Fake Base Station Detection At Network Side

Thesis submitted by

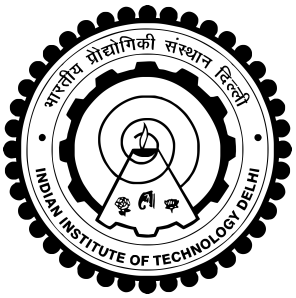
Bhuvnesh Kumar
2023MCS2011

under the guidance of

Prof. Vireshwar Kumar, Indian Institute of Technology Delhi

in partial fulfilment of the requirements
for the award of the degree of

Master of Technology



Department Of Computer Science and Engineering
INDIAN INSTITUTE OF TECHNOLOGY DELHI

July 2025

THESIS CERTIFICATE

This is to certify that the thesis titled **Fake Base Station Detection using measurement Reports at Core in 5G Network**, submitted by **Bhuvnesh Kumar (2023MCS2011)**, to the Indian Institute of Technology, Delhi, for the award of the degree of **Master of Technology**, is a bona fide record of the research work done by him under our supervision. The contents of this thesis, in full or in parts, have not been submitted to any other Institute or University for the award of any degree or diploma.

Prof. Vireshwar Kumar
Dept. of Computer Science and Engineering
IIT-Delhi

Place: New Delhi

Date: 3rd July 2025

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to my thesis advisor, **Prof. Vireshwar Kumar**, for his invaluable guidance, constant support, and insightful feedback throughout the course of this research. His mentorship has been instrumental in shaping both the direction and quality of this work.

I am also sincerely thankful to **Neha**, (PhD), for her continuous encouragement, technical insights, and timely suggestions. Her experience and patience helped me navigate through several challenges during implementation and experimentation.

ABSTRACT

The rapid evolution of mobile networks into the fifth generation (5G) brings significant advancements in data speed, latency, and connectivity. However, it also introduces new security vulnerabilities, including the threat posed by **Fake Base Stations (FBS)**—unauthorized transmitters that mimic legitimate gNBs to deceive user equipment (UE). This thesis presents a machine learning-based approach to detecting FBS in **5G networks** by analyzing **Reference Signal Received Power (RSRP)** measurements reported by UEs.

A comprehensive simulation environment was built using **NS-3 with the 5G-LENA module**, enabling accurate modeling of a dense urban microcell network comprising 12 gNBs and 300 UEs. These UEs were differentiated into two categories: **low-latency UEs** with mobility and **voice UEs** with static positions, adding realism to the scenario. One of the gNBs was designated as a fake base station with manipulated power levels, designed to deceive UEs during the initial access procedure.

Measurement data was collected by simulating real-world signal interactions and behaviors. A **regression-clustering detection pipeline** was developed using Random Forest regression and KMeans clustering to learn normal signal patterns and identify anomalies based on deviations from predicted RSRP values. The detection model was tested under multiple configurations, including varying transmission powers of both legitimate gNBs and the FBS.

To bridge simulation and real-world applicability, the **srsRAN 5G prototype** was enhanced to support full measurement reporting functionality as per **3GPP TS 38.331**, including both **periodic and event-triggered reports** (A1–A6). This enhancement enables more realistic testing and offers a foundation for future extensions like mobility-based detection or real-time analytics.

This thesis demonstrates a **practical, scalable, and standards-aligned framework** for detecting fake base stations in 5G networks using a combination of simulation, machine learning, and real-world protocol enhancements.

Contents

List of Tables

List of Figures

ABBREVIATIONS

3GPP	3rd Generation Partnership Project
AMF	Access and Mobility Management Function
ARFCN	Absolute Radio Frequency Channel Number
AUSF	Authentication Server Function
gNB	Next Generation Node B (5G base station)
CU	Central Unit of gNB
DU	Distributed Unit of gNB
DoS	Denial of Service
EPRE	Energy Per Resource Element
FBS	Fake Base Station
IMSI	International Mobile Subscriber Identity
LTE	Long Term Evolution
MAC	Medium Access Control
NAS	Network Attached Storage
NEF	Network Exposure Function
NRF	Network Repository Function
NSSF	Network Slice Selection Function
NS-3	Network Simulator 3
PCF	Policy Control Function
PCI	Physical Cell Identity
PDCP	Packet Data Convergence Protocol
RLC	Radio Link Control
RRC	Radio Resource Control
RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
RSSI	Received Signal Strength Indicator
SINR	Signal-to-Interference-plus-Noise Ratio
SSB	Synchronization Signal Block
SMF	Session Management Function
UE	User Equipment
UDM	Unified Data Management
UPF	User Plane Function

Chapter 1

INTRODUCTION

5g Network have 3 key components:

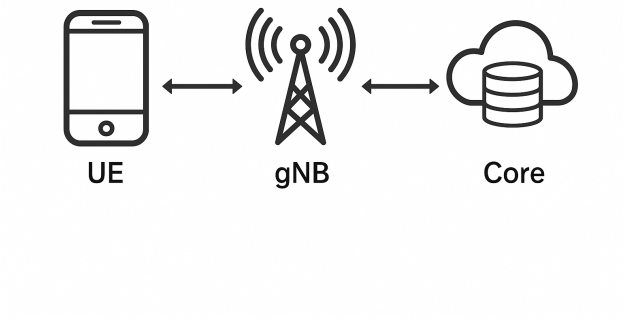


Figure 1.1: 5G Network Overview

- User Equipment (UE): The UE is the end device (Mobile Phone) used by the subscriber, It communicates with the gNB over the air interface using the 5G NR (New Radio) protocol stack.
- gNB (Next Generation Node B): The gNB is the 5G base station connecting UEs to the core network over the air interface. It handles radio access and relays data/control messages to/from the core via the NG interface. A gNB is split into:
  - CU (Central Unit): manages higher layer protocols (RRC, SDAP, PDCP)
  - DU (Distributed Unit): handles lower layers (RLC, MAC, PHY)
  - Interfaces:
    - F1 interface: connects CU and DU
    - NG interface: connects gNB to 5G Core
- 5G Core Network (5GC): The 5GC is service-based and cloud-native, enabling flexible deployment. It consists of multiple functional entities: AMF (Access & Mobility Management Function) SMF (Session Management Function) UPF (User Plane Function) AUSF (Authentication Server Function) UDM (Unified Data Management) PCF (Policy Control Function) NEF, NRF, NSSF

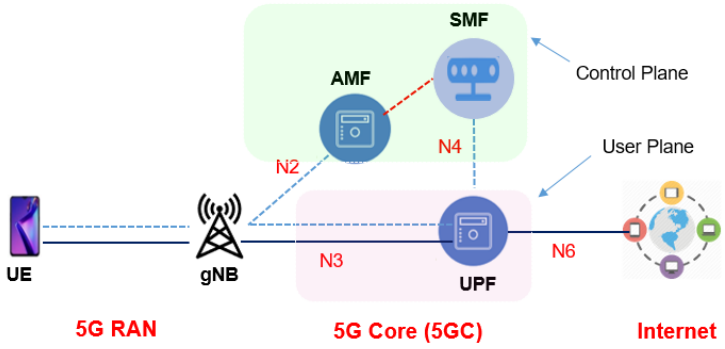


Figure 1.2: 5G Network Architecture

What is Fake Base Station ?

