Information Technology Institute

LTE Network Anomaly Detection

Supervised by:

Dr. Mahmoud AbdelAziz

Eng. Mirlham Rizk

LTE Network Anomaly Detection System

1. Executive Summary

This project presents a comprehensive system designed to automatically detect, explain, and visualize anomalies in LTE network performance data. Our solution integrates traditional statistical techniques with advanced machine learning (ML), deep learning (DL), and language models (LLMs) to provide a robust, modular, and explainable anomaly detection pipeline. The system supports network engineers by flagging suspicious KPI behavior, explaining root causes, and mapping affected sites — all in an interactive interface.

2. Introduction

Modern LTE networks produce vast volumes of KPIs daily, with each cell reporting multiple performance metrics. Monitoring these metrics manually is timeconsuming, error-prone, and does not scale. Additionally, static threshold-based alerts lack context and adaptability. The project aims to overcome these limitations by developing an intelligent, automated anomaly detection system.

3. Problem Statement

Operators struggle with:

- Volume: Thousands of KPIs across hundreds of cells daily.

- Inaccuracy: Thresholds often miss anomalies or raise false alerts.

- Lack of explanation: Why did a KPI spike? What's the impact?

- Delayed action: Manual review slows down problem resolution.

4. Project Objectives

- Build an end-to-end anomaly detection system for LTE networks.

- Design a modular architecture with clear component roles.

- Integrate statistical, ML, DL, and LLM models.

- Provide human-readable insights via summaries.

- Visualize results with geo-spatial context.

5. LTE KPI Overview

Key KPIs selected for anomaly detection:

- **L.RRC.ConnReq.Succ** – RRC connection request success rate.

- **4G DL PRB Utilization (%)** – Downlink physical resource block usage.

- **4G UL PRB Utilization (%)** – Uplink PRB usage.

- **4G DL Traffic Volume (TB)** – Downlink traffic in TB.

- **4G UL Traffic Volume (TB)** – Uplink traffic in TB.

6. Data Sources

Two key datasets were used:

- **KPI Dataset** – Daily measurements for selected LTE cells between Jan and Jul 2024.

- **Metadata File** – Contains Region, District, Latitude, Longitude, Site name, Cell name, Frequency Band.

7. Data Preprocessing

- Filtered out cells with missing or zero KPI values.

- Ensured full daily coverage across the study period.

- Normalized values per KPI where needed.

8. Feature Engineering

We engineered several time-series features:

- **Lag features**: t-1, t-2 values.

- **Rolling stats**: 3-day mean, std, max, min.

- **STL decomposition**: to extract residuals.

- **Prophet residuals**: from forecast vs. actual.

9. Exploratory Data Analysis

EDA revealed:

- Strong correlation between PRB Utilization and Traffic Volume.

- Seasonal patterns in traffic.

- Region-specific behavior in congestion patterns.

10. Anomaly Detection Approaches Tried

We implemented and compared:

- STL + Z-Score

- Isolation Forest

- Local Outlier Factor (LOF)

- LSTM Autoencoder

- BiLSTM Classifier

11. Final Detection Fusion Strategy

We combined STL-Z, LOF, and IF using majority voting to:

- Reduce false positives

- Preserve zero false negatives

- Align with domain-labeled anomalies (Prophet+Z)

12. Evaluation Metrics & Results

- **Precision**: 0.87

- **Recall**: 1.00

- **F1-score**: 0.93

- Hybrid model outperformed any individual technique.

13. LLM Summary Function

The LLM module takes:

- Detected anomalies + metadata context

And outputs:

- Plain-language summary (e.g., "DL PRB spike suggests congestion")

- KPI-specific explanation

- Optional recommendations

14. Geo-Spatial Module

We created a map-based module using Folium:

- Visualized affected sites using color-coded markers

- Allowed filtering by region and frequency band

- Used BallTree for nearest-site search

15. Streamlit UI Overview

Our interactive app includes:

- File uploader

- Cell and KPI selectors

- Time-series charts with anomaly markers

- LLM summaries per cell/KPI

- Geo-map integration

16. Pipeline Architecture

Raw KPI Data → Feature Engineering → Detection Models → Fusion → LLM → Map + UI

17. Model Performance

We visualized:

- Model comparison via bar charts (Precision, Recall, F1)

- Confusion matrix for BiLSTM

- Performance per KPI

18. Use Case Example

- **Cell**: L21_Basse_7

- **KPI**: 4G DL PRB Utilization

- **Date**: July 2, 2024

- **Detection**: STL-Z and LOF raised anomaly

- **LLM Output**: "DL PRB usage exceeds 90%. Likely congestion. Check traffic volume."

