Deep Learning for Network Performance Prediction

18.04.2025

—

Overview

The increasing complexity of modern telecommunications networks driven by technologies like 4G,LTE, 5G and IoT has created many challenges in maintaining performance, reliability, and user satisfaction. This research explores the application of deep learning techniques for **predicting and enhancing network performance** across key areas like **traffic forecasting**, **fault detection**, and **quality of service (QoS) management**.

By using deep neural networks such as LSTM, CNN, Transformers, Autoencoders and GANs the study demonstrates how machine learning can automate network monitoring, reduce downtime, and improve resource allocation in real-time environments.

Goals

1. Develop deep learning models that can **predict network behavior**, identify **anomalies and faults**, and help manage **QoS parameters** (latency, throughput)
2. Compare the performance of various architectures (LSTM, CNN, Transformer, Hybrid, Autoencoder, GAN) across tasks
3. Offer a data-driven alternative to traditional network management techniques for more **scalable**, **adaptive**, and **real-time** network operations

Specifications

Data Inputs:

Time-stamped network performance data including:

1. Signal strength (dBm)
2. Latency (ms)
3. Throughput (Mbps)
4. RF measurements
5. Locality, Network Type

Models Used

1. **Anomaly Detection :** Autoencoder, GAN, LSTM, CNN
2. **Traffic Forecasting :** LSTM, CNN, Transformer, Hybrid (CNN+LSTM)
3. **QoS Prediction :** CNN, LSTM, Transformer, Hybrid Deep Learning

Links

I. Datasets: Datasets for ML project (BITS F464)
II. Google Colab (Implementation): https://colab.research.google.com/drive/1dFot1z9rtNHWhhAZHjlEVXBd4fzCob2L?usp=sharing
III. https://colab.research.google.com/drive/1-k8Vig0ABJ_pFGOIozgK37W6aFewkbo7?usp=sharing (for anomaly detection)
IV. Research Papers: Research papers for ML Project

Members

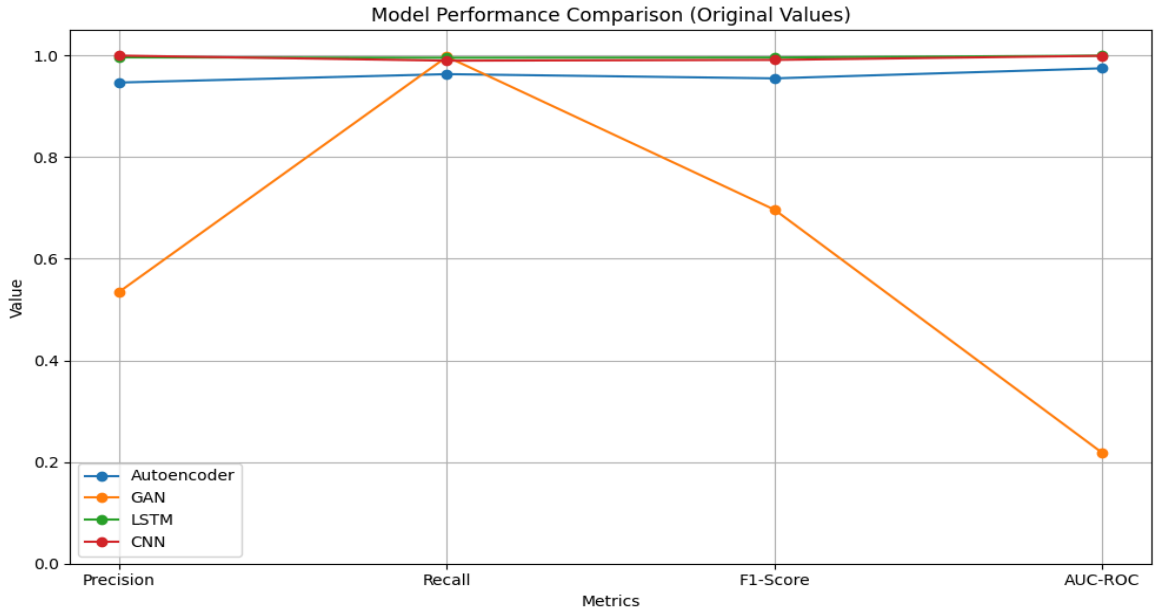
1. **Samanyu Reddy Allipuram - 2023A2PS0910H**
2. **Aarush Kanipakam - 2023A7PS1160H**
3. **Himnish Lalchandani - 2023AAPS1131H**
4. **Shantan Kadiyala - 2023A7PS0003H**