- Unauthorized radio transmitters that mimic legitimate base stations (gNB), tricking mobile devices into connecting to it instead of a legitimate base station.

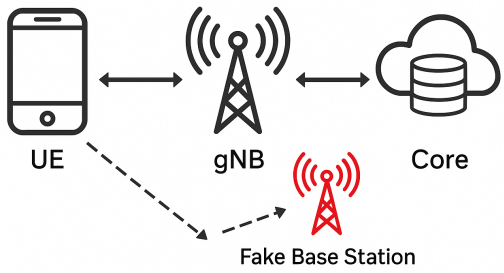


Figure 1.3: FBS in 5G Network setup

Chapter 2

MOTIVATION

Fake base stations are a serious cybersecurity and privacy threat. FBS exploits the fact that mobile phones are designed to connect to the strongest available signal without verifying the authenticity of the base station, especially at the radio access level. This vulnerability makes it easy for attackers to lure UEs (User Equipment) to connect.

Key Risks and Threats:

- **Privacy Invasion**
  - **Location Tracking**: Fake base stations can track a device's real-time location with high precision.
  - **IMSI Disclosure**: Can force devices to reveal their IMSI (International Mobile Subscriber Identity), exposing the user's identity and enabling surveillance
- **Data Interception**
  - In 2G/3G/4G networks (especially if encryption is disabled or downgraded), attackers can **intercept calls, SMS, and data traffic**.
  - Some rogue stations perform **downgrade attacks** to force a UE from 5G/4G to 2G/3G to exploit weaker security.
- **Denial of Service (DoS)**
  - A fake base station can prevent the UE from connecting to legitimate networks, cutting off all services (calls, data, emergency services).
- **Message Spoofing or Manipulation**
  - Attackers can send **fake broadcast messages**, such as emergency alerts or operator notifications, causing confusion or spreading misinformation.
- **Phishing and Malware**
  - Through false redirection (e.g., fake captive portals), users may be tricked into entering credentials or downloading malicious apps

Chapter 3

Problem Statement

The presence of fake base stations (FBS) in 5G networks poses a serious threat to user privacy and network security by exploiting vulnerabilities in the initial access and measurement procedures. This work focuses on the detection of such FBS using machine learning techniques applied to anomalous RSRP (Reference Signal Received Power) measurement reports. A simulation environment was created using ns-3 with a grid-based deployment of gNBs and UEs, where realistic RSRP data was collected under varying FBS power conditions. A regression-clustering approach using Random Forest models was trained to learn expected signal behaviors and identify deviations that indicate the presence of an FBS. The proposed method demonstrates robust detection performance across multiple power scenarios, making it suitable for practical FBS mitigation strategies in 5G networks.

3.1 Different Approaches to detect FBS:

3.1.1 At the User Equipment (UE)

Advantages:

- Immediate response: The UE can immediately disconnect or avoid connecting to a suspected FBS.
- Reduced core network load.

Limitations:

- Limited computational resources: UEs are battery-powered and have limited processing capabilities, which restricts the complexity of detection algorithms.
- Limited information: A UE only has a local view (e.g., its own measurements) and lacks global network context that might improve detection.
- Vulnerability: If the UE is compromised, the detection mechanism can be disabled or bypassed.

3.1.2 At the gNB (5G Base Station)

Advantages:

- Better computational resources: gNBs have more processing power than UEs, allowing for more sophisticated detection algorithms.
- Localized view: A gNB can collect measurements from multiple UEs in its coverage area, allowing it to detect anomalies that are consistent across several UEs (e.g., an FBS in the vicinity).
- Faster than core: While not as immediate as UE-side, it is faster than sending data to the core.

Limitations:

- Limited scope: A gNB only has information about UEs in its own cell and neighboring cells. It may not detect FBS that are outside its coverage.
- Security risks: gNBs are exposed to physical attacks and if one is compromised, it might fail to report FBS or even become an FBS itself.

3.1.3 At the Core Network

Advantages:

- Comprehensive view: The core network has a global view of the entire network, allowing it to correlate information from multiple gNBs and UEs to detect FBS more accurately.
- Advanced processing: The core can run complex machine learning models on aggregated data from the whole network.

Limitations:

- Latency: Sending measurement reports to the core and waiting for analysis introduces delay, which might be critical in fast-moving attacks.
- Signaling overhead: Transmitting large amounts of measurement data from UEs/gNBs to the core consumes more bandwidth.
- Privacy concerns: Aggregating detailed UE measurements at the core raises privacy issues and requires strict data protection measures.

3.2 Threat Model: Fake Base Station in 5G Networks

1. Adversary Capabilities

The attacker controls a rogue radio device that impersonates a legitimate 5G gNB. The fake base station is capable of:

- Broadcasting synchronization signals (SSBs) and fake system information blocks (SIBs)
- Transmitting at variable power levels to manipulate RSRP measurements
- Forcing UEs to connect by exploiting initial access procedures before authentication
- Operating independently without being part of the legitimate network's neighbor relations

The adversary may also change transmit power or physical location to evade simple detection heuristics.

2. Attack Goals

- **Hijack UE Connections**: Lure UEs away from legitimate gNBs by offering a stronger signal.
- **Eavesdrop or Intercept Data**: Especially in 4G/5G fallback scenarios where encryption may be delayed or weak.
- **Launch Denial-of-Service (DoS)**: Prevent UEs from connecting to legitimate networks.
- **Impersonate Operator Services**: Send spoofed paging or broadcast messages.

3. Attack Surface

The FBS targets vulnerabilities in the **initial access and measurement reporting phases**:

- UEs scan and rank cells by RSRP without verifying gNB legitimacy.
- The fake gNB manipulates its signal strength to appear as the strongest option.
- The attack exploits the fact that **authentication occurs after cell selection**.

4. Detection Point

In this work, detection occurs **at the 5G Core Network**, which receives measurement reports from UEs connected to various gNBs. The detection model:

- Uses statistical/machine learning analysis of UE-gNB signal behavior
- Compares predicted and actual RSRP to identify inconsistencies
- Flags gNBs with high residual errors as suspicious

5. Assumptions

- The attacker does not have access to the core network or subscriber data.
- UEs send reliable and periodic measurement reports to the core.
- Legitimate gNBs follow standard placement, power levels, and mobility configurations.
- Only **one FBS** is active at a time in the simulated setup (can be extended).
- Measurement Reports are sent from gNB to 5G Core by using a Network Attached Storage (NAS) or a database server.

6. Security Goal

- The goal is to **identify and isolate fake gNBs** by detecting statistical anomalies in RSRP measurements reported by UEs, without relying on direct physical layer access or cryptographic methods.

