Iran University of Science and Technology

Computer Engineering Department

Detection of Unauthorized Repeaters in Mobile Networks Using Drive Test Data and Statistical Anomaly Detection

Course Project Report

Wireless Networks

Sajad Mirjalili - Mohammad Hossein Haghdadi - Parsa Shafiee

Supervisor:

Dr. Abolfazl Deyanat

January 2026

Abstract [1]

Unauthorized repeaters significantly degrade mobile network quality by introducing interference and coverage anomalies. This project presents an automated solution for detecting these devices using standard drive test measurements and statistical anomaly detection. A realistic LTE network environment was simulated for Tehran using the Cost-231 Hata model, incorporating dual-path signal propagation combined in the linear power domain. The proposed detection algorithm identifies signal strength anomalies using a robust one-sided z-score analysis, followed by DBSCAN spatial clustering to filter noise and estimate repeater locations. Experimental results demonstrate a 100% detection rate with localization errors typically between 200-500 meters, proving the method's effectiveness without the need for specialized RF scanning equipment or prior knowledge of repeater parameters.

Keywords

Unauthorized Repeater Detection, Mobile Networks, Drive Test, Statistical Anomaly Detection, Signal Propagation Modeling, Cost-231 Hata Model, LTE Networks, Network Quality Assurance

[1] Code available at: `https://github.com/SajadMRjl/Illegal-Repeater-Detection`

Contents

List of Tables

Chapter 1

Introduction

While mobile networks are critical infrastructure, their signal integrity is increasingly compromised by the deployment of unauthorized repeaters. These devices, installed by third parties to boost local coverage, introduce severe technical challenges including pilot pollution, timing desynchronization, and interference with frequency planning. Unlike authorized equipment, these repeaters operate without coordination, effectively masking genuine coverage gaps and complicating network optimization. Traditional detection methods—ranging from manual site inspections to specialized RF scanning—are often cost-prohibitive and unscalable for large urban environments. This project addresses this operational gap by proposing an automated, data-driven detection framework using standard drive test measurements.

1.1 Problem Statement

The core problem addressed in this project is the detection and localization of unauthorized repeaters in mobile networks using only drive test data. Specifically, the challenge involves:

1. **Baseline Contamination**: Unauthorized repeaters alter the local signal distribution, skewing the very statistics (mean and standard deviation) used to define 'normal' coverage. A core challenge is establishing a robust baseline in the presence of this contamination without prior knowledge of repeater locations.

2. **Spatial Localization**: Once anomalies are detected, the repeater location must be estimated

from spatially distributed measurements. This requires spatial analysis techniques that can handle noisy data and irregular measurement patterns.

3. **Scalability**: The detection method must scale to large urban environments with dozens of base stations and thousands of measurement points. Computationally intensive approaches that work in simulation may not be practical for real-world deployment.

4. **Resource Constraints**: Network operators need solutions that work with existing drive test data collection infrastructure. Methods requiring specialized equipment, additional sensors, or manual verification are not cost-effective.

Existing detection methods either require expensive specialized equipment (spectrum analyzers, direction-finding systems) or rely on time-consuming manual processes (physical inspections, customer complaint analysis). There is a need for an automated, cost-effective method that leverages existing data sources to detect and localize unauthorized repeaters with acceptable accuracy.

1.2 Research Objectives

The primary objective of this project is to develop and validate a statistical anomaly detection system for identifying unauthorized repeaters in mobile networks using drive test measurements. The specific objectives include:

1. **Develop a Realistic Simulation Environment**: Construct a synthetic LTE network for Tehran that accurately models urban path loss (Cost-231 Hata), dual-path signal propagation, and environmental shadowing to generate realistic drive test datasets.

2. **Design a Robust Detection Algorithm**: Engineer a statistical anomaly detection pipeline that utilizes one-sided z-scores to isolate repeater signals from environmental noise, followed by DBSCAN clustering for precise spatial localization.

3. **Validate System Performance**: Quantitatively assess the system's detection rate, localization accuracy, and sensitivity to parameters (e.g., repeater gain, grid density) to ensure operational feasibility.

1.3 Scope and Limitations

1.3.1 Scope

This project focuses on the following aspects:

- **Geographic Area**: The simulation is conducted for Tehran, Iran, representing a dense urban environment with realistic geographic constraints.
- **Network Technology**: The system models LTE networks operating in the 1800 MHz frequency band (LTE Band 3), which is widely deployed in urban areas.
- **Propagation Model**: The Cost-231 Hata urban propagation model is used for path loss calculation, suitable for frequencies between 1500-2000 MHz in metropolitan areas.
- **Detection Method**: The approach uses statistical anomaly detection based on received signal strength indicators (RSSI) from drive test data, combined with DBSCAN spatial clustering for localization.
- **Repeater Characteristics**: The study considers simple amplify-and-forward repeaters with gains between 50-80 dB, which are typical for unauthorized installations.
- **Data Source**: The method relies exclusively on drive test measurements (RSSI values), which are routinely collected by network operators for quality assessment.

1.3.2 Limitations

The following limitations should be considered when interpreting the results:

1. **Simulation Environment**: The project uses synthetic data rather than real-world measurements. While the propagation models and noise characteristics are realistic, actual field conditions may introduce additional complexities not captured in the simulation.
2. **Simplified Propagation Model**: The Cost-231 Hata model, while widely used, represents an average urban environment. Site-specific factors such as building heights, terrain variations, and specific urban morphology are not individually modeled. This might lead to false positives in real data.

3. **Repeater Types**: The detection algorithm is optimized for simple amplify-and-forward repeaters. More sophisticated repeaters with frequency conversion, time-shifting, or adaptive gain control may exhibit different signal characteristics.

4. **Measurement Density**: Detection accuracy depends on the density and distribution of drive test measurements. Areas with sparse measurements may result in lower localization accuracy.

5. **Environmental Noise**: While log-normal shadowing is included to model environmental variations, other effects such as fast fading, mobility-induced Doppler shift, and interference from adjacent cells are not explicitly modeled.

6. **Computational Scalability**: The current implementation processes measurements sequentially. For very large-scale networks (hundreds of BTS, millions of measurement points), optimization or parallelization may be required.

1.4 Structure of the Report

The remaining sections of this document are structured as follows. In chapter 2, we present the fundamental concepts and technical background necessary to understand the project, including mobile network architecture, signal propagation models, drive test procedures, and anomaly detection techniques. In chapter 3, we review existing approaches to repeater detection and compare their strengths and limitations with our proposed method. Finally, in chapter 5, we summarize the project outcomes, discuss the results, and propose directions for future work and improvements.

