Ashika Ruwanthi

Development of Machine Learning Based Models for Detecting GNSS Signal Jamming in Real-World Scenarios Using AGC Data

School of Technology and Innovations
Master's Thesis
Sustainable and Autonomous Systems

Vaasa 2025

UNIVERSITY OF VAASA
School of Technology and Innovations
Author: Ashika Ruwanthi
Title of the thesis: Development of Machine Learning Based Models for Detecting GNSS Signal Jamming in Real-World Scenarios Using AGC Data
Degree: Master of Computer Science
Discipline: Sustainable and Autonomous Systems
Supervisor: Heidi Kuusniemi
Evaluator Petri Välisuo
Year: 2025 **Pages:** 71

ABSTRACT:

Although Global Navigation Satellite Systems (GNSS) provide high-precision positioning under optimal situations, they remain vulnerable to intentional Radio Frequency Interference (RFI) due to the low signal power received at ground level and the increasing availability of jamming devices. Previous studies have demonstrated that traditional jamming detection methods, such as fixed-threshold-based detection, are limited in handling dynamic scenarios and therefore remain less efficient under real-world conditions. This study addresses these limitations by applying machine learning (ML) techniques to detect GNSS jamming using AGC data.

The primary objective of the study is to analyse supervised and unsupervised machine learning (ML) models for detecting jamming using multidimensional features derived from AGC signals. The theoretical foundation is based on anomaly detection, statistical learning, and time-series signal analysis. Two machine learning models were applied: a supervised classifier (XGBoost) and an unsupervised anomaly detector (Isolation Forest). Both were trained and validated on AGC data measured during a controlled jamming test in Norway. The experiment is conducted under various jamming conditions, which enable realistic and reproducible data collection in a dynamic vehicular environment.

Feature extraction was performed using the sliding-window approach across various GNSS frequency bands, retaining the temporal and spectral dynamics of AGC. The supervised model was trained on labelled samples to distinguish normal and jammed windows, while the unsupervised model was trained on normal data only to identify anomalies. The test consisted of typical classification metrics and interpretability methods, such as feature importance analysis, to understand the model's decisions.

Both models demonstrated the ability to detect jamming effectively. The supervised model showed strong performance, revealing that AGC features from specific frequency bands, particularly the G1 band, were most indicative of jamming. The unsupervised model performed reliably on normal data, although it generated some false predictions, which may be attributed to sudden variations in positioning data. Visual analysis offers a deeper understanding of the relationship between prediction results and the behavior of positioning parameters.

The proposed ML-based approaches provide better adaptability, eliminate the need for manual threshold tuning, and scale effectively across various conditions. They are well-suited for real-time deployment in GNSS receivers. Future work may enhance these models by combining them to provide a total localization solution.

KEYWORDS: (GNSS, Jamming, Detection, Isolation Forest, XGBoost, AGC, Machine Learning)

Contents

Figures

Tables

Abbreviations

AGC – Automatic Gain Control

AI - Artificial Intelligence

AV – Autonomous Vehicles

CNN – Convolutional Neural Network

CW - Continuous Wave

DGNSS - Differential GNSS

DME - Distance Measuring Equipment

EMA – Exponential Moving Average

FM - Frequency Modulation

GAN – Generative Adversarial Network

GIS - Geospatial Information Systems

GNSS – Global Navigation Satellite Systems

GPS Global Positioning System

IMU – Inertial Measurement Unit

IF – Isolation Forest

kNN - K Nearest Neighbours

KS - Kolmogorov–Smirnov

LSTM – Long Short-term Memory

ML – Machine Learning

PNT - Positioning, Navigation, and Timing

PPD - Personal Privacy Devices

PPP - Precise Point Positioning

RAIM - Receiver Autonomous Integrity Monitoring

RFI - Radio Frequency Interference

RNN – Recurrent Neural Network

RTK – Real-Time Kinematic

SBAS - Satellite-Based Augmentation System

SLAM - Simultaneous Localization and Mapping

SNR - Signal to Noise Ratio

SVM – Support Vector Machine

TACAN - Tactical Air Navigation

UAV – Unmanned Aerial Vehicles

1 Introduction

The introduction chapter highlights the growing vulnerabilities of GNSS systems to jamming, especially in positioning and navigation. It presents the motivation for using real-world data in machine learning based jamming detection using AGC data. The chapter also includes research problems, objectives, scope of study, and the structure of the thesis.