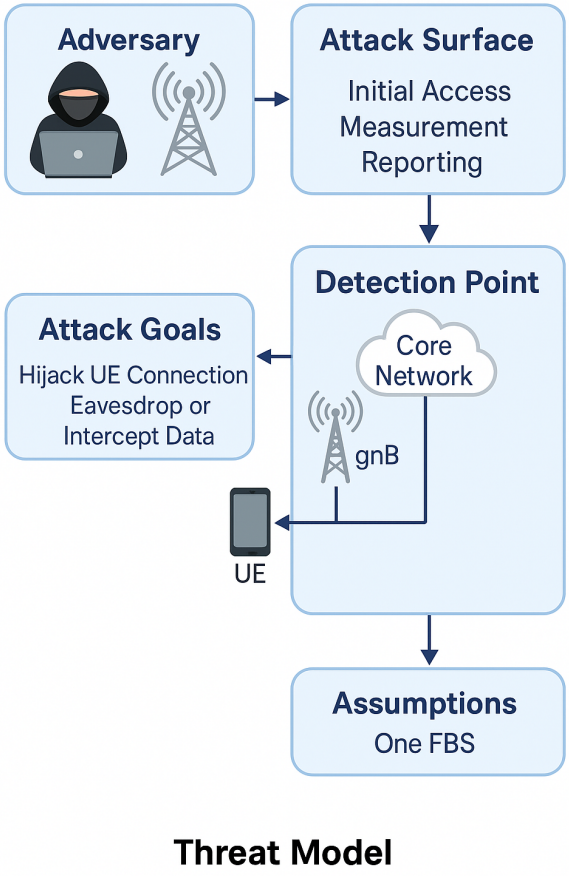


Figure 3.1: FBS Threat Model

3.3 Challenges of Fake Base Station Detection at the 5G Core

Detecting fake base stations (FBS) in 5G networks is particularly challenging, especially when the detection is performed centrally at the **5G Core Network**, relying on UE-generated reports and aggregated network data. The following are the key challenges:

1. **Delayed Visibility at the Core**
   Detection at the core relies on **periodic or triggered measurement reports** (e.g., RSRP) sent by UEs. These reports may be **delayed** or **filtered**, limiting the timeliness of detection compared to edge-based methods.

2. **Lack of Direct Radio Context**
   The core does not have direct access to physical-layer metrics like beam configurations or detailed signal propagation context. This limits its ability to distinguish between **legitimate signal degradation** and **FBS-induced anomalies**.

3. **High Variability in RSRP Measurements**
   Measurement reports received at the core reflect **natural fluctuations** in

signal due to UE mobility, fading, and interference. This makes it hard to set fixed thresholds or rules, increasing the risk of false positives or missed detections.

4. **Mimicry by Sophisticated FBS**
   Advanced FBS may closely **emulate the characteristics** of legitimate gNBs — such as timing, cell ID, or SSB structure — making them indistinguishable without **learned behavioral baselines** and anomaly detection models.

5. **UE Diversity and Reporting Frequency**
   UEs may vary in their **reporting capabilities and intervals**, resulting in **incomplete or inconsistent coverage** of gNBs in measurement data collected at the core.

6. **Network Density and Overlap**
   In dense 5G deployments, with overlapping small cells and multiple neighboring gNBs, it becomes increasingly difficult to infer abnormal behavior solely from RSRP trends at the core.

7. **Lack of Ground Truth at Inference Time**
   At the core, there is **no definitive label** indicating which gNBs are legitimate or fake during real-time operation, so detection must rely entirely on **statistical deviation** or machine-learned models trained offline.

These challenges necessitate robust, adaptive detection mechanisms at the core that can **learn normal signal patterns**, **model expected behaviors**, and **flag anomalies** based on aggregated UE reports — as proposed in this thesis through a regression-clustering-based detection pipeline using RSRP features.

Chapter 4

Related Work

Several efforts have been made to detect false base stations (FBS) using signal characteristics and advanced detection techniques. Notably, **Murat: Multi-RAT False Base Station Detector** (arXiv:2102.08780v1) presents a lightweight and efficient Rule Based method for detecting fake base stations by leveraging multi-RAT (Radio Access Technology) capabilities of user equipment. It uses a cross-verification strategy across multiple RATs (e.g., LTE, UMTS, GSM) to identify inconsistencies that are typically observed in fake base stations.

Another significant work is **Applying Machine Learning on RSRP-based Features for False Base Station Detection** (dl.acm.org/doi/10.1145/3538969.3543787), which proposes a data-driven approach to identify FBS using supervised machine learning techniques in LTE. By analyzing signal strength metrics such as RSRP (Reference Signal Received Power) and other radio parameters, the study demonstrates that models like decision trees and support vector machines can accurately distinguish legitimate base stations from rogue ones. This method highlights the effectiveness of using physical layer features and ML classifiers in detecting sophisticated FBS attacks in real-world scenarios.

Chapter 5

Background

Measurement Reports are messages sent by the **User Equipment (UE)** to the base stations (gNB) containing information about the signal conditions of the current serving cell and neighboring cells. These reports help the network make **mobility decisions**, such as **handover**, **cell reselection**, or **radio link failure recovery**.

5.1 Key Metrics in Measurement Reports:

- RSRP – Reference Signal Received Power
  - **Definition**: The **average power** received from specific reference signals transmitted by the base station.
  - **Unit**: dBm (typically ranges from –140 dBm to –44 dBm).
  - **Purpose**: Used to measure **cell coverage strength** and **detect neighboring cells**.
  - **Higher RSRP = Better signal strength**.
- RSRQ – Reference Signal Received Quality
  - Combines RSRP with RSSI (total received power including interference and noise).
  - Reflects **signal quality** (used to differentiate between two cells with similar RSRP).
- SINR – Signal-to-Interference-plus-Noise Ratio
  - Measures signal quality by comparing desired signal to background noise and interference.
  - Crucial for **throughput estimation** and **link adaptation**.

5.2 How Measurement Reports Work (Step-by-Step Process)

1. **UE Measures** signal parameters like RSRP/RSRQ/SINR for its serving cell and neighboring cells.
2. If certain **reporting criteria** (configured by the base station via RRC reconfiguration messages) are met (e.g., RSRP of neighbor > threshold), UE **triggers a Measurement Report**.

3. The **Measurement Report (MeasReport)** is sent to the base station (gNB).
4. The base station uses this info to make decisions, e.g.:
   - Initiate **handover** to a better cell.
   - **Blacklist** suspicious cells.
   - Analyze **signal degradation** or detect **fake base stations**

5.3 Role of Measurement Reports in FBS Detection

Fake base stations often:

- **Broadcast stronger RSRP** values than nearby legitimate gNBs to lure UEs in a particular area.
- **Do not have proper neighbor cell lists**, which can be detected via **incomplete measurement responses**.
- **Lack coordination** with other cells (e.g., not present in real neighbor tables).

Thus, by analyzing patterns in measurement reports, it's possible to:

- Detect **suspicious cells**.
- Train **machine learning models** on RSRP/RSRQ/SINR features to classify rogue vs. legitimate base stations.

5.4 Key Measurement Events (LTE/5G):

These are **event-based triggers** that determine when UEs send reports:

3GPP specification 38.331 specified following events defined for 5G NR.

- Event A1 (Serving becomes better than threshold)
- Event A2 (Serving becomes worse than threshold)
- Event A3 (Neighbor becomes offset better than SpCell)
- Event A4 (Neighbor becomes better than threshold)
- Event A5 (SpCell becomes worse than threshold1 and neighbor becomes better than threshold2)
- Event A6 (Neighbour becomes offset better than SCell)

These help avoid unnecessary reporting and optimize network resources.