1) Anomaly Detection

Anomaly detection helps us spot unusual patterns or suspicious activity in a network like a sudden spike in traffic or strange usage behavior that could signal attacks or system faults. It's crucial for keeping networks secure and running smoothly.

Implementation Table - The following table contains the **Precision, Recall, F1 - score and AUC-ROC** of the required models

Model	Dataset	Precision	Recall	F1 - Score	AUC-ROC
Autoencoder	**Dataset 3**	**0.9470**	**0.9635**	**0.9552**	**0.9750**
GAN	**Dataset 3**	**0.5351**	**0.9978**	**0.6966**	**0.2181**
LSTM	**Dataset 3**	**0.9965**	**0.9958**	**0.9962**	**0.9999**
CNN	**Dataset 3**	**1.0000**	**0.99**	**0.9915**	**0.9996**

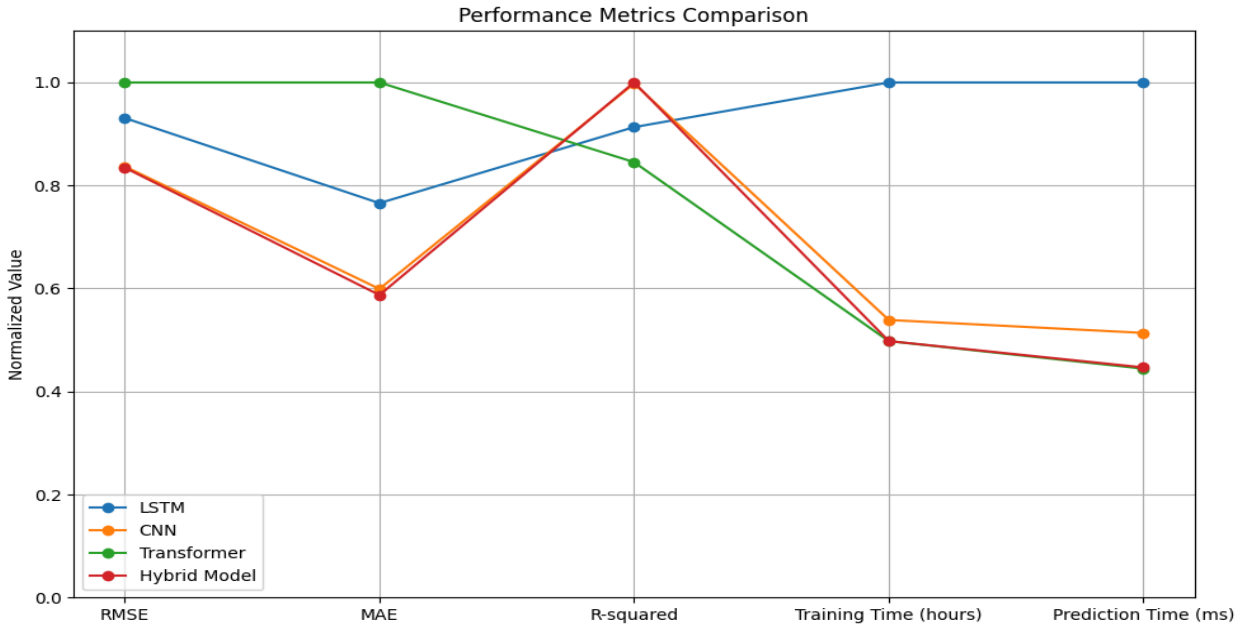


2) Traffic Forecasting prediction

Traffic forecasting is about predicting how much data will flow through a network at future times. This helps network providers manage bandwidth, prevent congestion, and plan infrastructure more efficiently.