1.1 Background and Motivation

Over the last few years, applications of Global Navigation Satellite Systems (GNSS) have grown exponentially due to their capability of providing accurate and precise positioning and timing information. The global availability of GNSS signals has enabled them to play a significant role in numerous industries, including transportation, agriculture, logistics, and infrastructure management. As reliance on GNSS continues to increase, particularly in high-precision applications such as connected and autonomous vehicles, the requirement for real-time and reliable positioning data has become increasingly critical. Despite having numerous advantages, GNSS signals are vulnerable to attacks due to the low transmission power levels. This inherent vulnerability raises deep concerns about the resilience and integrity of GNSS-based services, particularly in safety-critical and real-time operational environments.

GNSS signals need to propagate nearly 20,000 km to reach the ground as the satellites orbit in Medium Earth Orbit (MEO). Normally, the signal strength will decrease over the distance. The average signal power decreases to approximately -130 dBm (L1 band) when it reaches the GNSS receivers (Spanghero et al., 2025). Therefore, the GNSS signals are easily interfered with by radio frequency interference (RFI), which can be either intentional or nonintentional. Electronics devices are an example of a non-intentional interference source. Even low-power jammers can easily overwhelm the actual satellite signals, resulting in poorer positioning performance or complete service denial.

Jamming in GNSS systems refers to the intentional broadcasting of radio frequency signals meant to disrupt GNSS receiver operation. The signals are typically broadcast at high power and on frequencies near GNSS frequencies, such as L1, L2, and L5, with the purpose of malfunctioning the receivers to disrupt their ability to acquire or track satellite signals (Radoš et al., 2024). As a result, the receiver may lose satellite information or be unable to calculate valid positioning data. Small, inexpensive jamming devices can also disrupt GNSS services across extensive ranges, and jamming is a viable and significant threat that is easily accessible. Although jamming devices are less complex than more advanced threats like spoofing, their extensive use can cause severe problems, especially in situations where uninterrupted GNSS access is critical.

GNSS jamming poses a significant threat to a wide range of systems that rely on precise positioning, navigation, and timing services. Jamming results in loss of lock, lowered accuracy, or GNSS-based failure. GNSS jamming is a considerable topic not only in navigation but also in other critical applications such as telecommunications, power grid synchronization, aviation, and maritime operations. Cascading failure or operational delay can be experienced even for minor interruptions in time-sensitive systems. Nowadays, the impact of jamming presents a serious risk to both safety and service continuity as the reliance on GNSS applications.

Traditional jamming detection methods in GNSS rely mainly on signal features and statistical pattern observation in the receiver. These types of methods are mostly categorized into pre-correlation and post-correlation methods. Pre-correlation methods, such as monitoring Automatic Gain Control (AGC) levels, statistical signal analysis, and transformed domain techniques, are applied at the receiver front-end to detect anomalies before signal correlation occurs. Postcorrelation techniques, including the analysis of carrier-to-noise density ratio (C/N_o) and correlation function behavior, detect interference based on disruptions observed during or after signal acquisition and tracking (Reda et al., 2024). Many of these methods depend on predefined thresholds or reference models, where deviations in signal power or quality trigger interference alerts. While such techniques may work well under controlled or weak interference

environments, they will fail in strong or complex jamming environments, where signal tracking itself may fail (C. Liu et al., 2025). Moreover, prior knowledge of interference behavior is required in traditional techniques. Therefore, they are not as appropriate for dynamic and uncertain environments.

Traditional detection methods struggle to detect jamming due to the growing complexity and sophistication of GNSS jamming techniques. This highlights a need for robust and novel detection approaches, such as data-driven machine learning (ML) methods. ML algorithms can be trained on vast amounts of historical GNSS data. This process enables the automated extraction of features and the identification of hidden patterns that are difficult to detect using traditional threshold-based methods. Compared to static models, ML algorithms can learn and adapt to diverse and dynamically changing interference scenarios, thereby improving detection accuracy over time. Recent research has demonstrated that ML methods are highly effective in detecting and classifying jamming signals by leveraging advanced data representations and signal transformations. Their flexibility, scalability, and ability to process complex signal characteristics make ML-based techniques an essential component of the design of strong and reliable GNSS interference detection systems (Reda et al., 2024).

GNSS functionality has been embedded with smartphones, enabling them to capture raw measurement data such as pseudorange, Doppler shift, C/N_o, and AGC. Among these, AGC is particularly valuable for detecting signal strength variations that may indicate the presence of interference. However, despite its relevance, AGC has mostly been utilized with C/N_o, rather than as an independent feature in machine learning-based jamming detection. This study focuses specifically on AGC to explore its potential as an independent indicator of GNSS signal integrity. The high availability of smartphones offers a cost-effective and scalable platform for interference detection. Thereby, a broader geographic coverage and practical deployment in real-world environments can be facilitated. By incorporating AGC data into machine learning frameworks, this approach aims to develop adaptive and robust jamming detection models that do not rely on specialized or high-end GNSS equipment.