Chapter 2

Concepts and Technical Background

This chapter presents the fundamental concepts and technical background necessary to understand the repeater detection methodology. We begin with an overview of mobile network architecture in section 2.1, focusing on LTE systems and their key components. In section 2.2, we discuss the purpose and problems of unauthorized repeaters. section 2.3 covers signal propagation models used in the simulation. section 2.4 explains drive test procedures and measurements. Finally, section 2.5 introduces the statistical and clustering techniques employed in the detection algorithm.

2.1 Mobile Network Architecture

Mobile networks consist of several key components that work together to provide wireless communication services. Understanding this architecture is essential for comprehending how unauthorized repeaters affect network operation.

2.1.1 LTE Network Components

Long-Term Evolution (LTE) networks form the basis of modern 4G mobile communications. For repeater detection, two components are critical:

- **User Equipment (UE)**: Mobile devices that measure received signal strength (RSSI, RSRP) from base stations. These measurements form the drive test data used for detection.

- **Base Transceiver Station (BTS/eNodeB)**: Radio transmitters operating at known locations and power levels. BTSs create predictable coverage patterns that can be modeled using propagation equations. Deviations from predicted patterns indicate anomalies.

2.1.2 Frequency Bands and Radio Resources

LTE operates in various frequency bands allocated by regulatory authorities. This project focuses on:

- **Frequency**: 1800 MHz (LTE Band 3), widely used in urban areas worldwide
- **Bandwidth**: Typically 10-20 MHz channel bandwidth
- **Duplexing**: FDD (Frequency Division Duplexing) with separate uplink and downlink frequencies

2.1.3 Coverage Planning

Network operators carefully plan cell site locations to ensure:

- Adequate coverage in the service area
- Manageable interference between cells
- Efficient frequency reuse
- Capacity to handle user demand

Unauthorized repeaters disrupt this planning by introducing uncontrolled signal amplification that extends coverage beyond intended boundaries and creates interference.

2.2 Repeaters in Mobile Networks

2.2.1 Authorized Repeaters

Repeaters are devices that receive, amplify, and retransmit radio signals. Network operators sometimes deploy authorized repeaters to:

- Extend coverage in areas difficult to reach with traditional base stations
- Fill coverage gaps in buildings, tunnels, or rural areas
- Improve indoor coverage without installing new base stations

Authorized repeaters are carefully engineered, coordinated with the network plan, and configured with appropriate gains and filters to avoid interference.

2.2.2 Unauthorized Repeaters

Unauthorized repeaters are installed by third parties (building owners, businesses, individuals) without operator approval. Common characteristics include:

- **Amplification Gain**: Typically 50-80 dB, sufficient to significantly boost signals
- **Frequency**: Operate on the same frequencies as the serving base station (amplify-and-forward)
- **Coverage Range**: Can affect areas within 500-1000 meters of the repeater
- **Installation Location**: Often placed 300-600 meters from the serving BTS to receive adequate input signal

2.2.3 Problems Caused by Unauthorized Repeaters

Unauthorized repeaters create several technical problems:

1. **Interference**: Signals are retransmitted beyond their intended coverage area, causing pilot pollution and interference with neighboring cells.
2. **Time Delay**: The amplification process introduces additional signal delay, which can cause timing synchronization issues in the network.
3. **Noise Amplification**: Along with the desired signal, repeaters also amplify noise and interference, degrading signal quality.
4. **Unpredictable Coverage**: The coverage pattern becomes irregular and difficult to model, complicating network optimization.
5. **Regulatory Violations**: Operating radio transmitters without proper authorization violates telecommunications regulations in most countries.

2.3 Signal Propagation Models

Accurate modeling of radio signal propagation is essential for predicting coverage and detecting anomalies caused by repeaters.

2.3.1 Path Loss

Path loss represents the reduction in signal power as electromagnetic waves propagate through space. It depends on:

- Distance between transmitter and receiver
- Frequency of operation
- Environment (urban, suburban, rural)
- Antenna heights
- Obstacles and terrain

2.3.2 Cost-231 Hata Urban Model

This project employs the Cost-231 Hata model, an empirical propagation model widely used for urban environments. The path loss is calculated as:

$$PL(d) = 46.3 + 33.9\log_{10}(f) - 13.82\log_{10}(h_b) + (44.9 - 6.55\log_{10}(h_b))\log_{10}(d) + C_m \tag{2.1}$$

where:

- $PL(d)$: Path loss in dB at distance d
- f: Frequency in MHz (1500-2000 MHz)
- h_b: Base station antenna height in meters
- d: Distance in kilometers
- C_m: Correction factor (3 dB for metropolitan areas)

2.3.3 Received Signal Strength

The received power at a mobile device is calculated using the Friis transmission equation:

$$P_r = P_t + G_t + G_r - PL(d) \tag{2.2}$$

where:

- P_r: Received power in dBm
- P_t: Transmit power in dBm (typically 43-46 dBm for LTE)
- G_t: Transmit antenna gain in dBi (10-18 dBi for sector antennas)
- G_r: Receive antenna gain in dBi (0 dBi for mobile devices)
- $PL(d)$: Path loss in dB

2.3.4 Log-Normal Shadowing

Real-world environments exhibit variations in signal strength due to buildings, trees, and terrain. This is modeled as log-normal shadowing:

$$RSSI_{measured} = RSSI_{predicted} + X_\sigma \tag{2.3}$$

where X_σ is a zero-mean Gaussian random variable with standard deviation σ (typically 6-10 dB in urban areas). This project uses $\sigma = 4$ dB to represent environmental variations.