Implementation Table - The following table contains the **RMSE, R-squared and MAE** of the required models.

Model	Dataset	RMSE	R-Squared	MAE
LSTM	Dataset1	0.149632	0.673879	0.085378
CNN	Dataset1	0.134536	0.736362	0.066808
Transformer	Dataset1	0.160726	0.623726	0.111503
Hybrid Model	Dataset1	0.134153	0.737861	0.065487

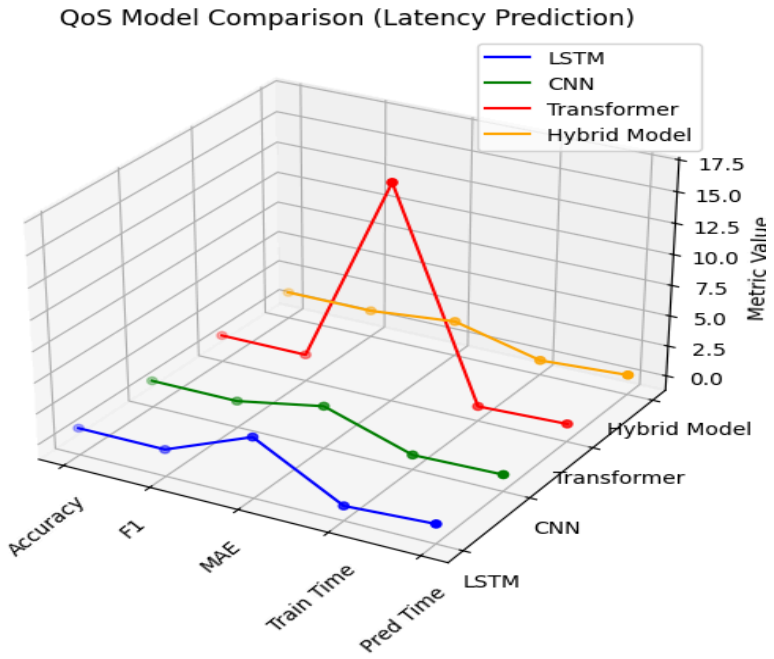


3) QoS/QoE Prediction

QoS prediction is used to estimate how well a network will perform for users—things like speed, reliability, and responsiveness. By forecasting QoS, providers can maintain a good user experience and fix issues before they affect customers.

Implementation Table - The following table contains the **Accuracy, F1-Score and MAE** of the required models.

Model	Dataset	Accuracy	F1 - Score	MAE	Prediction Time (ms)
LSTM	**Dataset1**	0.99	0.99	3.75	0.4
CNN	**Dataset1**	0.98	0.98	2.26	0.17
Transformer	**Dataset1**	0.99	0.99	16.49	0.27
Hybrid Model	**Dataset1**	1	1	1.68	0.43



Improvements and Findings

To improve upon the research paper, we explored additional model architectures and usability techniques aiming to improve both prediction performance and explainability in real-world network environments.

Traffic Forecasting and QoS Prediction

The research paper primarily focused on models such as LSTM, CNN, Transformer, and Hybrid architectures for traffic forecasting and QoS prediction. To improve upon this work, we incorporated additional deep learning architectures:

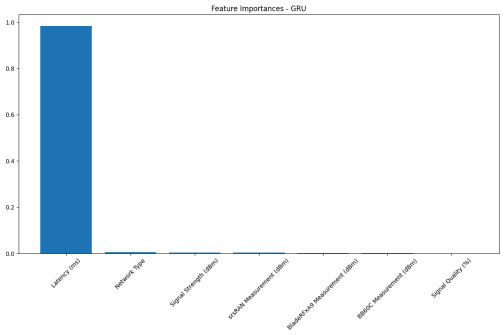
- GRU (Gated Recurrent Units): GRUs are simplified variants of LSTMs that retain performance while offering faster training. We used GRU models to better capture sequential dependencies in network data while reducing computational complexity.