Real-world data play a crucial role in developing effective GNSS jamming detection methods. Unlike simulated data, real-world data captures the complexity, diversity, and randomness of real-world jamming scenarios, which include environmental noise, signal variations, and various interference patterns. Training and testing detection models on such data ensures better generalization and robustness, enabling the models to perform well in real-world settings. This is particularly the case for machine learning approaches, which rely on representative data in order to learn meaningful patterns and make sound predictions.

1.1.1 Jammertest

The Jammertest is an event conducted by the Norwegian government that aims to promote the robust and intelligent use of Global Navigation Satellite Systems (GNSS). The event provides a controlled testbed where experts from industry, academia, and public authorities can collaboratively examine GNSS vulnerabilities under realistic conditions (Test Catalogue, 2024). It is held annually at Andøya. Unlike traditional military jamming exercises, Jammertest is a civilian-accessible environment that focuses on testing the effects of jamming, spoofing, and meaconing in a safe and regulated setting.

Jammertest features a structured and flexible test catalogue that enables detailed and repeatable GNSS interference testing. It supports diverse threat scenarios and promotes transparency by publishing machine-readable test data on GitHub, fostering collaboration and enhancing global GNSS protection efforts. Further information about Jammertest can be found on (*Previous Jammertests*, n.d.)

1.1.2 Motivation

The primary motivation for this study is to explore the effectiveness of machine learning (ML) models in detecting GNSS jamming using AGC data collected from smartphones. Although machine learning-based solutions have been promising in interference

detection, current research has mostly employed AGC alongside other features such as C/N_0 rather than its sole efficacy being assessed. Furthermore, there is a visible lack of integration in the comparative study of supervised and unsupervised machine learning models in GNSS jamming detection that restricts our knowledge about their relative strengths and limitations.

Figure 1: Jammertest Locations at Andøya; Red: Bleik; Green: Grunnvatn; Blue: Stave (Test Catalogue, 2024)

This study addresses these gaps by focusing on AGC as an independent input for ML models and evaluating both supervised and unsupervised learning techniques. Additionally, the research is grounded in real-world data, ensuring practical relevance and applicability. This approach supports the development of cost-effective and adaptable solutions which are suitable for deployment in dynamic environments. As the reliance on GNSS across numerous sectors, including transportation, emergency services, and autonomous technology, continues to grow, it is both opportune and essential to develop the resilience of positioning systems to deliberate interference. The objective of

this study is to further the creation of sophisticated GNSS protection methods through the application of a definite and comparative machine learning procedure.

1.2 Research Problems

While there is an increasing dependence on GNSS for timing and navigation, the systems remain highly vulnerable to intentional interference in the form of jamming, especially due to the low power of satellite signals at the ground level. Traditional jamming detection methods often depend on static thresholds or fixed models, which limit their applicability under dynamic, real-world scenarios.

This research addresses the following core problems

- To what extent can AGC data, collected from consumer-grade GNSS-enabled devices, be used as a standalone feature for detecting jamming signals?
- How can supervised machine learning models be trained on AGC data to reliably detect various types of GNSS jamming?
- What is the potential of unsupervised machine learning techniques to identify jamming patterns in AGC data without labelled ground truth?
- How do supervised and unsupervised models compare in terms of detection accuracy, generalizability, and applicability in real-world GNSS jamming scenarios?

1.3 Research Objectives

This research aims to develop an effective and scalable approach for detecting GNSS jamming using AGC data alone. The specific objectives are as follows:

- To examine the viability of AGC as a standalone feature for detecting GNSS jamming, using data collected from consumer-grade GNSS-enabled devices.
- To design and implement supervised machine learning models trained exclusively on AGC data for the reliable identification of jamming events.
- To develop unsupervised machine learning models capable of detecting

jamming anomalies in AGC data without the need for labelled training data.

- To perform a comparative analysis of supervised and unsupervised models in terms of detection accuracy, robustness, and adaptability to real-world GNSS interference scenarios.

1.4 Scope of Work

This research is limited to the development and evaluation of machine learning-based methods for detecting GNSS jamming using AGC data obtained from smartphones. The study focuses exclusively on detecting stationary jamming scenarios. However, it does not address spoofing, mobile jamming, or signal mitigation techniques. The methodology will involve AGC data preprocessing, the development of both supervised and unsupervised machine learning models, and a systematic comparison of their performance in terms of accuracy and adaptability. Real-world datasets, specifically from the Jammertest event, will be used to ensure the practical relevance of the models under realistic signal conditions. The overall goal is to assess the feasibility and effectiveness of using AGC data alone for reliable jamming detection, providing a lightweight and scalable approach that does not rely on specialized GNSS hardware.