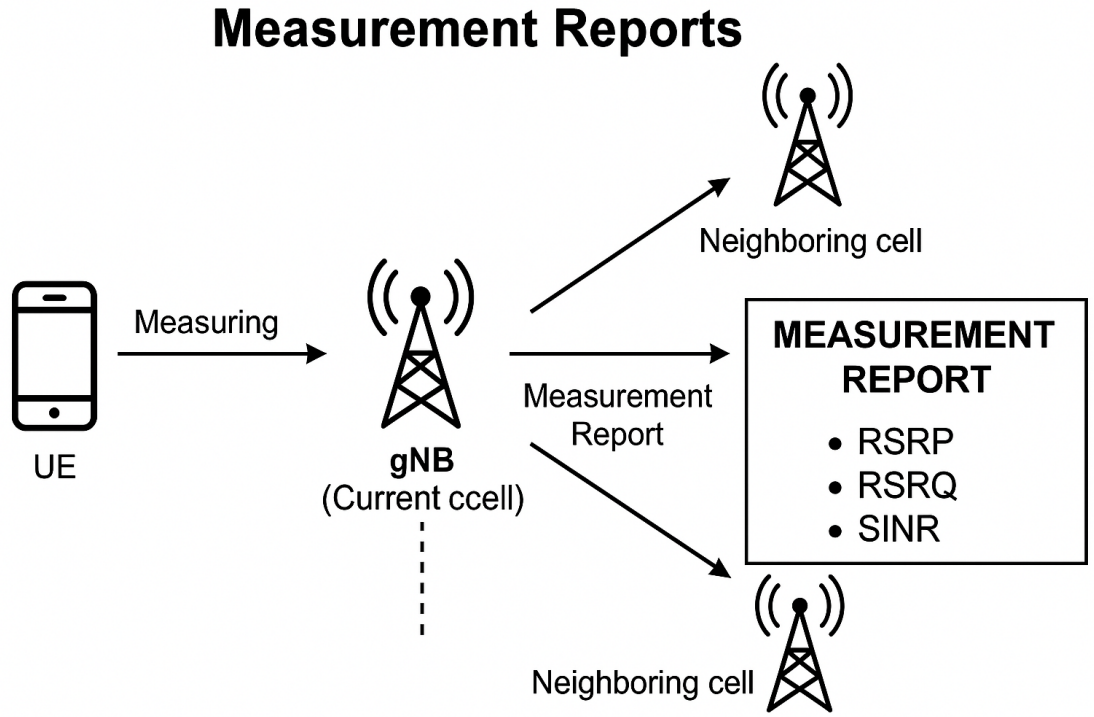


Figure 5.1: Measurement Report

Chapter 6

Experiment Setup

- To evaluate the feasibility of detecting false base stations (FBS) using RSRP-based features and machine learning, a custom simulation framework was developed using the NS-3 simulator. This section details the simulation topology, data collection methodology, and the detection pipeline inspired by the paper "Applying Machine Learning on RSRP-based Features for False Base Station Detection."
- For 5G functionalities 5G-LENA module is used.

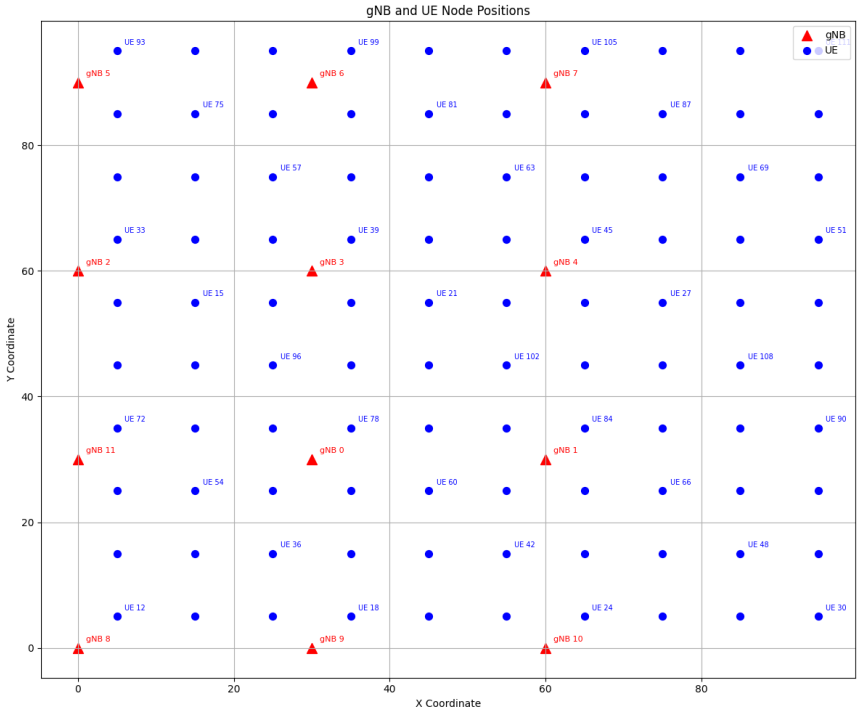


Figure 6.1: Network Layout

6.1 Network Architecture:

- The simulation scenario consists of:
  - **12 gNBs** (base stations) placed in a **4×3 grid layout**. All gNBs are fixed in position at 30m inter-station distance using the constant mobility model.
  - **300 User Equipments (UEs)** uniformly distributed throughout the area.
    - Half of these UEs are configured as Low-latency UEs with Random mobility using ***RandomWalk2dMobilityModel.***

    - Remaining half are configured as Voice UEs with Static positions using ***ConstantPositionMobilityModel***.

- The gNBs were configured to provide 5G coverage, and one of them was programmed to behave as a **fake base station** with anomalous RSRP levels.
- Two sets of UEs were used:
  - **200 UEs for training**
  - **100 UEs for testing**
- gNBs are placed at 25 meters height and UEs are placed at random heights between 1.5 to 2 meters.
- Dual Band Operation is used for UEs:
  - **Band 1 (60MHz)**
  - **Band 2 (50MHz)**
- Antenna Configuration:
  - gNB: 4x8 array (isotropic)
  - UE: 2x4 array (isotropic)
- Traffic Modeling:
  - Low-Latency Traffic (NGBR_LOW_LAT_EMBB):
    - UDP packet size: 100 bytes
    - Port: 1234
  - Voice Traffic (GBR_CONV_VOICE):
    - UDP packet size: 1252 bytes
    - Port: 1235
  - Traffic starts at 400ms, ends at 1000ms
- 3GPP Urban Microcell (UMi-Street Canyon) model is used as a path loss model which simulates dense urban areas with 3D distances (Accounts for UE/gNB height differences).

6.2 Data Collection in NS-3:

- Each UE was configured to connect to the gNB with the **maximum RSRP** using the AttachToMaxRsrpGnb() method. During the initial phase of SSB (Synchronization Signal Block), each UE scanned surrounding gNBs and recorded the RSRP values for all detected neighbors. These values represent the **received signal power from each gNB**, and form the basis for learning signal behavior in normal and anomalous (fake) conditions.
- The **x** and **y** coordinates of all entities (gNBs and UEs) were recorded using the ***netanim-module*** of NS-3 simulator.