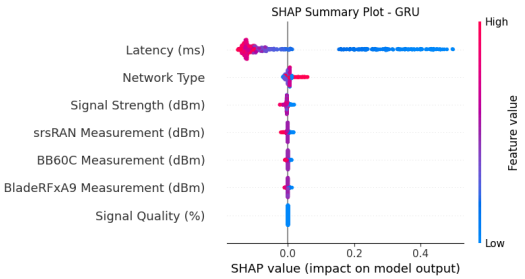
- Temporal Convolutional Networks (TCNs): TCNs apply 1D dilated convolutions over time-series data, allowing the model to efficiently capture long-range dependencies without the vanishing gradient issues common in RNNs. This made TCNs particularly suitable for forecasting future traffic and QoS metrics.

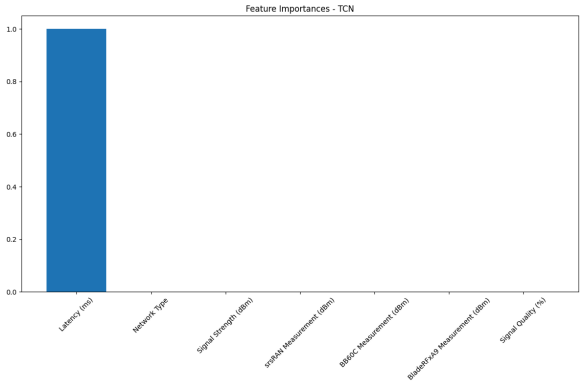
By introducing these models, we aimed to benchmark and potentially outperform the architectures used in the original paper, providing more options for handling network performance prediction.

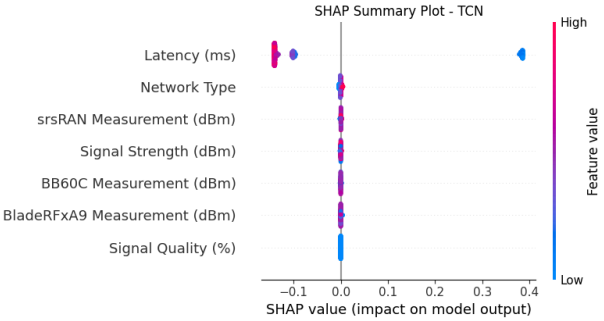
NEW MODEL	Dataset	R-squared	MSE
GRU for traffic forecasting	Dataset 1	0.642000662763454	0.024578236129165515
TCN for traffic forecasting	Dataset 1	0.7377702567497146	0.018003230395472403
GRU for QOS prediction	Dataset 1	-0.016867476504809797	3225.8856282721695
TCN for QOS prediction	Dataset 1	0.9999654079380851	0.10973901512434295

From these we can conclude that TCN is the best method found here for QOS Prediction and Traffic Forecasting.









Anomaly Detection

For anomaly detection, we focused on using advanced time series models, as the dataset contained sequential features reflecting past connection histories (e.g., `count`, `srv_count`, etc.). The models we used include:

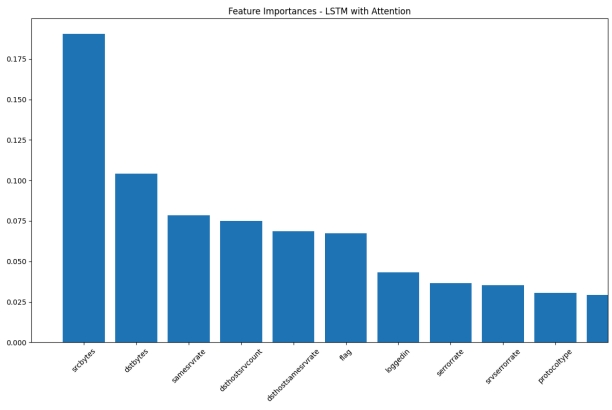
- Temporal Convolutional Networks (TCN): Employed to capture long-range temporal patterns in the data, enabling efficient identification of subtle anomalies over time.