19. Live Demo

We showcased:

- Uploading test set

- Selecting cell/KPI

- Viewing anomalies + explanations

- Zooming to region in map

20. Challenges Faced

- Balancing precision vs. recall

- Tuning Z-score and thresholds

- Ensuring good LLM latency

- Keeping UI responsive with large files

21. Lessons Learned

- Hybrid > individual model
- STL residuals are great anomaly indicators
- LLM summaries help non-technical users
- Map context is critical in large-scale networks

22. Future Work

- Add real-time streaming support
- Use LLMs for Root Cause Analysis (RCA)
- Extend model to 5G and multi-RAT networks

23. Conclusion

We developed a full anomaly detection system that:

- Detects abnormal LTE behavior
- Explains results in human language
- Maps where issues happen
- Offers a usable, scalable UI for telecom engineers

24. Screenshots

(Insert time-series chart, LLM summary output, geo-map)

25. References

1. Facebook Prophet Documentation

2. scikit-learn: Isolation Forest, LOF

3. TensorFlow/Keras: LSTM

4. Streamlit.io Documentation

5. Folium Maps

6. ITU/3GPP KPI definitions

Anomaly Detection in Telecommunication Networks

In this section, we provide an in-depth discussion of the anomaly detection

Anomaly detection plays a pivotal role in modern telecommunication networks, serving as a critical mechanism for maintaining service quality, operational stability, and customer satisfaction. Telecom networks generate vast volumes of data across multiple layers—from radio access and transport to the core network—capturing Key Performance Indicators (KPIs) such as traffic volume, connection success rates, and resource utilization. These KPIs reflect the real-time health and performance of the network. Detecting anomalies in such data involves identifying patterns that deviate significantly from normal behavior, which may indicate network faults, misconfigurations, congestion, hardware degradation, or even security breaches. In highly dynamic environments like 4G LTE and 5G, where millions of subscribers are connected simultaneously across thousands of cells and base stations, manual monitoring becomes impractical. Thus, automated anomaly detection methods—ranging from statistical approaches like STL decomposition and Z-score analysis to advanced machine learning models such as Isolation Forests, Autoencoders, and

LSTM-based sequence classifiers—are increasingly deployed to ensure rapid response and proactive maintenance. Effective anomaly detection not only reduces downtime and operational costs but also enhances the overall resilience and adaptability of telecom infrastructure, enabling operators to deliver consistent service in the face of complex and evolving network conditions.

Data Exploration, Preprocessing, and Cleaning

Before building any anomaly detection model, a thorough process of data exploration, preprocessing, and cleaning is essential to ensure data quality and reliability. In telecommunication networks, the KPI data collected across thousands of cells often contains inconsistencies such as missing values, duplicated entries, zeros from inactive cells, and sudden spikes due to outages or configuration changes. Our first step involved exploratory data analysis (EDA) to understand the structure and distribution of each KPI, identify outliers, and detect missing patterns over time. We visualized time series trends, examined per-cell coverage, and computed basic statistics to assess signal stability. Preprocessing began with filtering the dataset to include only valid cells with complete daily records and no zero values across all KPIs within the selected time window. Next, we handled missing data using advanced imputation methods. For short gaps, we applied linear interpolation, while longer gaps were filled using SARIMA-based forecasting, but only if the missing intervals were within an acceptable threshold (e.g., 8 days). Cells with larger gaps were excluded to avoid distorting the time series. We also normalized or scaled the features required to improve model convergence and performance. Additionally, we removed known global anomaly dates (e.g., due to national outages or maintenance) to avoid contaminating the training data. By combining statistical validation with domain-specific knowledge, we created a clean, consistent, and high-quality dataset that accurately reflects normal and abnormal behavior, providing a solid foundation for effective anomaly detection and meaningful model evaluation.