1.5 Thesis Structure

- Chapter 1 – Introduction

  Introduces the research by outlining the background and motivation. Further, it explains the problem statement, research questions, objectives, and scope. Finally, the overall structure of the thesis is given.

- Chapter 2 – Literature Review

  Examines existing studies on GNSS jamming detection, with a focus on traditional techniques and the integration of machine learning approaches. It also highlights the limited use of AGC data and identifies gaps that this study aims to address.

- Chapter 3 – Methodology

  Describes the research design, including the use of AGC data, data collection from real-world sources, preprocessing methods, and the development of supervised and unsupervised machine learning models. The chapter also outlines the criteria for evaluating model performance.

- Chapter 4 – Experimental Design and Analysis

  Details the experimental setup, including the definition of stationary jamming scenarios, model training and validation processes, and the strategy for comparing the performance of different machine learning models.

- Chapter 5 – Results and Discussion

  Presents the experimental results, evaluates the effectiveness of the supervised and unsupervised models, and discusses their practical implications and limitations based on real-world jamming conditions.

- Chapter 6 – Conclusion and Future Work

  Summarizes the key findings, reflects on the research contributions and limitations, and proposes directions for future studies, including potential expansion to mobile jamming and multi-feature detection frameworks.

Consent and Details Regarding AI-Generated Content

I confirm that parts of this master thesis were prepared with the assistance of a Large Language Model (LLM) developed by OpenAI, specifically GPT-4o-mini, a variant of the GPT-4 architecture. The AI was used as a supportive tool for drafting, phrasing, and generating ideas. All final content was critically reviewed and edited by me to ensure academic integrity and originality. I acknowledge responsibility for the entire thesis content and certify that the use of the AI tool complies with the ethical guidelines and policies of my institution.

2 Literature Review

This chapter provides an overview of the state-of-the-art research on GNSS signal degradation due to jamming, focusing on detection techniques. It briefly discusses common sources of error in GNSS, traditional jamming detection techniques, and new machine learning techniques. The smartphone-based GNSS data usage for jamming detection is also discussed. The chapter ends by highlighting significant areas of research deficiency, namely the lack of use of AGC data alone and the lack of comparative analysis of supervised and unsupervised machine learning algorithms in real-world scenarios.

2.1 Overview of GNSS

GNSS is modern satellite navigation systems that provide Positioning, Navigation, and Timing (PNT) services worldwide. These include leading global systems like the United States' Global Positioning System (GPS), Russia's GLONASS, Europe's Galileo, and China's BeiDou. In addition to these, there are regional systems such as Japan's QZSS and India's NavIC. These systems are a critical component of a wide range of applications, including automotive navigation, aerospace, maritime transport, agriculture, geospatial information systems (GIS), emergency response, and others, so in autonomous vehicles (G. Li & Geng, 2019).

GNSS positioning relies on the calculation of the time it takes for signals from multiple satellites to reach a receiver using distance measurements from at least four satellites. As shown in **Figure 2,** the receiver is able to compute its three-dimensional position and corrected time using the trilateration principle (Samalla & Naveen Kumar, 2024).

Over the last few years, GNSS technology has developed significantly in several directions. Specht et al., (2020) emphasized that the utilization of multi-constellation and multi-frequency function in GNSS navigation. Meanwhile, the GNSS receivers have revolutionized in technology that enables miniaturization in size and reducing cost. These advancements have helped them to easily integrate with everyday devices such as smartphones, vehicles, and IoT systems. The availability of receivers has increases

with this integration. Additionally, modern positioning techniques like Precise Point Positioning (PPP) and Real-Time Kinematic (RTK) have emerged, offering high-precision location estimates. Thereby, they are able to ensure centimeter or decimeter level accuracy, even when using affordable or mobile hardware (Odolinski et al., 2020).