6.3 Detection Algorithm Overview:

A custom Python-based pipeline was developed to model expected RSRP values and detect inconsistencies:

6.3.1 Feature Engineering:

- For each UE-gNB pair, spatial features were extracted:
  - Coordinates, distances, relative positions (dx, dy, distance, log(distance)).

6.3.2 Distance Filtering:

In the simulation setup, the 12 gNBs were arranged in a **4×3 grid layout**, with each gNB placed **30 meters apart both horizontally and vertically**.

To identify the neighboring gNBs for each UE during model training and testing, a **distance-based thresholding approach** was employed. Specifically, a **radius of 45 meters** was chosen as the **distance threshold**. This value was selected intentionally because it is slightly greater than the inter-site distance (30 meters), allowing only the **immediately adjacent (1-hop) neighboring gNBs** to be considered within the UE's neighborhood.

By doing this, each UE only considers gNBs that are within **one cell spacing**, thereby:

- Mimicking realistic neighbor cell measurement behavior in mobile networks.
- Filtering out the very low-power signals received from far distances.
- Enhancing the accuracy of the machine learning model by focusing on meaningful RSRP patterns from relevant nearby gNBs.

6.3.3 Training Phase:

- A **regression clustering approach** was used:
  - For each gNB, RSRP values were clustered using **KMeans (3 clusters)**.

Cluster	Signal Strength (approximate)	Interpretation
0	Strong RSRP	UE is close to gNB
1	Medium RSRP	UE is at mid distance
2	Weak RSRP	UE is far from gNB or obstructed

Table 6.1: Interpretation of RSRP Clustering Results

- For each cluster, **features** were extracted for each UE-gNB pair, and then trained a **Random Forest Regressor** on these features to predict the RSRP for that gNB.
- We used 3 clusters because 2 clusters might oversimplify (merging medium and weak signals) and 4 or more clusters may lead to overfitting or insufficient samples per cluster.

6.3.4 Testing Phase:

- For test data generation, ideally, we would have to introduce a new cell with existing PCI. But this was not supported by ns-3 because ns-3 natively avoids PCI collision by automatically assigning PCIs up to 65,535 distinct PCIs. Therefore, we envision a story as follows. We assume that one of the cells has been decommissioned, but the cell topology is not yet updated. The attacker capitalizes on this and starts its own false cell with the PCI of the decommissioned cell and lower signal strength. Mind that even though we could not simulate the exact scenario we wanted with PCI collision, the final effect is that the radio conditions (RSRP and RSRQ) will be affected and our main goal still remains valid in the sense that we want to detect changes in the radio conditions even though there is no new PCI. We generated separate testing data with each cell as decommissioned.
- For each gNB and test UE within 45 meters:
  - The trained KMeans models were used to predict which RSRP cluster the test UE falls into.
  - Use the corresponding Random Forest model to predict expected RSRP.
  - The **residual** (absolute difference between predicted and actual RSRP) was calculated for each gNB-UE pair.
  - gNBs were ranked by their **mean residuals** across all test UEs.
  - The **mean residual** across all UEs is used as a **suspicion score** for that gNB.
  - If a gNB has a significantly higher residual than others, it's flagged as a **potential fake base station**.

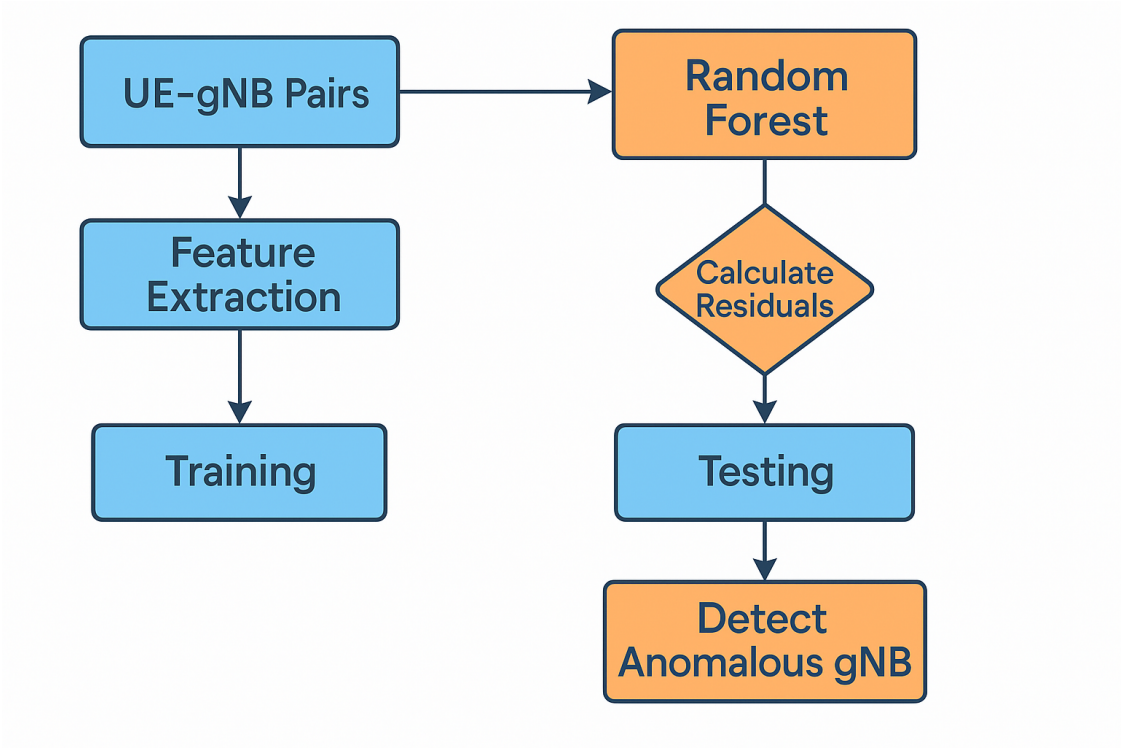


Figure 6.2: FBS Detection Pipeline

Chapter 7

Results

- We repeated this experiment with legitimate gNB's transmitting power of **32.3676 dBm** and **42.3676 dBm** and FBS transmitting power of **(~25%, ~50% and ~75%)** of the legitimate gNBs.

