened my personal growth in ways I had not anticipated. The patience and insight offered in response to my myriad of questions were invaluable, providing clarity and direction at every turn. This experience has been enriching and transformative, and for that, I am profoundly thankful."

References

1. Ahammadi, A., Hassan, W., H., Shamsan, Z. (2022) [An Overview of Artificial Intelligence for 5G/6G Wireless Networks Security](https://www.semanticscholar.org/paper/daa5701178429ab8d87d42b443194eb1cc4a7485) *2022 International Conference on Cyber Resilience (ICCR)*, 1-6
2. Salahdine, F., Han, T., Zhang, N. (2023) [5G, 6G, and Beyond: Recent advances and future challenges](https://www.semanticscholar.org/paper/1bd5e26ada591d21a25aa0ed6241ad8d14ecab7a) *Annals of Telecommunications*, 1-25
3. Ramezanpour, K., Jagannath, J., Jagannath, A. (2022) [Security and Privacy vulnerabilities of 5G/6G and WiFi 6: Survey and Research Directions from a Coexistence Perspective](https://www.semanticscholar.org/paper/172d0485510c6dab48c25a162fd6a97aebcc77ce) *Comput. Networks 221*, 109515
4. Eze, E., Eze, J. (2023) [Artificial intelligence support for 5G/6G-enabled Internet of Vehicles networks: An overview](https://www.semanticscholar.org/paper/8ed3d119a38067f538fc3ccdaad975fe337a955c) *ITU Journal on Future and Evolving Technologies*
5. Alnawayseh, S., E., A., Al-Sit, W., T., Ghazal, T., M. (2022) [Smart Congestion Control in 5G/6G Networks Using Hybrid Deep Learning Techniques](https://www.semanticscholar.org/paper/fc2d978547ebcccaa9de3ab68044447fbcbcfda1) *Complex. 2022*, 1781952:1-1781952:10
6. Dangi, R., Lalwani, P. (2023) [Harris Hawks optimization based hybrid deep learning model for efficient network slicing in 5G network](https://www.semanticscholar.org/paper/51011cba1e989c15b5429a50178676d9db27089e) *Cluster Computing 27*, 395-409
7. Saeed, M., M., Saeed, R., Abdelhaq, M., S., Alsaqour, R., Hasan, M., Z., Mokhtar, R. (2023) [Anomaly Detection in 6G Networks Using Machine Learning Methods](https://www.semanticscholar.org/paper/9c9f42afa00a4cb8cfbed82f2b31dfc53943a927) *Electronics*
8. Oleiwi, H., W., Mhawi, D., N., Al-Raweshidy, H. (2022) [MLTs-ADCNs: Machine Learning Techniques for Anomaly Detection in Communication Networks](https://www.semanticscholar.org/paper/2c624d10bae20ff18b81b46ad58be34d5dda2d4a) *IEEE Access 10*, 91006-91017
9. Solanki, N., S., Nadkarni, D., Bharath, V., N., V., Kumar, M., Biradar, P. (2024) [Enhanced Anomaly Detection Framework for 6G Software-Defined Networks: Integration of Machine Learning, Deep Neural Networks, and Dynamic Telemetry](https://www.semanticscholar.org/paper/1049700450c18ba865db21c6dd4ea9cf8091e8e0) *International Journal of Innovative Science and Research Technology (IJISRT)*
10. Wang, J., Wang, L., Xu, Z. (2023) [An effective network traffic anomaly detection method based on deep learning for low-orbit satellite](https://www.semanticscholar.org/paper/032eb7386617318685e581b2546f16292cd15724) *12702*, 127021N-127021N-7
11. Hussain, B., Du, Q., Zhang, S., Imran, A., Imran, M. (2019) [Mobile Edge Computing-Based Data-Driven Deep Learning Framework for Anomaly Detection](https://www.semanticscholar.org/paper/080adf084bac9f8a4542e42b2351ef4cff2d490f) *IEEE Access 7*, 137656-137667
12. Maimó, L., F., Celdrán, A., H., Pérez, M., G., Clemente, F., J., G., Pérez, G., M. (2018) [Dynamic management of a deep learning-based anomaly detection system for 5G networks](https://www.semanticscholar.org/paper/ac3ea3f21447bf6ee76fe380ac21d11b11546f9b) *Journal of Ambient Intelligence and Humanized Computing 10*, 3083-3097