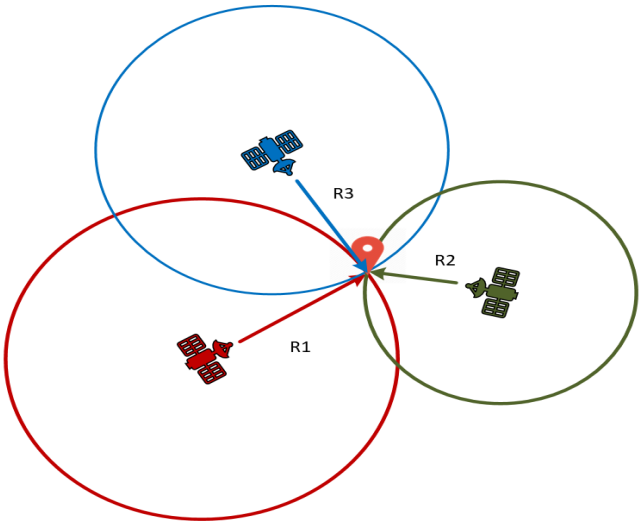

Figure 2: Trilateration of GNSS Positioning

Atmospheric delays, satellite geometry, multipath propagation, and signal interference are the source of errors that can affect for the GNSS receiver performance. Such effects are particularly prominent in urban canyons as well as GNSS-denied environments, whose signal accuracy and reliability are greatly undermined.

Modern transportation infrastructure, e.g., autonomous cars (AVs) and smart traffic systems (ITS), increasingly use GNSS for positioning, routing, and central control of traffic. As argued by Ghanbarzadeh et al., (2025), GNSS plays a significant role in maximizing efficiency of operations and security. However, as Siemuri et al., (2022) put strong emphasis on, susceptibility to interference, particularly purposeful jamming, poses enormous risks to such applications and necessitates strong detection and countermeasures.

2.2 GNSS Errors and Vulnerabilities for Navigation

In vehicular navigation, GNSS is prone to several errors and interferences that may reduce the performance of the positioning information obtained. GNSS has become beneficial and essential for most modern transportation modes, but this navigation may be influenced by a number of factors that cause the receivers to deviate from the actual positions, hence affecting not only navigation but also safety, efficiency, and functionality of transport systems (Aggrey et al., 2020). These disruptions may stem from sources such as ionospheric and tropospheric delays, satellite clock errors, multipath propagation, and hardware-related biases, each contributing to varying levels of positional inaccuracy depending on environmental and operational conditions (Siemuri et al., 2022).

Radio Frequency Interference (RFI) poses a significant risk to the reliability of GNSS systems since GNSS signals arriving at the Earth's surface are naturally weak in power levels (Mehr & Dovis, 2025). Non-intentional RFI occurs due to emissions from other communication systems operating within the vicinity or within the frequency bands of GNSS. Dovis, (2015) highlights that typical sources are distance measuring equipment (DME), tactical air navigation (TACAN) equipment, or emissions from digital TV transmitters and other electronic devices. Such RFIs are typically an artifact of harmonic distortion or intermodulation products and are not intended to impact GNSS signal performance or likely cause any signal quality degradation or negative impact on navigation performance.

Intentional RFI, however, is the purposeful transmission of radio signals for the intent of interfering with GNSS operations. This category includes jamming, spoofing, and meaconing, which represent levels of increasing sophistication and threat, and jamming attempts to overwhelm GNSS receivers with high-power noise signals that make it impossible for them to be able to track actual satellite transmissions. Spoofing, on the other hand, transmits counterfeit GNSS-like signals in an effort to trick a receiver into calculating an incorrect position or time. Mehr & Dovis, (2025) further emphasized that

meaconing differs somewhat in that it captures and retransmits genuine GNSS signals, most often with a delay in time, which provides erroneous positioning information without introducing new signals. Such rogue threats are particularly undesirable in safety-critical applications and point to the need for successful interference detection mechanisms.

2.2.1 Jamming in GNSS Navigation

Jamming is one of the most critical threats to the integrity and reliability of GNSS signals, particularly in safety-critical applications such as vehicular navigation, aviation, and maritime systems. It refers to the intentional transmission of high-power radio frequency signals intending to disrupt or deny the reception of genuine GNSS signals by overwhelming the receiver's front end (Kaplan & Hegarty, 2017). Given that GNSS signals are extremely weak when they reach the Earth's surface, typically below the thermal noise floor, jammers do not require significant transmission power to be effective over short to medium distances. As such, even small, low-cost jamming devices can significantly degrade or completely block positioning services.

The jamming for GNSS receivers is illustrated in **Figure 3**.