Actual FBS index	**Detected FBS when:(Legitimate power, FBS power)**					
	(32.3676, 7.1388)	(32.3676, 12.3676)	(32.3676, 22.7815)	(42.3676, 9.35729)	(42.3676, 22.3676)	(42.3676, 31.91)
0	0	0	0	0	0	4
1	1	1	1	3	1	4
2	2	2	2	3	2	4
3	3	3	3	3	3	3
4	4	4	4	4	4	4
5	5	5	5	5	5	5
6	6	6	6	6	6	7
7	7	7	9	7	7	7
8	8	8	9	3	7	8
9	9	9	9	3	7	9
10	10	3	9	10	10	10
11	9	3	9	11	7	7

Table 7.1: Actual vs Detected Fake base stations

- Detection Accuracy per Power Configuration:

Legitimate gNB Power (dBm)	**FBS power (dBm)**	**Correct Detections**	**Total FBS Cases**	**Detection Rate (%)**
32.3676	7.1388	11	12	91.67
32.3676	12.3676	10	12	83.33
32.3676	22.7815	8	12	66.67
42.3676	9.35729	8	12	66.67
42.3676	22.3676	9	12	75.00
42.3676	31.91	7	12	58.33

Table 7.2: Detection Accuracy per power configuration

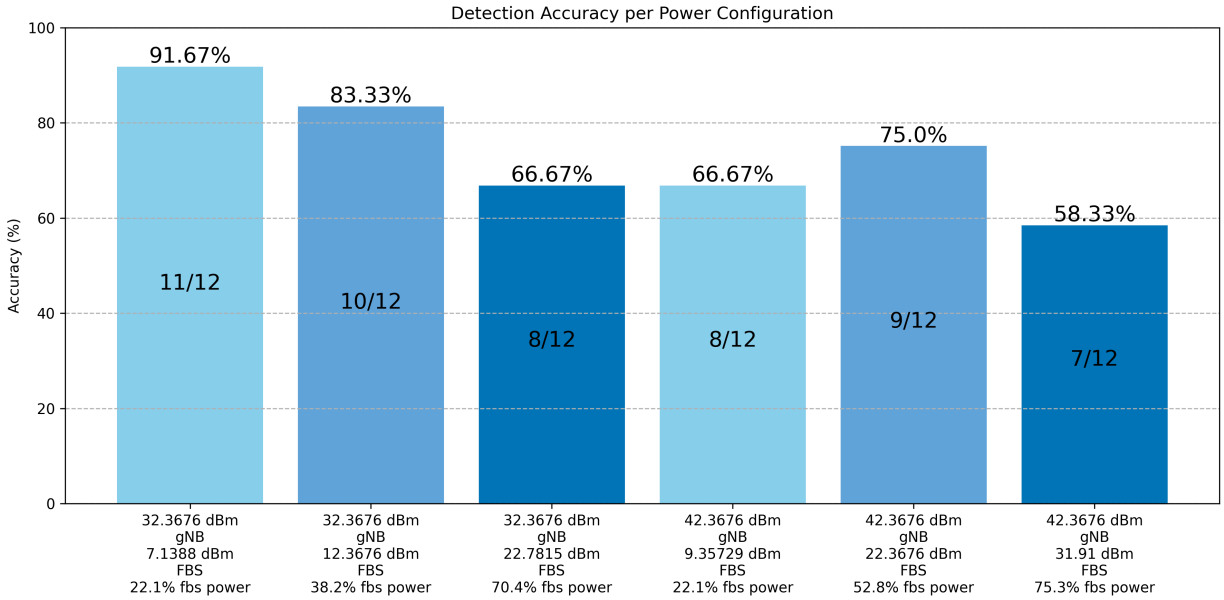


Figure 7.1: Accuracy per power configuration

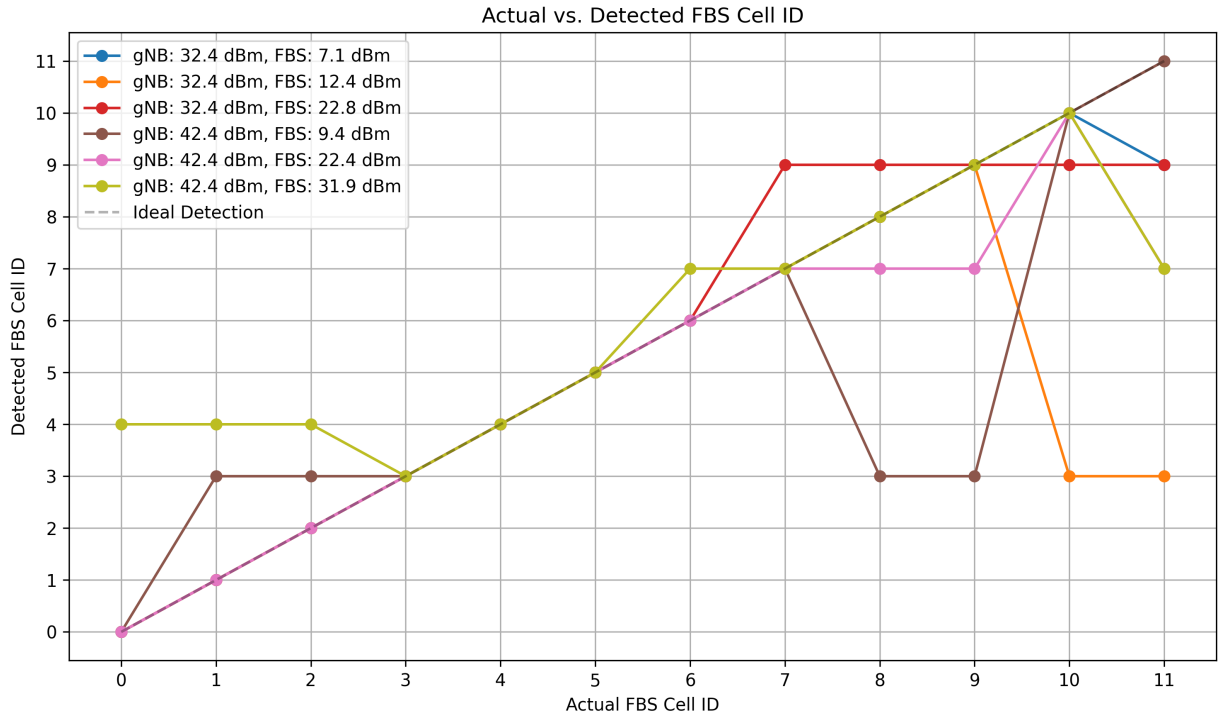


Figure 7.2: Actual vs detected FBS indices

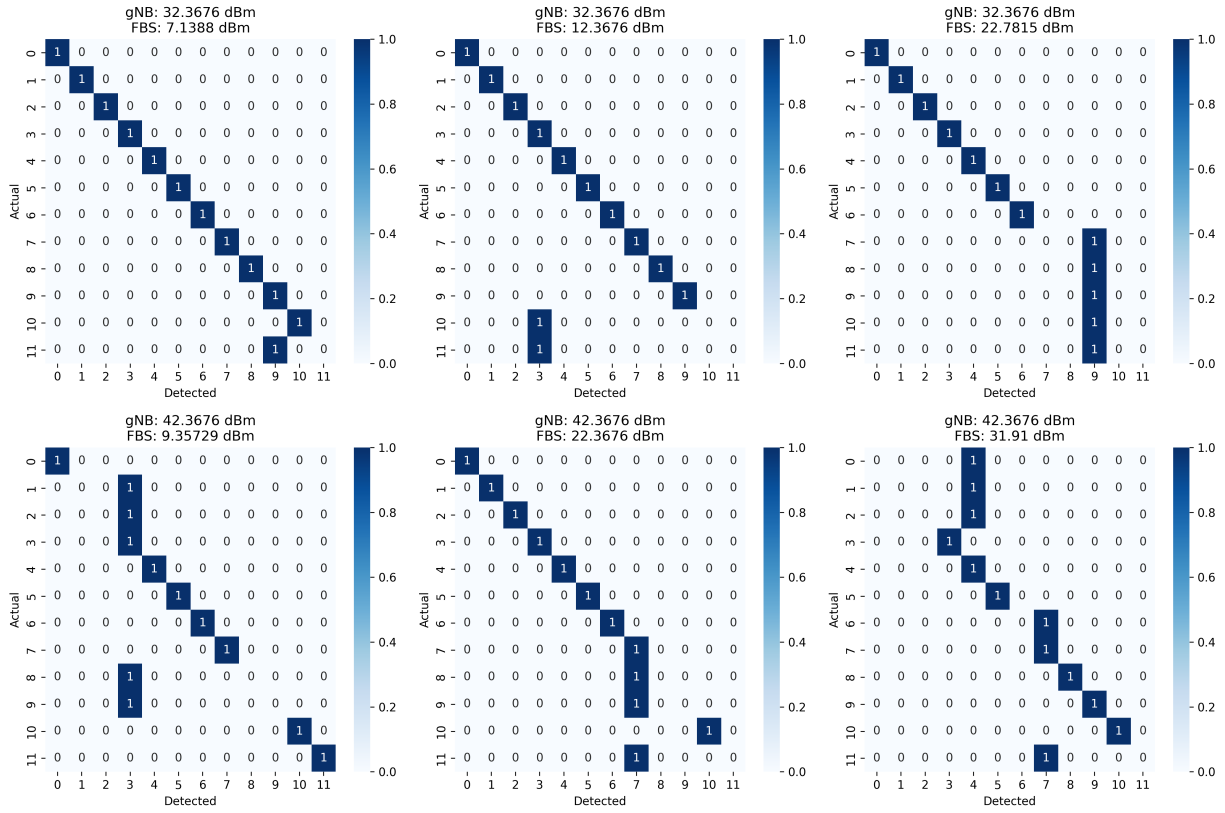


Figure 7.3: Confusion Matrices per power configuration

Chapter 8

Other Work: Implementation of Measurement Reporting in srsRAN 5G Prototype of UE

To enable intelligent decision-making and support seamless handovers in 5G networks, accurate and timely measurement reporting from the User Equipment (UE) is essential. In this implementation, the srsRAN 5G prototype has been extended to support comprehensive measurement reporting functionality, covering both periodic and event-triggered reports. Enhancements were made on both the UE and gNB sides of the simulator to accommodate flexible report generation and processing. The following sections detail the key components of the implementation.

Simulation Setup:

- Open5gs as a 5G core.
- gNB from srsRAN Project
- 5G UE prototype from srsran 4g

1. UE-Side Enhancements

The UE in srsRAN has been augmented with the capability to collect, evaluate, and transmit measurement reports as per 3GPP specifications. The following major additions were made:

1.1 Measurement Data Acquisition The first step involves acquiring the required signal strength metrics from both the serving and neighboring cells. This includes:

- **Serving Cell Measurements:** The UE continuously monitors the RSRP (Reference Signal Received Power), RSRQ (Reference Signal Received Quality) and SINR (Signal-to-Interference-plus-Noise Ratio) of the current serving cell.
- **Neighboring Cell Measurements:** Parallel to the serving cell monitoring, the UE scans the environment for neighboring cells and records their signal quality metrics, including RSRP and RSRQ.

1.2 Report Type Handling The UE has been equipped with logic to dynamically determine the type of measurement report to be generated, based on the configuration received from the gNB via RRC reconfiguration signaling. The supported report types include:

- **Periodic Reporting:**
  - Measurement reports are sent at regular intervals as specified in the configuration (e.g., every 200 ms).
  - Useful for continuous network monitoring without specific triggering events.
- **Event-Triggered Reporting:**
  - Reports are sent only when certain conditions or thresholds are met, reducing signaling overhead.
  - These are the events implemented which are specified in 3GPP specification 38.331 for 5G NR:
    * Event A1 (Serving becomes better than threshold)
    * Event A2 (Serving becomes worse than threshold)