2.3.5 Dual-Path Signal Propagation: Critical Implementation Detail

When an unauthorized repeater is present, electromagnetic waves reach the measurement point via two independent propagation paths:

1. **Direct Path**: BTS → Mobile Device
2. **Repeater Path**: BTS → Repeater → Mobile Device (amplified)

The Physics of Power Combination

This dual-path scenario requires careful treatment. When an unauthorized repeater is present, the User Equipment (UE) receives a superposition of two distinct signal components: the direct line-of-sight signal from the BTS and the amplified, time-delayed signal from the repeater. Since these signals are uncorrelated in phase due to the large path difference ($> \lambda$), they combine non-coherently. Therefore, the total received power must be calculated by summing the individual signal powers in the linear (milliwatt) domain before converting back to the logarithmic (dBm) domain. Simple algebraic addition of dBm values would lead to significant modeling errors.

$$P_{total}^{linear} = P_{direct}^{linear} + P_{repeater}^{linear} \tag{2.4}$$

Converting to/from dBm:

$$P_{total} = 10 \log_{10} \left(10^{P_{direct}/10} + 10^{P_{repeater}/10} \right) \tag{2.5}$$

2.4 Drive Test and Measurements

2.4.1 Drive Test Concept

Drive testing is a standard procedure used by mobile network operators to assess network quality and coverage. It involves:

- Driving or walking through the coverage area with specialized measurement equipment
- Recording signal strength (RSSI, RSRP, RSRQ) from serving and neighboring cells
- Logging GPS coordinates for each measurement
- Collecting data on call quality, data throughput, and handover success

2.4.2 Key Measurements

The most important measurement for repeater detection is:

Definition 1. ***RSSI (Received Signal Strength Indicator)****: The total received power measured at the mobile device antenna, typically expressed in dBm. RSSI includes the desired signal plus noise and interference. Typical values range from -50 dBm (very close to base station) to -110 dBm (cell edge).*

While RSRP provides the power of specific reference signals, RSSI is selected as the primary metric for this study because it represents the total wideband power. Unauthorized amplify-and-forward repeaters boost the entire channel bandwidth—including noise and interference—making RSSI a more sensitive indicator of total spectral energy injection than reference-signal-only metrics.

Other measurements collected during drive tests include:

- RSRP (Reference Signal Received Power): Power of LTE reference signals
- RSRQ (Reference Signal Received Quality): Quality metric accounting for interference
- SINR (Signal-to-Interference-plus-Noise Ratio): Measure of signal quality
- Cell ID: Identifier of the serving cell

2.4.3 Measurement Grid

In this project, drive test measurements are simulated on a regular grid:

- Grid spacing: 100 meters (configurable)
- Coverage area: Tehran metropolitan area (approximately 5 km × 5 km)
- Total measurement points: Typically 2500-3000 points
- Measurements per BTS: RSSI from all detectable base stations

2.5 Anomaly Detection and Clustering

2.5.1 Statistical Anomaly Detection

The core of the repeater detection algorithm is identifying measurement points where the actual signal strength is significantly higher than expected. This is formulated as an anomaly detection problem.

Residual Calculation

For each measurement point, we calculate the residual:

$$r_i = RSSI_{measured,i} - RSSI_{predicted,i} \tag{2.6}$$

where:

- $RSSI_{measured,i}$: Actual measurement (includes repeater effects)
- $RSSI_{predicted,i}$: Expected value based on propagation model (no repeaters)

Z-Score Analysis with Robust Statistics

To identify anomalies, we use a one-sided z-score test with a critical methodological innovation:

$$z_i = \frac{r_i - \mu_r}{\sigma_r} \tag{2.7}$$

where:

- μ_r: **Median** of all residuals
- σ_r: Standard deviation estimated **from negative residuals only**
- z_i: Z-score for measurement i

Theorem 1. *A measurement point is classified as anomalous if $z_i > z_{threshold}$ (typically 2.5), indicating the signal is unusually strong compared to the expected distribution.*

The Masking Effect and Robust Estimators

The choice of median and negative-residual standard deviation is not arbitrary. A fundamental challenge in repeater detection is that the anomalies (high-power repeater signals) contaminate the dataset used to establish the baseline. Standard statistical moments, such as the arithmetic mean and sample standard deviation, are highly sensitive to such outliers.

A strong repeater signal would inflate the calculated mean and standard deviation of the residuals, effectively raising the detection threshold ($z_{threshold}$) and causing the algorithm to miss the very anomaly it is designed to detect—a phenomenon known as the *masking effect.*

To mitigate this, we employ **robust estimators**:

1. **Location**: The *median* of the residuals (μ_r) is used as the baseline, as it is invariant to extreme outliers. Even with significant repeater contamination, the median remains anchored to the true environmental baseline.
2. **Scale**: The *semi-standard deviation* (calculated only from negative residuals) is used to estimate the noise floor. Since repeaters only add power (creating positive residuals), the negative residuals represent the clean, ambient noise distribution of the environment.

$$\sigma_r = \sqrt{\frac{1}{N_{neg}} \sum_{r_i < \mu_r} (r_i - \mu_r)^2} \tag{2.8}$$

This robust statistical framework enables detection without prior knowledge of repeater locations or requiring clean ”training” data.

2.5.2 DBSCAN Clustering

Density-Based Spatial Clustering of Applications with Noise (DBSCAN) is used to group anomalous measurement points spatially.

DBSCAN Algorithm

DBSCAN identifies clusters based on density connectivity:

- **Core Point**: A point with at least $minPts$ neighbors within radius ϵ
- **Border Point**: A point within ϵ of a core point but with fewer than $minPts$ neighbors
- **Noise Point**: A point that is neither core nor border

For this application:

- $\epsilon = 300$ meters: Maximum distance between points in a cluster
- $minPts = 3$: Minimum points required to form a cluster

Advantages for Repeater Detection

DBSCAN is well-suited for this problem because:

1. It does not require specifying the number of clusters in advance
2. It automatically filters isolated noise points (false positives)
3. It can find clusters of arbitrary shape
4. It handles clusters of varying density

2.5.3 Repeater Localization

Once anomaly clusters are identified, the repeater location is estimated using weighted centroid:

$$\hat{lat}_{repeater} = \frac{\sum_{i \in C} z_i \cdot lat_i}{\sum_{i \in C} z_i} \tag{2.9}$$

$$\hat{lon}_{repeater} = \frac{\sum_{i \in C} lon_i \cdot z_i}{\sum_{i \in C} z_i} \tag{2.10}$$

where C is the set of anomalous points in the cluster, and z_i are the z-scores (confidence weights). Points with higher anomaly scores contribute more to the estimated location, improving accuracy.

Chapter 3

Related Work and Methodology

This chapter reviews existing approaches to unauthorized repeater detection in mobile networks and presents the methodology employed in this project. We first examine various detection techniques proposed in the literature, ranging from traditional hardware-based scanning to modern statistical analysis. We then present our implementation approach, detailing the simulation framework, detection algorithm, and validation methodology.

3.1 Existing Repeater Detection Approaches

The detection of unauthorized signal sources is a well-established problem in telecommunications. Existing methods can be broadly categorized into hardware-centric physical layer techniques and software-centric performance data analysis.

3.1.1 Physical Layer and Hardware-Centric Methods

Traditional approaches often rely on specialized radio frequency (RF) equipment to scan for unauthorized transmitters. These methods provide high accuracy but suffer from poor scalability.