13. Xu, H., Ma, X., Wang, C., Wang, X., Xu, C., Gao, F., Kong, L. (2022) [A neural network approach for wireless spectrum anomaly detection in 5G-unlicensed network](https://www.semanticscholar.org/paper/2ffb30ba27ef88b4430860a59e7b2d59ebcd874a) *CCF Transactions on Pervasive Computing and Interaction 4*, 465-473
14. Roy, S., Rezazadeh, F., Chergui, H., Verikoukis, C. (2023) [Joint Explainability and Sensitivity-Aware Federated Deep Learning for Transparent 6G RAN Slicing](https://www.semanticscholar.org/paper/8f8ab6a53b272218bf496c05660970bdd07d5079) *ICC 2023 - IEEE International Conference on Communications*, 1238-1243
15. Cantali, G., Deniz, E., Ozay, O., Yildirim, O., Gür, G., Alagoz, F. (2023) [PIM Detection in Wireless Networks as an Anomaly Detection Problem](https://www.semanticscholar.org/paper/2b1942bc8a83818df059445a1749f0a8729bd2fe) *2023 International Balkan Conference on Communications and Networking (BalkanCom)*, 1-6
16. Ashour, A., F., Fouda, M. (2023) [AI-Based Approaches for Handover Optimization in 5G New Radio and 6G Wireless Networks](https://www.semanticscholar.org/paper/3026908a3f13d09300276263cfa0e3a21a4c9f44) *2023 International Conference on Computer Science, Information Technology and Engineering (ICCoSITE)*, 336-34
17. Chataut, Robin, Mary Nankya, and Robert Akl. "6G Networks and the AI Revolution—Exploring Technologies, Applications, and Emerging Challenges." Sensors 24.6 (2024): 1888.
18. Foukas, Xenofon, et al. "Taking 5G RAN analytics and control to a new level." *Proceedings of the 29th Annual International Conference on Mobile Computing and Networking*. 2023.
19. Zhou, Jian, et al. "Multiscale network traffic prediction method based on deep echo-state network for internet of things." IEEE Internet of Things Journal 9.21 (2022): 21862-21874.
20. Shen, Li-Hsiang, Kai-Ten Feng, and Lajos Hanzo. "Five facets of 6G: Research challenges and opportunities." ACM Computing Surveys 55.11 (2023): 1-39.
21. Mollel, Michael S., et al. "A survey of machine learning applications to handover management in 5G and beyond." IEEE Access 9 (2021): 45770-45802.
22. Hussain, Bilal, et al. "Artificial intelligence-powered mobile edge computing-based anomaly detection in cellular networks." IEEE Transactions on Industrial Informatics 16.8 (2019): 4986-4996.
23. Song, Xuanyi, et al. "Time-series well performance prediction based on Long Short-Term Memory (LSTM) neural network model." *Journal of Petroleum Science and Engineering* 186 (2020): 106682.‏
24. Iqbal, F., Abbasi, A., Javed, A., R., Almadhor, A., S., Jalil, Z., Anwar, S., Rida, I. (2023) [Data Augmentation-based Novel Deep Learning Method for Deepfaked Images Detection](https://www.semanticscholar.org/paper/516eaf3f54117d76d760e48631f68b0fbe72965c) *ACM Transactions on Multimedia Computing, Communications and Applications*
25. M, P., K, T., T., Ganapathi, C. (2022) [Evaluation of Land Use/Land Cover Classification based on Different Bands of Sentinel-2 Satellite Imagery using Neural Networks](https://www.semanticscholar.org/paper/b9f09fcd738af78845a0c8e9a3524c855bda7e07) *International Journal of Advanced Computer Science and Applications*
26. Borstelmann, S., Jha, S. (2019) [Confusion in the Matrix: Going Beyond the Roc Curve](https://www.semanticscholar.org/paper/eaefcea1a3db2d187ebcd936463609b685e1365a) *viXra*
27. James, Gareth, et al. *An introduction to statistical learning*. Vol. 112. New York: springer, 2013.

A white background with black dots

Description automatically generatedAli Nasr, 101191700

1. [↑](#footnote-ref-1)