    * Event A3 (Neighbor becomes offset better than SpCell)
    * Event A4 (Neighbor becomes better than threshold)
    * Event A5 (SpCell becomes worse than threshold1 and neighbor becomes better than threshold2)
    * Event A6 (Neighbour becomes offset better than SCell)

Each of these events is triggered based on signal measurements and timer conditions defined in the measurement configuration. The UE continuously evaluates the measurement criteria and triggers the appropriate event when the conditions are fulfilled.

1.3 RSRQ Calculation In addition to receiving RSRP values, the UE calculates RSRQ values internally to support event conditions that require quality metrics. The calculation is done as per 3GPP formulas, factoring in the total received power and the number of resource blocks.

- **Estimate RSSI:**

  Using:
  - **EPRE** (Energy Per Resource Element)
  - **Number of REs** used (**no_of_re**)
  - **N (thermal noise power) in dB** → n0_db

  Assuming EPRE and no_of_re relate to the full bandwidth used, approximate:

$$RSSI\ (linear) = EPRE\ (linear) no\_of\_re$$

- **Estimate RSRQ**

  Using:
  - **RSRP (linear)**
  - **RSSI (linear)**
  - **N** = Number of RBs (can estimate from ARFCN & bandwidth)

$$\text{RSRQ}_{\text{lin}} = \frac{N \times \text{RSRP}_{\text{lin}}}{\text{RSSI}_{\text{lin}}}$$

  And convert to dB:

$$\text{RSRQ}_{\text{dB}} = 10 \log_{10}(\text{RSRQ}_{\text{lin}})$$

1.4 Report Generation and Transmission Once the appropriate report type is determined and the triggering condition is satisfied, the UE composes the RRC Measurement Report message. This report includes identifiers, signal quality data, and event-specific details. It is then transmitted over the uplink to the gNB for further processing.

2. gNB-Side Enhancements

To ensure proper handling and evaluation of the measurement reports, corresponding updates were made at the gNB (base station) side in the simulator.

2.1 Support for All Report Types The original implementation of the srsRAN gNB was limited to handling periodic measurement reports. In this enhancement, support for all the standardized event-triggered report types (A1 to A6) has been added. The gNB now accepts and processes measurement reports based on any of the above-listed conditions.

2.2 Correction of A5 Threshold Configuration An important bug fix was implemented for **Event A5**, which involves two thresholds:

- **Threshold 1** for the serving cell.
- **Threshold 2** for the neighboring cell.

Previously, the gNB configuration for threshold 2 was incorrectly transmitted to the UE, leading to mis-triggering or suppression of the A5 event. This issue has now been corrected by properly configuring both thresholds in the RRC re-configuration message.

3. Outcomes

With the successful implementation of this measurement reporting framework:

- The UE can now autonomously assess radio conditions and report changes that impact its connectivity.
- The gNB is equipped to interpret and act on these reports, enabling scenarios such as handovers, cell reselection, or load balancing.
- Both periodic and event-driven measurement procedures are now fully supported in the prototype, aligning with 3GPP TS 38.331.

This feature greatly improves the fidelity and realism of the 5G simulation in srsRAN, making it suitable for advanced research in radio resource management, mobility, and network optimization.