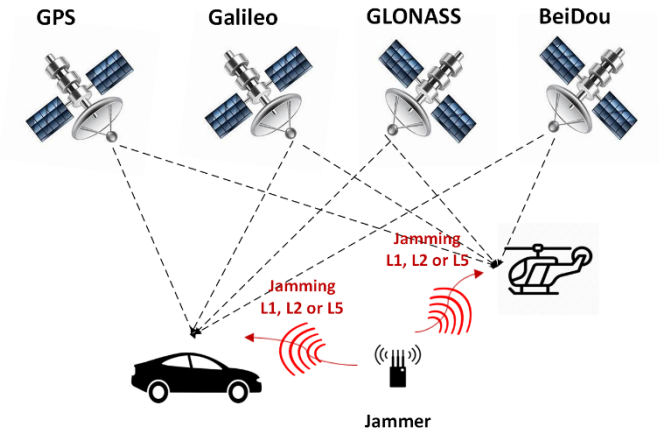

Figure 3: Illustration of Jamming for GNSS Receivers

Ferre et al. (2019) provided a comprehensive classification of GNSS jamming signals based on their modulation characteristics and complexity. They have described AM jammers as simple continuous wave signals, either single- or multi-tone. Chirp jammers

sweep their frequency over time, while FM jammers apply sinusoidal frequency modulation. Pulse jammers transmit short, high-power bursts periodically, and narrowband noise jammers focus interference within specific spectral bands. Each type poses different challenges for GNSS signal detection and reliability.

Jamming signals also vary in complexity, ranging from continuous wave (CW) interference and frequency-modulated (FM) chirp signals to advanced, adaptive interference. Jamming signals may either be structured as narrowband, focused on specific frequency components of GNSS signals, or wideband, which cover entire satellite navigation bands (Elghamrawy et al., 2020). In vehicular contexts, mobile jammers—often carried by vehicles—can lead to intermittent and geographically distributed signal outages, making detection and mitigation particularly challenging (Kreuzer & Munz, 2021). Furthermore, increased availability of online marketplace jamming devices has helped promote the threat. The personal privacy devices (PPDs) are commonly marketed as vehicle tracking blockers, even though they are used illegally in most authorities (Elghamrawy et al., 2022).

The impact of jamming on GNSS receivers is significant in that it can shut down both the acquisition and tracking. In the acquisition process, strong interference in the form of jamming can prevent satellite signals from being received by the receiver, whereas in the tracking process, jamming can result in loss of lock on the signal. This is then followed by erroneous estimates of position, velocity, and time (PVT), or total loss of navigation function (Humphreys et al., 2012). This has direct implications in automotive applications, where GNSS is usually the primary or alternate source of navigation, especially in urban environments where other sensors are already being weakened by multipath or signal blockage. In transport networks, such interference may affect traffic control, fleet management, and more importantly, autonomous driving systems.

2.3 GNSS Jamming Detection Methods

GNSS jamming detection is a necessary component in the context of the reliability and safety of satellite navigation systems. These detections are required in situations where signal integrity is critical, such as transportation, aviation, and emergency services. Unintentional or intentional jamming harms the operation of GNSS receivers by introducing high-power signals that interfere with actual satellite signals. These attacks can potentially reduce positioning accuracy or cause a general loss of signal. Powerful detection mechanisms are essential to enable the implementation of mitigation techniques. Various jamming detection methods, ranging from conventional signal monitoring techniques to sophisticated, data-driven machine learning approaches, will be described under this subsection.

2.3.1 Traditional Approaches for Jamming Detection

Traditional GNSS jamming detection methods primarily rely on monitoring signal power levels, signal-to-noise ratio (SNR) metrics, or other statistical parameters. These approaches detect jamming by identifying abnormal behaviors of these parameters, which may indicate the presence of interference. However, these methods often depend on predefined thresholds. However, these threshold-based methods lead to false alarms or missed detections, especially in dynamic or complex environments (Ferre et al., 2019).

Another conventional technique has been mentioned by Radoš et al., (2024) that involves analyzing the correlator output of GNSS receivers to detect distortions indicative of jamming. Statistical tests, such as the Kolmogorov–Smirnov (KS) test, have been applied to monitor these outputs for anomalies. While this method enhances detection capabilities, it still faces challenges in accurately identifying jamming signals under varying conditions.

Time-frequency analysis methods, including the Wigner–Ville distribution and its variants, have been employed to detect GNSS interference (Sun et al., 2016). These techniques analyze the energy distribution of signals over time and frequency to identify

patterns associated with jamming. They are typically afflicted with cross-term interference and are computationally intensive, which means that they are not as well-suited to real-time applications (Sun et al., 2021).

Furthermore, traditional detection methods may not effectively identify sophisticated jamming techniques, such as frequency-swept or chirp jammers, which can evade simple power or SNR-based detection (Sakorn & Supnithi, 2021a). This limitation underscores the need for more advanced detection mechanisms capable of adapting to evolving jamming strategies.