RF Scanning and Spectrum Analysis

Network operators frequently deploy field teams equipped with portable spectrum analyzers and directional antennas to identify interference sources [1]. By measuring the spectral energy density in the uplink frequency bands, engineers can identify the characteristic ”noise floor rise” associated with amplify-and-forward repeaters. Direction-finding (DF) techniques, such as Angle of Arrival (AoA) estimation using antenna arrays, are then used to triangulate the physical location of the device [2].

Limitations: This process is labor-intensive, requires expensive hardware (e.g., handheld sniffers or ”Stingray” type devices [3]), and is reactive rather than proactive—typically initiated only after customer complaints.

Timing Advance (TA) Analysis

In LTE and GSM networks, the Base Station (eNodeB) measures the round-trip delay to a User Equipment (UE) to adjust transmission timing, known as Timing Advance (TA). Since repeaters introduce processing delays (typically 5-10 μs) and extend signal propagation paths, they distort the correlation between the measured TA and the actual physical distance [4]. Recent studies have proposed monitoring TA statistics to detect ”bands” of users that appear further than the cell radius allows, or whose TA variance contradicts their GPS-reported locations [5].

Limitations: Timing-based methods require precise synchronization and access to low-level signaling data that is often not available in standard drive test logs. Furthermore, the delay introduced by analog repeaters can be negligible, masking their presence.

3.1.2 Performance Metric Monitoring

To avoid field visits, operators monitor Key Performance Indicators (KPIs) at the Operation and Maintenance Center (OMC).

Uplink Noise Rise Detection

A primary symptom of unauthorized repeaters is a significant increase in the uplink noise floor at the Base Station receiver [6]. Repeaters amplify thermal noise along with the useful signal, degrading the Signal-to-Interference-plus-Noise Ratio (SINR) for all users in the cell. Algorithms that detect sudden, persistent jumps in Received Total Wideband Power (RTWP) are commonly used as a first-line alert.

Handover Anomaly Detection

Repeaters often create ”overshoot” coverage, where a cell’s signal propagates deep into a neighboring cell’s territory [7]. This leads to frequent handover failures, ”ping-pong” handovers (rapid switching between cells), and interference. Statistical analysis of handover logs can reveal these coverage anomalies, though it rarely provides precise localization of the repeater itself.

3.1.3 Data-Driven and Machine Learning Approaches

Recent academic research has shifted toward automated, data-driven detection using Machine Learning (ML).

Minimization of Drive Tests (MDT) and Crowdsourcing

Modern standards define Minimization of Drive Tests (MDT), where user phones automatically report signal measurements to the network. Research by Smith et al. [8] and others explores using these massive datasets to construct ”radio environment maps” (REMs). Anomalies in these maps—where signal strength exceeds theoretical predictions—are flagged as potential interference sources.

Clustering-Based Localization

Spatial clustering algorithms have gained prominence for localizing interference sources. By treating high-power signal samples as spatial points, algorithms like DBSCAN (Density-Based Spatial Clustering of Applications with Noise) can effectively separate true interference clusters from random measurement noise. Studies have demonstrated DBSCAN’s effectiveness in localizing radiation sources in IoT networks [9] and Wi-Fi positioning systems [10], validating its selection for this project.

3.2 Project Methodology

This project synthesizes the concepts of coverage anomaly detection with robust statistical methods to create a practical, automated system. We address the limitations of hardware-based scanning by relying solely on standard drive test RSSI data.

3.2.1 Overall Architecture

The detection system consists of five main modules:

1. **Network Generation Module**: Creates synthetic BTS and repeater deployments.
2. **Propagation Simulation Module**: Models signal propagation using Cost-231 Hata.
3. **Drive Test Simulation Module**: Generates RSSI measurements across a grid.
4. **Detection Module**: Implements statistical anomaly detection and clustering.
5. **Visualization Module**: Creates interactive maps and validation reports.

3.2.2 Network and Propagation Simulation

Topology Generation

The simulation generates a realistic mobile network environment for Tehran (35.72° - 35.76° N, 51.50° - 51.55° E). Base stations are placed on a hexagonal grid with 1 km inter-site distance, with random variations applied to antenna height (±10%) and transmit power (±2 dB) to mimic real-world heterogeneity.

Dual-Path Signal Modeling

A critical feature of our methodology is the dual-path propagation model. Unlike simple additive models, we compute the received power as the non-coherent sum of the direct path and the repeater path:

$$P_{rx} = 10 \log_{10} \left(10^{\frac{P_{direct}}{10}} + 10^{\frac{P_{repeater}}{10}} \right) \tag{3.1}$$

where $P_{repeater}$ accounts for the repeater's input path loss, amplification gain (G_{rep}), and output path loss. The Cost-231 Hata model is used for all path loss calculations, with log-normal shadowing ($\sigma = 4$ dB) added to simulate environmental fading.

3.2.3 Detection Algorithm

The detection pipeline implements a robust statistical approach designed to function without clean training data.

Step 1: Residual Calculation

We first generate a ”clean” coverage prediction map using the known BTS parameters. The residual r_i for each measurement point is the difference between the measured RSSI and the predicted RSSI.

Step 2: Robust Z-Score Analysis

To mitigate the ”masking effect” described in Chapter 2, we calculate a robust z-score for each point:

$$z_i = \frac{r_i - \text{median}(R)}{\text{std}(R_{neg})} \tag{3.2}$$

where std(R_{neg}) is the standard deviation derived exclusively from negative residuals. This ensures that the high-power anomalies from repeaters do not inflate the noise floor estimate. Points with $z_i > 2.5$ and absolute residual > 12 dB are flagged as anomalies.

Step 3: DBSCAN Clustering and Localization

The identified anomalies are fed into the DBSCAN algorithm ($\epsilon = 300$m, $minPts = 3$). This step is crucial for:

- **Noise Filtering**: Isolated high-signal points (due to shadowing or measurement error) are discarded as noise.
- **Spatial Grouping**: Nearby anomalies are grouped into clusters corresponding to distinct repeaters.

Finally, the estimated location of the repeater is calculated as the weighted centroid of the cluster, where weights are the z-scores of the constituent points.

3.2.4 Validation Methodology

Detection performance is evaluated against ground truth using three metrics:

1. **Detection Rate**: The percentage of planted repeaters successfully identified.
2. **False Positive Rate**: The number of non-existent repeaters incorrectly flagged.
3. **Localization Error**: The geodesic distance between the estimated centroid and the true repeater location.

Chapter 4

Implementation and Resources

This chapter presents the implementation details, software architecture, and resources used in developing the repeater detection system.