4. Measurement Report prepared by UE and sent to gNB:

```
 2025-05-06T19:00:40.346302 [RRC-NR ] [D] SRB1 - Tx measurementReport (8 B)
0000: 00 00 05 e1 73 87 94 00
2025-05-06T19:00:40.346303 [RRC-NR ] [D] Content:[
{
  "UL-DCCH-Message": {
    "message": {
      "c1": {
        "measurementReport": {
          "criticalExtensions": {
            "measurementReport": {
              "measResults": {
                "measId": 1,
                "measResultServingMOList": [
                  {
                    "servCellId": 1,
                    "measResultServingCell": {
                      "physCellId": 1,
                      "measResult": {
                        "cellResults": {
                          "resultsSSB-Cell": {
                            "rsrp": 28,
                            "rsrq": 30,
                            "sinr": 118
```

```
                        }
                      }
                    }
                  }
                }
```

5. Measurement Report recieved at GNB:

```
    2025-05-06T19:00:40.592421 [RRC     ] [D] ue=0 c-rnti=0x4601: Rx SRB1 DCCH UL mea
2025-05-06T19:00:40.592422 [RRC     ] [D] ue=0 c-rnti=0x4601: Containerized measureme
 {
   "UL-DCCH-Message": {
     "message": {
       "c1": {
         "measurementReport": {
           "criticalExtensions": {
             "measurementReport": {
               "measResults": {
                 "measId": 1,
                 "measResultServingMOList": [
                   {
                     "servCellId": 1,
                     "measResultServingCell": {
                       "physCellId": 1,
                       "measResult": {
                         "cellResults": {
                           "resultsSSB-Cell": {
                             "rsrp": 28,
                             "rsrq": 30,
                             "sinr": 118
                           }
]
2025-05-06T19:00:40.592427 [CU-CP   ] [D] ue=0: Received measurement result with meas
```

Chapter 9

Novel contributions

9.1 Simulation in 5G Environment Using NS-3 + 5G-LENA (Not LTE as in Prior Work)

- **Novelty**: Prior work like Murat's or the RSRP-based ML paper conducted experiments in **LTE environments**, whereas out study leverages the **NS-3 simulator with the 5G-LENA module**, enabling simulation in **actual 5G architecture**.
- **Significance**: This allows our method to capture **5G-specific phenomena** (e.g., beamforming, dual-band) that aren't present or accurately modeled in LTE simulations.

9.2 Comprehensive Power Analysis of gNB and FBS Configurations

- **Novelty**: Unlike earlier research that used a single static power level for legitimate and fake base stations, our work evaluates detection performance under **multiple transmit power levels** of both legitimate gNBs and fake base stations.
- **Significance**: This shows **robustness and sensitivity** of our detection algorithm under realistic attack variations, making our findings more applicable to dynamic and adversarial 5G environments.

9.3 Use of Heterogeneous UEs with Different Latency Requirements

- **Novelty**: Our simulation includes **two types of UEs**:
  - Low-latency UEs with random mobility (e.g., emulating autonomous or real-time applications)
  - Voice UEs with static positions (e.g., emulating conversational services)
- **Significance**: This adds **realistic user diversity** to the experimental setup, enhancing generalizability and ensuring the model handles heterogeneous UE behavior.

9.4 Implementation of Full 5G Measurement Reporting in srsRAN UE

- **Novelty**: Extended the **srsRAN 5G prototype UE** to support full **periodic and event-triggered measurement reporting**, as defined by **3GPP TS 38.331**, including events A1–A6.
- **Significance**: This enables accurate simulation of **real-world measurement behavior** and **UE-core communication**, supporting both advanced detection and future extensions to mobility and handover scenarios.

Chapter 10

Conclusion

This thesis presents a novel and practical approach for detecting Fake Base Stations (FBS) in 5G networks using machine learning techniques applied to Reference Signal Received Power (RSRP) data collected through measurement reports. By leveraging a realistic simulation environment built with NS-3 and the 5G-LENA module, a dense urban scenario was created consisting of 12 gNBs and 300 heterogeneous UEs with varying latency requirements. A fake gNB with manipulated power configurations was introduced to emulate realistic attack scenarios.

A regression-clustering-based detection pipeline was designed using Random Forest regression and KMeans clustering, which successfully modeled expected RSRP patterns and flagged anomalies indicative of FBS behavior. The detection system demonstrated high accuracy across lower power configurations of FBS. In addition, real-world applicability was addressed by extending the srsRAN 5G prototype to support full measurement reporting functionality, adhering to 3GPP TS 38.331 specifications.

This work advances the current state of the art by (1) simulating in an actual 5G environment rather than LTE, (2) performing a detailed power-level analysis of both legitimate and fake gNBs, (3) incorporating user diversity in simulation (low-latency and static voice UEs), and (4) contributing implementation-level support for measurement reporting in 5G open-source tools.

Chapter 11

Future Enhancement

Several directions can be explored to further enhance its effectiveness and generalization:

Mobility-Aware Detection Models: Extend the model to capture temporal patterns and mobility trajectories of UEs, enabling dynamic behavior modeling for more accurate detection in high-mobility environments.

Multi-Metric Feature Fusion: Incorporate additional features such as RSRQ, SINR, and timing advance to improve detection precision and reduce false positives, especially in dense deployments.

Distributed Detection Mechanism: Collaborate detection logic across the edge (UE/gNB) and core to enable a hierarchical and more efficient detection strategy, minimizing latency and load on central systems.

Adversarial Robustness and Adaptive Models: Investigate adversarial machine learning techniques to make the detection system resilient against sophisticated FBS attackers who mimic legitimate signal characteristics.

Multiple FBS Detection and Localization: Expand the system to detect and geolocate multiple simultaneously active FBS instances using spatial correlation of measurement anomalies from various UEs.

Real-World Deployment and Validation: Deploy the model in testbeds or real 5G environments using commercial off-the-shelf equipment to validate effectiveness under practical conditions and refine model assumptions.

Through these extensions, the proposed system can evolve into a more comprehensive, scalable, and production-ready solution for securing next-generation mobile networks against FBS-based threats.

Bibliography

5G-Architecture Diagram:
http://telcosought.com/5g-core/service-based-architecture-for-5g-system/,

5G-measurement report Events:
https://www.techplayon.com/5g-nr-measurement-events/,

5G-lena (NR) Module for NS-3:
https://gitlab.com/cttc-lena/nr,

srsRAN 5G Project for gNB:
https://github.com/srsran/srsRAN_Project,

Open5gs as a 5G core in srsRAN setup:
https://github.com/open5gs/open5gs,

5G UE prototype:
https://github.com/srsran/srsran_4g,

NS-3 Simulator:
https://github.com/nsnam/ns-3-dev-git,

References

1. Prajwol Kumar Nakarmi , Mehmet Akif Ersoy , Elif Ustundag Soykan and Karl Norrman "Murat: Multi-RAT False Base Station Detector" 2021.

2. Prajwol Kumar Nakarmi Jakob Sternby Ikram Ullah "Applying Machine Learning on RSRP-based Features for False Base Station Detection" 2022.