The summary of traditional GNSS jamming detection methods is given in **Table 1.**

Table 1: Summary Table of Traditional GNSS Jamming Detection Methods

Detection Method	Description	Limitation
Signal power, AGC, and SNR monitoring (Elghamrawy & Noureldin, 2023)	Detects anomalies in signal strength and SNR values	Prone to false alarms, rely on fixed thresholds
Correlator Output Analysis (e.g., KS Test) (Zhou et al., 2024)	Monitors receiver correlator outputs for distortions	Sensitivity to environmental variations; potential for missed detections
Time-Frequency Analysis (e.g., Wigner–Ville) (Sun et al., 2016)	Analyzes signal energy distribution over time and frequency	Computationally intensive; affected by cross-term interference
Basic Threshold-Based Detection (Sakorn & Supnithi, 2021b)	Uses predefined thresholds to identify interference	Ineffective against sophisticated jamming techniques like chirp jammers

2.3.2 Machine Learning for GNSS Jamming Detection

Machine learning (ML) techniques have emerged as highly effective tools for GNSS jamming detection, offering greater adaptability and accuracy compared to traditional signal processing methods. Among supervised learning approaches, algorithms such as Support Vector Machines (SVM), k-Nearest Neighbors (kNN), and Decision Trees have been widely applied to classify jamming signals. They analyse features like signal-to-noise ratios, Doppler shifts, and correlation distortions. For instance, Qin & Dovis, (2022) utilized the kNN method to effectively detect and classify chirp jamming signals, demonstrating the technique's potential in practical GNSS interference scenarios. SVMs, in particular, have demonstrated robust performance in distinguishing between different types of jammers, such as continuous-wave and frequency-sweeping signals, by leveraging well-structured, labeled datasets.

Recent advancements in deep learning have significantly improved GNSS jamming detection, especially by Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks. CNNs are effective in automatically learning hierarchical spatial features from spectrograms or time-frequency representations of GNSS signals, enabling them to identify complex interference patterns that conventional methods might miss (C. Liu et al., 2025). Meanwhile, LSTM networks are well-suited for capturing temporal dependencies in signal sequences, making them ideal for real-time detection of jamming events. In a notable study, Viana et al., (2022) combined CNN and LSTM architectures to detect jamming in UAV applications, achieving an accuracy rate of 99%, underscoring the high potential of hybrid deep learning models in dynamic environments.

Despite their promising performance, DL-based detection methods face several operational challenges. A key limitation is the reliance on large volumes of labelled training data, which are often scarce in the GNSS domain, especially datasets covering varied jamming types, power levels, and environmental conditions. Moreover, deep learning models are computationally demanding, which can hinder their deployment on

devices with limited processing capabilities, such as smartphones or embedded GNSS receivers. Another critical issue is the lack of model interpretability; complex neural networks often function as “black boxes,” making it difficult to understand the reasoning behind their decisions, a drawback that may restrict their use in safety-critical systems where transparency is essential (OpenAI, 2025).

Unsupervised learning methods have been explored to address the scarcity of labelled data in GNSS jamming detection. Techniques such as clustering and anomaly detection can identify unusual patterns in GNSS signals without the need for labelled datasets. For example, clustering algorithms have been used to group similar jamming signals, facilitating the identification of new or evolving jamming techniques. Anomaly detection methods can flag deviations from normal signal behavior, potentially indicating the presence of jamming. However, these unsupervised approaches may suffer from higher false positive rates and may not always provide clear distinctions between different types of jamming.

Hybrid approaches combining supervised and unsupervised learning have also been investigated. For instance, semi-supervised learning techniques can leverage a small amount of labelled data along with a larger pool of unlabelled data to improve model performance. Additionally, self-supervised learning frameworks have been proposed, where models are trained to predict parts of the data from other parts, effectively learning useful representations without explicit labels. These methods hold promise in reducing the dependency on labelled datasets while maintaining high detection accuracy. Furthermore, the application of transfer learning has shown promise in GNSS jamming detection. By leveraging pre-trained models on large datasets, transfer learning can mitigate the challenge of limited labelled data in the GNSS domain. For instance, employing a ResNet18 model with transfer learning has achieved high accuracy in classifying jamming signals, outperforming traditional ML models. This approach enables the adaptation of existing models to new jamming scenarios with reduced training requirements, facilitating more efficient deployment in diverse environments (OpenAI, 2025).

The **Table 2** gives the comparison between traditional detection methods and Machine learning based detection of GNSS jamming.