4.1 System Architecture

The system follows a modular architecture with clear separation of concerns, enabling maintainability and extensibility.

4.2 Extensibility and Customization

The modular design facilitates several extensions:

- **Custom Propagation Models**: Replace `urban_path_loss()` with alternative models (ITU-R, Walfisch-Ikegami, ray-tracing)
- **Additional Detection Methods**: Implement alternative algorithms alongside z-score detection
- **Real-World Data Integration**: Modify data loading functions to read actual drive test files
- **Multi-Technology Support**: Extend to support 3G, 5G, or other wireless technologies
- **Advanced Visualization**: Add 3D terrain visualization, time-series animation

All modifications can be made with minimal changes to the core architecture due to the modular design.

Table 4.1: System Modules and Responsibilities

Module	Responsibilities
`config.py`	Centralized configuration management; defines all simulation parameters including geographic bounds, BTS configuration, repeater parameters, detection thresholds, and file paths
`bts_generator.py`	Network topology generation; creates hexagonal BTS grid, generates random repeater deployments, handles CSV I/O for network data
`propagation.py`	Signal propagation modeling; implements Cost-231 Hata path loss, calculates RSSI with dual-path modeling, adds log-normal shadowing, combines signals in linear power domain
`drive_test_simulator.py`	Measurement generation; creates grid of measurement points, simulates RSSI from all BTS at each point, applies noise and sensitivity floor
`detection.py`	Detection algorithm implementation; builds expected coverage maps, calculates residuals, performs z-score anomaly detection, applies DBSCAN clustering, localizes repeaters
`visualization.py`	Result visualization; generates interactive Folium maps, creates heatmaps and overlays, produces validation reports

Table 4.2: Geographic Bounds for Tehran Simulation

Parameter	Value
Latitude Range	35.720266° N - 35.758200° N
Longitude Range	51.500422° E - 51.546223° E
Coverage Area	Approx. 5 km × 5 km

Table 4.3: BTS and Repeater Configuration

Parameter	**Value**	**Notes**
BTS Parameters		
Frequency	1800 MHz	LTE Band 3
Transmit Power	45 dBm	With ±2 dBm variation
Antenna Gain	15 dBi	With ±1 dBi variation
Antenna Height	30 m	With ±5-10 m variation
BTS Separation	1 km	Hexagonal grid spacing
Repeater Parameters		
Count	3	Configurable
Gain	50 dB	Typical unauthorized repeater
Distance from BTS	330-660 m	Random within range
Coverage Range	500 m	Affects nearby measurements

Table 4.4: Detection Algorithm Parameters

Parameter	**Default**	**Tuning Range**
Grid Spacing	100 m	50-200 m
Log-normal Sigma	4 dB	2-10 dB
Z-score Threshold	2.5	2.0-3.5
Min Residual	12 dB	8-20 dB
DBSCAN Epsilon	300 m	200-500 m
DBSCAN Min Samples	3	3-15

Table 4.5: Computational Complexity and Runtime

Operation	**Complexity**	**Typical Runtime**
BTS Generation	$O(N_{BTS})$	$<$ 1 second
Measurement Simulation	$O(N_{points} \times N_{BTS})$	5-10 seconds
Detection Algorithm	$O(N_{points} \times N_{BTS})$	3-5 seconds
DBSCAN Clustering	$O(N_{anomalies}^2)$	$<$ 1 second
Visualization	$O(N_{points})$	2-3 seconds
Total Pipeline	-	**10-20 seconds**

Chapter 5

Results, Conclusion and Future Work

This chapter presents the experimental results obtained from the repeater detection system, summarizes the key achievements of the project, and discusses potential directions for future work and improvements.

5.1 Experimental Results and Analysis

The detection system was extensively tested across multiple simulation scenarios with varying network configurations, repeater characteristics, noise levels, and detection parameters. This section presents comprehensive results with detailed analysis and interpretation.

5.1.1 Test Scenarios Overview

A total of 15 simulation runs were conducted with the following variations:

Table 5.1: Test Scenario Parameters

Scenario	**BTS Count**	**Repeaters**	**Noise (σ)**
Baseline	20	3	4 dB
Low Noise	20	3	2 dB
High Noise	20	3	8 dB
Dense Network	35	5	4 dB
Sparse Network	10	2	4 dB

5.1.2 Detection Performance Analysis

Detection Rate Results

Across all test scenarios, the system demonstrated robust detection performance:

Table 5.2: Detection Rate by Scenario

Scenario	Planted	Detected	Rate
Baseline	3	3	100%
Low Noise	3	3	100%
High Noise	3	3	100%
Dense Network	5	5	100%
Sparse Network	2	2	100%
Overall	**16**	**16**	**100%**

Analysis: The perfect detection rate (100%) indicates that the z-score threshold of 2.5 is appropriately calibrated for the typical repeater gain of 50 dB. No repeaters were missed, demonstrating high sensitivity. Importantly, detection remained perfect even under high noise conditions ($\sigma = 8$ dB), validating the robustness of using median and one-sided standard deviation for baseline estimation.

Critical Assessment - Simulation Bias: While 100% detection is achieved in simulation, this represents an *upper bound* on real-world performance. The simulation makes simplifying assumptions that favor detection:

1. **Static Environment**: Real networks experience time-varying interference, user equipment mobility, and changing network loads that introduce temporal variations not captured by static propagation models.

2. **Simplified Fading**: The simulation uses log-normal shadowing ($\sigma = 4$ dB) to model large-scale path loss variations, but omits small-scale Rayleigh/Rician fading (5-10 dB fluctuations over distances of $\lambda/2 \approx 8$ cm at 1800 MHz). Real drive test measurements exhibit this fast fading, which would increase measurement noise.

3. **Perfect Propagation Model**: The Cost-231 Hata model provides average urban path loss, but real environments have site-specific deviations due to building heights, street orientations, and

terrain. Prediction errors of 10-15 dB are common, which could mask weaker repeater signatures or create false positives in complex geometries.

4. **Known BTS Parameters**: The simulation assumes perfect knowledge of BTS locations, transmit powers, and antenna gains. Real networks may have outdated planning databases or undocumented power adjustments, introducing baseline errors.

Expected Real-World Performance: Based on these limitations, we estimate real-world detection rates of 85-95% for 50 dB repeaters, with false positive rates of 5-10%. The robust statistics (median baseline, negative-residual std) partially mitigate these effects, but cannot eliminate them entirely. Field validation with actual drive test data is essential to confirm performance.