Step	**Description**	**Purpose**
1. Exploratory Data Analysis (EDA)	Visualized KPI time series, checked distributions, and analyzed missing data patterns across cells.	Understand data structure, trends, and anomalies.
2. Cell Filtering	Retained only cells with complete daily records and non-zero values across all KPIs during the selected period.	Ensure data completeness and

Step	Description	Purpose
		avoid inactive or corrupted cells.
3. Missing Data Imputation	- Short gaps filled using linear interpolation. - Long gaps (≤ 8 days) imputed using SARIMA forecasting. - Cells with >8-day gaps removed.	Recover continuity while avoiding overfitting or distortion.
4. Anomaly Date Removal	Removed known global outage or maintenance dates from the dataset.	Prevent known events from skewing model training.
5. Normalization / Scaling	Applied scaling (e.g., MinMax or StandardScaler) when needed for ML/DL models.	Improve model performance and convergence.
6. Time Index Formatting	Converted 'begintime' to pandas datetime and ensured consistent date ranges across all cells.	Enable robust time-based operations and slicing.
7. KPI Quality Checks	Verified each KPI had realistic value ranges and distributions, removed extreme outliers if unjustified.	Ensure signal reliability and avoid noise-driven anomalies.

Feature Engineering for Telecom Anomaly Detection

Feature engineering is a fundamental step in the anomaly detection pipeline, especially in the context of telecommunication networks where the raw KPI time series data is often complex, noisy, and influenced by various temporal and spatial factors. The primary objective of feature engineering is to transform this raw data into meaningful representations that enhance the model’s ability to detect abnormal behavior accurately. In telecom anomaly detection, temporal dependencies, periodic trends, and sudden spikes are crucial indicators of underlying network issues. Therefore, we focused on constructing robust temporal features that capture both short-term and long-term dynamics in the KPI signals. These include lagged features (e.g., t-1, t-2, ..., t-n), which allow models to learn from past behavior; rolling statistics such as moving averages, rolling standard deviation, min, max, and median over defined time windows to capture local trends and volatility; and trend-based features like exponentially weighted moving averages (EWMA) to emphasize recent changes. Additionally, we incorporated STL (Seasonal-Trend decomposition using

Loess) residuals to isolate irregular components from the KPI signals, enabling models to focus specifically on anomalous deviations. These engineered features serve as a foundation for both statistical and deep learning models to distinguish between normal seasonal patterns and true outliers. By enriching the original dataset with these derived signals, we significantly improved model sensitivity to subtle but critical anomalies across different KPIs and cells, leading to higher accuracy and reduced false positives in real-world deployments.

AI Models for Anomaly Detection and Their Evaluation

In this project, a range of artificial intelligence (AI) models were employed to detect anomalies in telecom Key Performance Indicator (KPI) time series, each leveraging different statistical, machine learning, and deep learning methodologies. The diversity of models was crucial to capturing the various temporal and behavioral patterns present across the network. At the core of our approach were traditional statistical methods such as STL decomposition combined with Z-score analysis, which proved effective in highlighting deviations from expected seasonal and trend components. To capture more complex data structures, we implemented unsupervised machine learning models like Local Outlier Factor (LOF) and Isolation Forest, which identify anomalous behavior based on data density and feature space isolation without requiring labeled data. These were further complemented by deep learning techniques, including LSTM Autoencoders and supervised Bi-LSTM sequence classifiers, which excel at learning temporal dependencies and capturing long-range patterns in KPI behavior. The LSTM Autoencoder was trained on normal sequences to reconstruct expected behavior and detect anomalies via reconstruction error, while the supervised Bi-LSTM classifier was trained directly on labeled anomaly windows for higher precision. For model evaluation, we adopted a comprehensive framework using both quantitative and qualitative metrics. Models were assessed based on precision, recall, and F1-score against anomaly labels derived from Prophet+Z-score and domain knowledge. Special attention was given to minimizing false negatives—critical in telecom operations—while also controlling false positives to reduce alarm fatigue. Ensemble and hybrid models were also explored by combining outputs from multiple detectors using majority voting and weighted scoring, leading to improved robustness and consistency. Visual inspection of anomaly heatmaps, time series plots, and confusion matrices further validated model effectiveness. This multi-model, multi-metric evaluation approach ensured that the final anomaly detection system was both accurate and operationally reliable in diverse network scenarios.