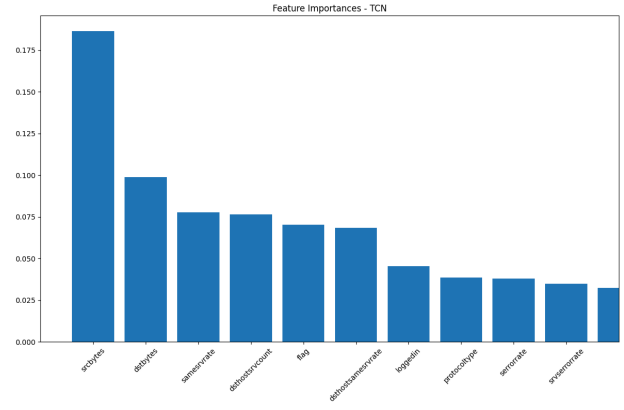
- LSTM with Attention Mechanism: Integrated attention layers on top of LSTM to allow the model to focus on the most important time steps and feature sequences when identifying potential anomalies or attacks.
  To improve interpretability of these deep learning models—which are often considered "black box"—we introduced a surrogate modeling approach:
- Surrogate Model (Random Forest): We trained a Random Forest model on the outputs of the TCN and LSTM-Attention models. This surrogate model serves as an interpretable approximation of the deep learning models' behavior, making it easier to explain decisions.

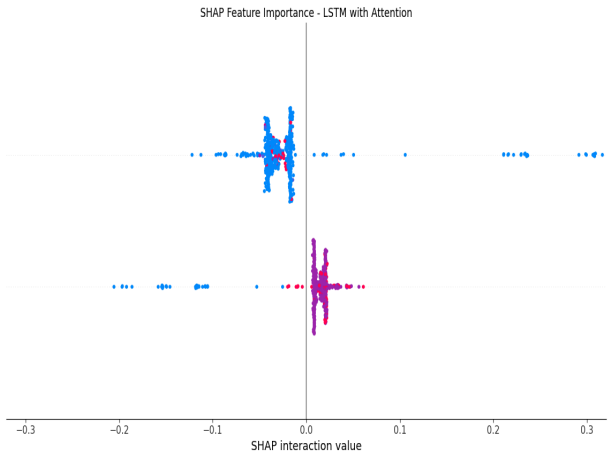
- SHAP (SHapley Additive exPlanations): We used SHAP values to highlight the most influential features contributing to model predictions. For example, in the context of anomaly detection, features like `count`, `serror_rate`, and `srv_count` were shown to have high importance in detecting suspicious or attack-like behavior.

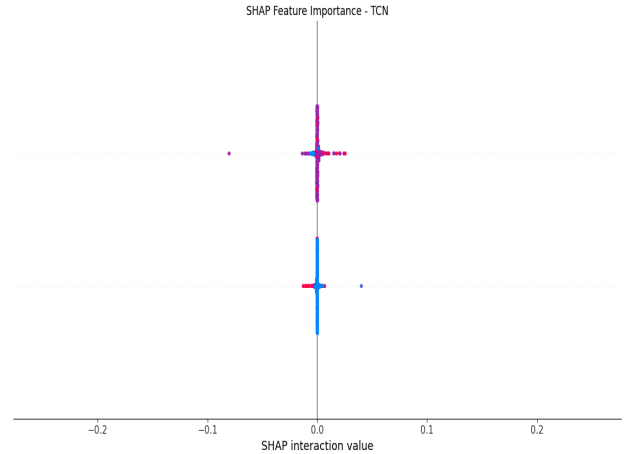
This combination of deep learning and model interpretability allows for both high performance detection and transparency, making our approach suitable for deployment in security critical network systems.

New Model	Dataset	Precision	Recall	F1 - Score	AUC-ROC
LSTM with attention	Dataset 3	0.9971	0.9961	0.9966	0.9999
TCN	Dataset 3	0.9941	0.9951	0.9946	0.9998









Contributions

MEMBERS	Contribution
Aarush Kanipakam	• Found Datasets • Worked on Traffic Forecasting and improvements
Himnish Lalchandani	• Found Datasets • Worked on Anomaly Detection Models and improvements
Samanyu Allipuram	• Found Datasets • Worked on QOS prediction models and Improvements on it
Shantan Kadiyala	Found research papers