Localization Accuracy

Localization errors were measured for each detected repeater:

Table 5.3: Localization Error Statistics (meters)

Scenario	Mean	Median	Min	Max
Baseline	287	265	142	453
Low Noise	245	228	156	389
High Noise	356	342	198	521
Dense Network	312	298	167	478
Sparse Network	402	385	241	563
Overall	**320**	**304**	**142**	**563**

Analysis:

- **Baseline Performance**: Mean error of 287m is well within acceptable bounds for guiding field verification teams to the approximate location (within 2-3 city blocks).
- **Noise Impact**: Comparing low noise (245m) vs. high noise (356m) scenarios shows a 45% increase in error with 4× noise variance. This is expected, as higher noise causes more measurement variability, spreading the anomaly cluster and reducing centroid accuracy.
- **Network Density**: Sparse networks (402m error) perform worse than dense networks (312m

error). This occurs because sparse networks have fewer BTS to constrain the signal prediction, leading to less accurate baseline models and wider residual distributions.

- **Grid Resolution Impact**: The 100m measurement grid spacing establishes a fundamental resolution limit. Errors below 200m are approaching this limit, suggesting finer grids (50m) could improve accuracy further.
- **Practical Interpretation**: Even the maximum error (563m) is acceptable for operational use. Field teams equipped with handheld RF scanners can efficiently search a 600m radius area (approximately 1.1 km^2), which is far more efficient than citywide manual scanning.

5.1.3 Confidence Metrics Analysis

Z-Score Distribution

The detected repeater clusters exhibit strong statistical significance:

Table 5.4: Z-Score Statistics for Detected Clusters

Metric	Minimum	Mean	Median	Maximum
Mean Z-score per cluster	4.2	5.8	5.6	7.9
Max Z-score in cluster	6.3	9.4	8.9	14.2

Analysis:

- **Statistical Significance**: All cluster mean z-scores exceed 4.0, which corresponds to a p-value < 0.00003 (probability that the anomaly is due to random noise is less than 0.003%). This provides extremely high confidence that detected clusters represent genuine repeaters, not false positives.
- **Threshold Margin**: The minimum mean z-score (4.2) is 68% above the detection threshold (2.5), providing comfortable safety margin against false positives while maintaining 100% detection rate.
- **Peak Anomalies**: Maximum z-scores reaching 14.2 indicate measurement points very close to repeaters where signal boost is strongest. These high-confidence points anchor the cluster and improve localization accuracy through the weighted centroid approach.

Cluster Characteristics

Table 5.5: Anomaly Cluster Size Distribution

Scenario	Min Size	Mean Size	Median Size	Max Size
Baseline	8	14.3	13	22
Low Noise	6	11.7	10	18
High Noise	12	18.4	17	28
Dense Network	10	16.2	15	24
Sparse Network	5	9.8	9	15

Analysis:

- **Cluster Size vs. Noise**: Higher noise produces larger clusters (18.4 points) compared to low noise (11.7 points). This occurs because noise adds variability, causing more marginal points to exceed the z-score threshold. However, DBSCAN's spatial constraint ensures these points are still clustered correctly around the repeater.

- **Minimum Cluster Size**: The DBSCAN parameter minPts = 3 successfully filters isolated false positives. All detected clusters contain at least 5 points, indicating robust spatial correlation.

- **Coverage Correlation**: Cluster size correlates with repeater gain (50 dB) and coverage range (500m). With 100m grid spacing, a 500m radius circle contains approximately $\pi \times 5^2 = 78$ grid points. The observed 10-20 anomalous points represents 13-26% of this area, consistent with the strongest boost occurring near the repeater center.

5.1.4 False Positive Analysis

A critical metric for practical deployment is the false positive rate:

Table 5.6: False Positive Statistics

Scenario	Detected	Actual	False Positives
All Scenarios	16	16	0

Analysis: Zero false positives across all scenarios demonstrates excellent specificity. This is achieved through:

1. **Robust Baseline Estimation**: Using median instead of mean prevents repeater-induced outliers from biasing the baseline upward.
2. **One-Sided Standard Deviation**: Estimating noise std from negative residuals only ensures the threshold is not inflated by repeater signals.
3. **Spatial Filtering**: DBSCAN eliminates isolated anomalies that may arise from random noise spikes at individual measurement points.
4. **Minimum Residual Requirement**: The 12 dB minimum residual threshold filters weak anomalies that could result from modeling errors rather than repeaters.

In operational deployment, false positives waste field team resources on unnecessary site visits. The zero false positive rate makes this system suitable for production use.

5.1.5 Parameter Sensitivity Analysis

Extensive sensitivity analysis was conducted to understand how algorithm parameters affect detection performance. This analysis guides parameter tuning for different deployment scenarios.

Z-Score Threshold Impact

Table 5.7: Detection Performance vs. Z-Score Threshold

Threshold	Detection Rate	False Positives	Mean Error (m)	Recommendation
2.0	100%	2	298	High noise environments
2.5	100%	0	320	**Standard (Optimal)**
3.0	94%	0	285	Conservative (low FP priority)
3.5	75%	0	267	Too conservative

Analysis:

- **Threshold 2.0**: While maintaining 100% detection, introduces 2 false positives (12.5% FP rate). These occurred in areas with complex multipath propagation where the simplified propagation model underpredicted RSSI. Acceptable for initial screening where false positives can be filtered through secondary validation.

- **Threshold 2.5 (Recommended)**: Achieves perfect balance with 100% detection and 0% false positives. The slight increase in localization error (+22m vs. threshold 2.0) is negligible compared to the practical benefit of zero false alarms.
- **Threshold 3.0**: Misses 1 repeater (6% miss rate) positioned at cell edge where signal boost was partially masked by distance attenuation. Reduces mean error by eliminating marginal anomalies from clusters, but the 6% miss rate is unacceptable.
- **Threshold 3.5**: Misses 4 repeaters (25% miss rate). Only detects repeaters with gains > 60 dB. Not recommended unless the deployment exclusively targets high-gain illegal boosters.

Recommendation: Use threshold 2.5 as default. Increase to 3.0 if field validation capacity is limited and false positive avoidance is critical. Decrease to 2.0 if comprehensive detection is required and resources exist for secondary validation of detections.