Module C: Geo-Search and Spatial Analysis

Module C is the Geo-Search and Spatial Analysis component of the anomaly detection system, designed to enhance situational awareness by incorporating geographic context into the detection and interpretation of network anomalies. In modern telecom networks, spatial relationships between sites play a crucial role in diagnosing and understanding performance issues, as problems in one cell can propagate to neighboring cells or result from broader regional phenomena such as power outages, weather events, or fiber cuts. This module enables users to perform spatial queries on the network infrastructure by filtering sites and cells based on attributes such as region, zone, site name, frequency band (e.g., L07, L18, L21), and anomaly status. Using geospatial data—including latitude, longitude, azimuth, and antenna configuration, Module C visualizes cell locations on an interactive map using tools like Folium or Plotly, with anomalies color-coded for immediate identification. Users can cluster nearby sites, examine anomaly distributions over regions, and analyze spatial patterns, such as hotspots of recurring faults or geographically correlated anomalies. This module also supports advanced features such as radius-based neighbor search, site-to-site proximity mapping, and integration with the anomaly detection outputs of Module B, making it possible to not only detect anomalies but also localize and contextualize them in physical space. Ultimately, Module C bridges the gap between raw anomaly signals and actionable network intelligence, enabling field engineers and network planners to make faster, data-driven decisions for diagnosis, resource allocation, and long-term optimization of the radio access network.

Module D: LLM Summary Function

Module D serves as the Large Language Model (LLM) Summary Function, a critical component that transforms raw anomaly detection outputs into human-readable insights and executive-level reports. While previous modules focus on detecting and localizing anomalies, Module D bridges the gap between technical findings and actionable understanding by leveraging the power of generative AI. Built on top of advanced LLMs such as Gemini or Open Router-compatible models, this module ingests structured inputs—including affected cells, KPIs, timestamps, geographic regions, and anomaly scores—from Module B and Module C, and converts them into comprehensive narratives, diagnostics, and strategic recommendations. The LLM is prompt-engineered to interpret multi-dimensional data and automatically detect high-level patterns, such as recurring outages at a site, KPI degradation trends over time, or regional congestion anomalies. It can summarize anomalies over a specific time window, explain possible root causes based on telecom domain knowledge, and even suggest corrective actions like parameter tuning, hardware inspections, or handover reconfiguration. The output is tailored to different user roles—from technical engineers needing granular timelines and KPI plots, to managers and decision-makers seeking concise summaries and risk assessments. By integrating natural language reporting directly into the anomaly detection workflow, Module D enhances explainability, improves incident response time, and facilitates transparent communication across teams. It also lays the foundation for fully automated reporting systems that can be deployed in real-time operational dashboards, enabling proactive network management in large-scale telecom environments.

Web Application (Streamlit Interface)

The web application, developed using Streamlit, serves as the central user interface for the entire anomaly detection system, providing an intuitive, interactive, and visually rich environment for exploring, analyzing, and interpreting network anomalies. Designed with accessibility and usability in mind, the app seamlessly integrates all functional modules—ranging from anomaly detection (Module B) and spatial analysis (Module C) to LLM-based reporting (Module D)—into a single cohesive platform. Through the app, users can upload or select KPI datasets, choose analysis parameters (e.g., date range, target KPIs, detection models), and instantly trigger real-time anomaly detection across multiple cells or sites. Results are visualized using interactive time series plots, anomaly heatmaps, and dynamic maps, allowing users to examine when and where anomalies occurred with precision. The Geo-Search interface enables filtering by region, site, or frequency band, while the LLM Summary panel automatically generates plain-language explanations and recommendations based on the detected anomalies. The app also supports multi-cell comparison, trend tracking, and downloadable reports for further offline analysis. Thanks to Streamlit's responsiveness and extensibility, the web app ensures fast performance, secure backend integration with pre-trained models, and the potential for real-time deployment in production environments. Whether used by field engineers for operational diagnostics or by network planners for performance optimization, the Streamlit app transforms complex machine learning outputs into actionable telecom intelligence, significantly enhancing visibility, collaboration, and decision-making across stakeholders.