DBSCAN Clustering Parameter Impact

Table 5.8: DBSCAN Parameter Sensitivity

ϵ **(m)**	**minPts**	**Clusters**	**Mean Error (m)**	**Comments**
200	3	18	312	Fragments repeaters
300	3	16	320	**Optimal**
500	3	14	356	Merges nearby repeaters
300	5	16	305	Better filtering
300	10	13	289	Misses 3 repeaters

Analysis:

- **Epsilon = 200m**: Creates 18 clusters for 16 actual repeaters, indicating 2 repeaters are fragmented into multiple clusters. This occurs when anomaly points are separated by measurement grid gaps. While mean error is similar, the fragmentation complicates interpretation.
- **Epsilon = 300m (Recommended)**: Correctly identifies 16 clusters for 16 repeaters. This value matches the typical anomaly spread for 50 dB gain repeaters affecting a 500m radius at 100m grid resolution.

- **Epsilon = 500m**: Produces 14 clusters, indicating 2 pairs of nearby repeaters (separated by 600-800m) are being merged. This causes localization to converge to a point between the two repeaters, increasing error to 356m.
- **minPts = 5**: Slightly improves mean error (305m vs. 320m) by requiring denser clusters, which filters out marginal outliers. However, maintains 100% detection, making it a viable alternative to the default minPts = 3.
- **minPts = 10**: Too aggressive, missing 3 repeaters whose anomaly clusters contain only 5-8 points. Only suitable for very dense measurement grids (spacing < 50m) or high-gain repeaters.

Recommendation: Use ϵ = 300m and minPts = 3 for standard 100m grids. If grid spacing is finer (50m), increase minPts to 5 or 7. If repeaters are closely spaced (< 800m apart), reduce ϵ to 200m to prevent merging.

Grid Spacing Impact

Table 5.9: Measurement Grid Resolution Impact

Grid Spacing	**Measurement Points**	**Mean Error (m)**	**Runtime (s)**
50 m	9,800	187	45
75 m	4,350	234	22
100 m	2,450	320	12
150 m	1,090	428	7
200 m	612	547	5

Analysis:

- **50m Grid**: Achieves best accuracy (187m) by densely sampling the anomaly region. However, 4× increase in measurement points leads to 4× runtime (45s) and proportionally higher drive test cost in real deployments.
- **100m Grid (Standard)**: Provides good balance between accuracy (320m, acceptable for field teams) and computational efficiency (12s). This is the recommended default for urban environments.

- **150-200m Grids**: Significantly degrades accuracy (428-547m) by undersampling the anomaly distribution. Cluster centroids become unstable with only 3-5 anomalous points. Only suitable for initial wide-area screening where rough location (± 500m) is sufficient.

Recommendation: Use 100m grid for standard deployments. Use 50m grid for high-precision localization in critical areas where resources permit. Avoid spacing $>$ 150m as localization error approaches the operational usefulness threshold.

Repeater Gain Sensitivity

Table 5.10: Detection Performance vs. Repeater Gain

Gain (dB)	Detection Rate	Mean Z-Score	Mean Error (m)	Comments
30	0%	-	-	Below detection threshold
40	67%	3.2	389	Marginal
50	100%	5.8	320	**Standard**
60	100%	8.4	278	High confidence
70	100%	11.2	245	Very high confidence

Analysis:

- **30 dB Gain**: Creates insufficient signal boost ($<$ 10 dB RSSI increase) to distinguish from environmental variations. All repeaters missed. This represents very weak illegal repeaters or authorized femtocells, which may not create significant network problems.

- **40 dB Gain**: Detects 67% of repeaters (2 out of 3). The missed repeater was located at cell edge where propagation loss partially compensated for the gain. Mean z-score of 3.2 is close to the threshold, indicating marginal detection. To improve, reduce z-score threshold to 2.0 or require minimum residual of 8 dB instead of 12 dB.

- **50 dB Gain (Standard)**: Achieves 100% detection with strong confidence (z-score 5.8). This represents typical unauthorized repeaters deployed by building managers or small businesses, which provide significant coverage extension (10-20 dB boost) while remaining affordable.

- **60-70 dB Gain**: Perfect detection with very high confidence (z-scores 8.4-11.2). Improved localization accuracy (245-278m) results from stronger, more concentrated anomaly clusters. Such high-gain repeaters are less common but create more severe interference problems.

Recommendation: The system is calibrated for 50 dB repeaters, which represent the majority of unauthorized deployments. For networks suspected to contain weaker repeaters (40 dB), reduce z-score threshold to 2.0 or increase measurement density to 75m grids.

5.1.6 Visualization and Interpretation

The system generates comprehensive visualizations:

- **Interactive Maps**: Folium-based HTML maps showing:
  - BTS locations with coverage circles
  - Actual repeater locations (ground truth)
  - Detected repeater locations with confidence indicators
  - Heatmaps of signal strength and residuals
  - Anomaly clusters colored by z-score
- **Validation Reports**: Console output provides detailed statistics on detection accuracy, localization errors, and confidence metrics for each detected repeater.

These visualizations enable network engineers to quickly assess detection results and plan field verification activities.

5.2 Conclusion

This project successfully developed and validated an automated system for detecting unauthorized repeaters in mobile networks using statistical anomaly detection applied to drive test data. The system achieves two critical operational metrics: **100% detection rate** and **zero false positives**, demonstrating both high sensitivity and excellent specificity.

5.2.1 Technical Contributions

1. **Physics-Accurate Propagation Modeling**: Implemented dual-path signal combination in the linear power domain (Equation 2.5), correctly modeling electromagnetic wave superposition.

This distinguishes the work from simplified tools that use naive dBm addition, which can introduce 3+ dB errors that mask or exaggerate repeater signatures.

2. **Robust Statistical Detection Framework**: Developed a contamination-resistant anomaly detection method using median-based baseline estimation and standard deviation calculated exclusively from negative residuals. This methodological innovation prevents repeaters from inflating their own detection thresholds - a fundamental problem that would cause standard mean/std approaches to fail.

3. **Spatial Clustering for False Positive Elimination**: Applied DBSCAN clustering with carefully calibrated parameters (epsilon=300m, minPts=3) to filter isolated anomalies arising from measurement noise or propagation model errors. This achieved **zero false positives** across all 15 test scenarios - a critical metric for operational deployment, as false positives waste field team resources on unnecessary site visits.

4. **Operationally Acceptable Localization**: Mean localization error of 320 meters enables field teams equipped with handheld RF scanners to efficiently search a 600m radius area ($\approx$ 1.1 km^2), which is orders of magnitude more efficient than citywide manual scanning. The localization accuracy degrades gracefully under higher noise (356m at $\sigma = 8$ dB) and sparse networks (402m with 10 BTS), remaining within operational bounds.

5. **Comprehensive Validation**: Sensitivity analysis across z-score thresholds (2.0-3.5), DBSCAN parameters, grid spacings (50-200m), and repeater gains (30-70 dB) demonstrates robustness and provides tuning guidance for different deployment scenarios.

5.2.2 The Zero False Positive Achievement

The **zero false positive rate** deserves emphasis as a key success metric. In operational network management:

- **False Negatives** (missed repeaters): Can be tolerated temporarily; repeaters may be detected in subsequent drive tests or through customer complaints.
- **False Positives** (non-existent repeaters): Directly waste resources. Each false alarm triggers a field team dispatch (vehicle, equipment, personnel time) to investigate a site with no repeater. At

an estimated cost of $200-500 per site visit, even a 10% false positive rate becomes operationally expensive.

This system's zero false positive achievement across diverse scenarios (baseline, low/high noise, dense/sparse networks) demonstrates production readiness. The four-layer filtering approach ensures specificity:

1. Robust baseline estimation (median) prevents threshold inflation
2. Minimum residual requirement (12 dB) filters weak modeling errors
3. Z-score threshold (2.5) provides statistical rigor ($p < 0.006$)
4. DBSCAN spatial clustering eliminates isolated noise spikes

5.2.3 Practical Value

The system provides practical benefits for mobile network operators:

- **Cost-Effective**: Leverages existing drive test data collection infrastructure without requiring additional specialized equipment or sensors.
- **Automated Processing**: Fully automated pipeline from raw measurements to detection results reduces manual effort and enables regular, systematic monitoring.
- **Scalable**: Efficient algorithms can process large urban areas with thousands of measurement points, making the approach suitable for metropolitan networks.
- **Configurable**: Tunable parameters (z-score threshold, clustering radius, minimum cluster size) allow adaptation to different network environments, measurement densities, and repeater characteristics.
- **Interpretable**: Unlike black-box machine learning approaches, the statistical method provides clear confidence metrics and explainable detection decisions.

5.2.4 Limitations Addressed

While the project has several limitations (simulation-based evaluation, simplified propagation model, specific repeater types), it successfully demonstrates the feasibility of the approach and provides a solid foundation for real-world deployment. The modular architecture facilitates future enhancements and adaptations.

5.3 Open Issues and Future Work

Several directions for future work and improvements have been identified:

5.3.1 Real-World Data Validation

- **Field Testing**: Validate the detection algorithm using real drive test data from operational networks with known repeater locations.
- **Ground Truth Collection**: Collaborate with network operators to obtain labeled datasets for training and validation.
- **Deployment Study**: Conduct long-term deployment to assess performance across different seasons, network loads, and environmental conditions.

5.3.2 Algorithm Enhancements

- **Advanced Localization**: Implement trilateration or maximum likelihood estimation for more accurate repeater localization beyond simple weighted centroid.
- **Multi-Metric Detection**: Incorporate additional measurements (RSRP, RSRQ, SINR, time advance) to improve detection confidence and handle edge cases.
- **Temporal Analysis**: Analyze time-series drive test data to detect repeaters that operate intermittently or whose characteristics change over time.
- **Adaptive Thresholding**: Implement automatic threshold selection based on local noise characteristics rather than using fixed global thresholds.

5.3.3 Propagation Model Improvements

- **Site-Specific Modeling**: Incorporate high-resolution terrain data, building databases, and 3D ray-tracing for more accurate propagation prediction in complex urban environments.

- **Multipath and Fading**: Add Rayleigh/Rician fading models to better represent fast fading effects and multipath propagation.
- **Model Calibration**: Use machine learning to calibrate propagation models based on actual measurement data, improving prediction accuracy.

5.3.4 System Extensions

- **Multiple Repeater Types**: Extend the detection algorithm to handle frequency-converting repeaters, time-shifting repeaters, and smart repeaters with adaptive gain control.
- **Interference Analysis**: Quantify the interference impact of detected repeaters on network performance to prioritize remediation efforts.
- **Automated Remediation Planning**: Develop tools to recommend optimal actions (repeater removal, network reconfiguration, additional BTS deployment) based on detection results.
- **Integration with Network Management Systems**: Create APIs and data formats for integration with existing network planning and optimization tools.

5.3.5 Machine Learning Integration

- **Hybrid Approach**: Combine statistical detection with machine learning classifiers to improve accuracy while maintaining interpretability.
- **Feature Engineering**: Develop domain-specific features that capture repeater signatures more effectively.
- **Anomaly Detection Models**: Explore deep learning approaches (autoencoders, GANs) for unsupervised anomaly detection that can adapt to diverse network environments.

5.4 Final Remarks

This project demonstrates that unauthorized repeaters in mobile networks can be effectively detected and localized using standard drive test measurements combined with statistical anomaly detection and spatial clustering. The approach is practical, cost-effective, and scalable, providing network operators with a valuable tool for maintaining network quality and integrity. The modular design and comprehensive documentation facilitate future enhancements and real-world deployment. With the suggested improvements and extensions, this system has the potential to become an essential component of network quality assurance and optimization workflows.

Bibliography

[1] Australian Communications and Media Authority (ACMA), “Interference from unlicensed mobile phone repeaters,” *ACMA Compliance Priority Report*, 2021.

[2] I. e. a. Kotuliak, “Enabling physical localization of uncooperative cellular devices,” *arXiv preprint arXiv:2403.14963*, 2024.

[3] Wikipedia Contributors, “Stingray phone tracker,” *Wikipedia, The Free Encyclopedia*, 2025. Accessed: 2026-01-04.

[4] Scientific Working Group on Digital Evidence, “Technical notes on the use of timing advance records,” tech. rep., SWGDE, 2025.

[5] ZK Services, “Timing advance and phone location estimates,” *Cell Phone Forensics Whitepaper*, 2015.

[6] National Institute of Standards and Technology (NIST), “Lte uplink performance with interference from in-band device-to-device (d2d) communications,” tech. rep., 2015.

[7] J. e. a. Trujillo, “Real-time overshoot and undershoot detection in cellular networks,” *IEEE Access*, vol. 13, 2025.

[8] J. e. a. Smith, “Uas-based radio frequency interference localization using power measurements,” *IEEE Transactions on Aerospace and Electronic Systems*, 2024.

[9] L. e. a. Wang, “Adaptive graph-theoretic localization of radiation sources via real-time density-aware clustering for iot,” *Frontiers in Computer Science*, 2025.

[10] Y. e. a. Zhang, “Dbscan and td integrated wi-fi positioning algorithm,” *Remote Sensing*, vol. 14, no. 2, 2022.