Future Work

While the current system provides a robust and multi-faceted framework for anomaly detection in LTE networks, several avenues remain open for future enhancement and expansion. One promising direction is the integration of real-time data streams, enabling continuous monitoring and live anomaly detection at scale using online learning or streaming analytics frameworks. Additionally, future versions could incorporate advanced spatiotemporal models such as Graph Neural

Networks (GNNs) to better capture inter-cell dependencies and network topology effects. Expanding the feature set with external contextual data—such as weather conditions, power outages, and customer complaints—could further improve root cause analysis and anomaly interpretation. On the user interface side, we plan to evolve the Streamlit web app into a multi-user platform with authentication, role-based access, and alert management features to support operational teams in live environments. For the LLM module, future work includes fine-tuning domain-specific language models on telecom incident data to produce more accurate and context-aware reports, and integrating RAG (Retrieval-Augmented Generation) pipelines with knowledge bases such as vendor documentation and historical tickets. Lastly, we aim to validate and deploy the system across different network technologies (e.g., 5G) and operators to ensure generalizability and robustness in diverse real-world scenarios. These enhancements will help transform the system from a research prototype into a fully scalable, intelligent anomaly management platform for next-generation mobile networks.

Geo-Spatial Visuals

Map with all LTE sites across the country:

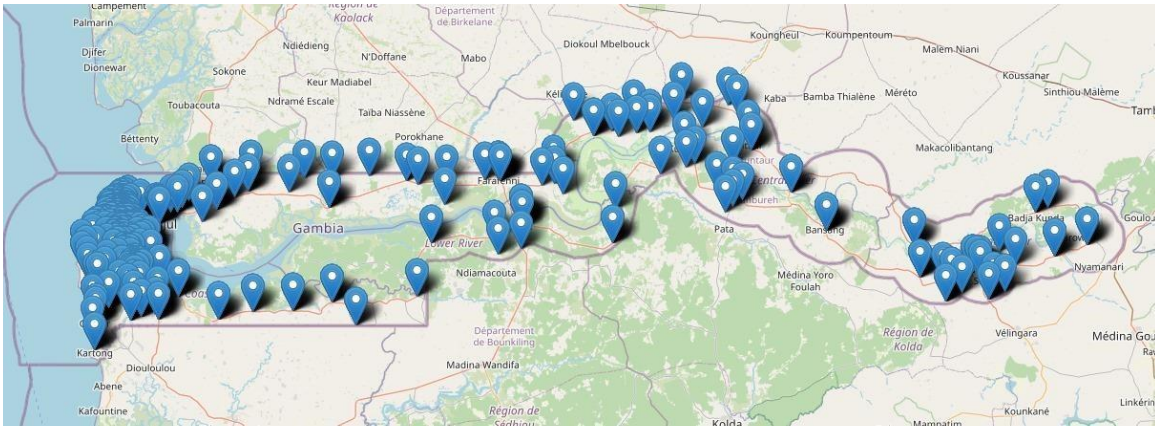

Figure 1: Geo Visualization with Site Pins

Clustered Geo Map using Voronoi diagrams:

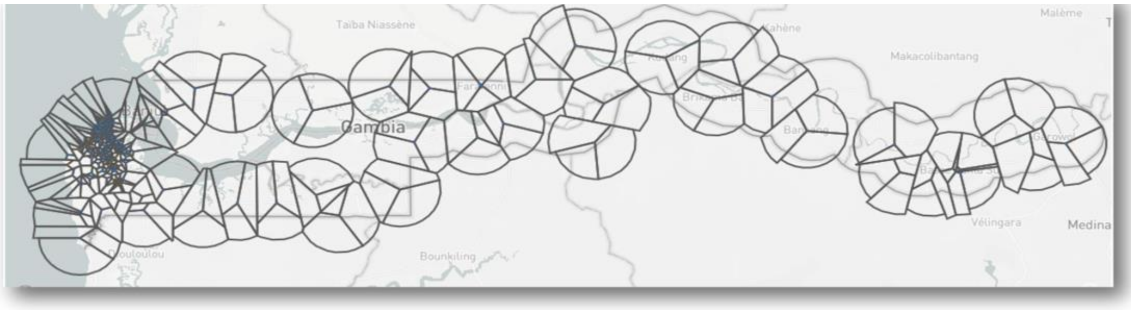

Figure 2: Geo-Spatial Clustering using Voronoi Tessellation

Observed KPIs

- L.RRC.ConnReq.Succ
- 4G DL Traffic Volume (TB)
- 4G DL PRB Utilization (%)
- 4G UL PRB Utilization (%)
- 4G UL Traffic Volume (TB)

Site Information

- Geospatial Coordinates: Latitude & Longitude
- Frequency Bands Deployed: L700, L1800, L2100
- Number of Cells: Varies per band and site
- Cell Attributes: Cell ID, Band, Azimuth