Table 2: Comparison of Traditional and Machine Learning-Based Methods for GNSS Jamming Detection

Feature	Traditional methods	Machine Learning Techniques
Detection Approach (Radoš et al., 2024)	Threshold-based monitoring of signal parameters	Pattern recognition through learned models
Adaptability (Radoš et al., 2024)	Limited to predefined scenarios	High adaptability to diverse and evolving jamming techniques
Data Requirement (Caputo, n.d.)	Minimal; relies on expert-defined thresholds	Requires large, labelled datasets for training (supervised); less for unsupervised
Computational Demand (Ghanbarzadeh et al., 2025)	Low; suitable for real-time processing on limited hardware	High, may require powerful processors or GPUs
Deployment Complexity (Ghanbarzadeh et al., 2025)	Simple; easy to implement and maintain	Complex; requires expertise in ML and continuous model updates
Robustness to Attacks (Caputo, n.d.)	Vulnerable to sophisticated jamming techniques	Can be robust, but susceptible to adversarial attacks

Machine learning–based GNSS jamming detection methods offer a significant advancement over traditional approaches by enabling the identification of complex and evolving interference patterns through data-driven models. Supervised techniques like SVMs and deep learning architectures such as CNNs and LSTMs have shown high

accuracy in classifying various jamming types. Meanwhile, unsupervised methods, including clustering and anomaly detection, help in scenarios with limited labelled data. Despite their promise, ML models face challenges related to data availability, computational demands, and interpretability. Hybrid and transfer learning approaches are emerging to mitigate these issues, making ML a powerful but still evolving solution in GNSS jamming detection.

2.4 Mitigation Techniques for GNSS Jamming

GNSS jamming poses a significant threat to the reliability and integrity of satellite-based positioning, particularly in safety-critical applications such as aviation, autonomous driving, and military operations. As the reliance on GNSS continues to grow, so does the need for effective countermeasures against intentional or unintentional signal interference. Mitigation techniques aim to detect, reduce, or eliminate the impact of jamming on GNSS receivers, ensuring continuity and accuracy of navigation services. These techniques range from traditional signal processing methods, such as antenna design and filtering, to advanced data-driven approaches like machine learning, which can identify and adapt to interference patterns in real time. This section explores various GNSS jamming mitigation strategies, focusing on both conventional and emerging solutions to enhance system resilience.

2.4.1 Traditional Error Mitigation Methods

The accuracy and reliability of GNSS are frequently compromised by various errors, including ionospheric delays, satellite clock discrepancies, orbital inaccuracies, and, most critically in hostile or urban environments, radio frequency interference such as jamming. In response to these challenges, several traditional error mitigation and signal integrity techniques have been developed, particularly for use in high-stakes sectors like aviation, autonomous vehicle navigation, and military operations (Paziewski et al., 2019).

Among the most widely used techniques is Differential GNSS (DGNSS), which significantly improves positioning precision by employing ground-based reference

stations that track satellite signals and compute real-time correction data. These corrections are transmitted to GNSS receivers to filter out common errors such as satellite clock drift, orbital errors, and atmospheric delays. DGNSS has been effectively applied in marine navigation, geodetic surveying, and aviation (W. Liu et al., 2019). However, its effectiveness is inherently limited by the density and distribution of reference stations, restricting its utility in sparsely covered regions.

Another key integrity mechanism is Receiver Autonomous Integrity Monitoring (RAIM), which operates independently of ground infrastructure. RAIM uses redundant satellite measurements and statistical analyses to detect inconsistencies or anomalies in signal data (Borhani-Darian et al., 2024). This method is particularly valuable in aviation, where navigation errors pose serious safety risks. Nevertheless, RAIM's performance depends on the geometric availability of at least five visible satellites, which can be a significant limitation in obstructed environments (Zangenehnejad & Gao, 2021).

Satellite-Based Augmentation Systems (SBAS) offer another layer of correction, broadcasting error mitigation data from geostationary satellites. Systems like WAAS in the U.S., EGNOS in Europe, and MSAS in Japan provide continent-wide correction services, enhancing GNSS accuracy and integrity for applications ranging from civil aviation to land transportation (Realini et al., 2017). These systems, however, often suffer from high latency and a dependency on terrestrial infrastructure, reducing their effectiveness in military or densely built urban areas.

One of the most pressing GNSS threats is intentional jamming, which involves the emission of high-powered radio signals that overwhelm the GNSS signal at the receiver. As GNSS signals are inherently weak upon reaching the Earth's surface, jammers require minimal power to be effective over short ranges (Broumandan & Lachapelle, 2018). In response, anti-jamming technologies have been developed, including adaptive antenna arrays capable of spatial filtering, notch filters to suppress specific interference bands, and dynamic power control to optimize receiver sensitivity (Lachapelle et al., 2018). While effective against low-power and narrowband interference, these techniques often

struggle against high-power, broadband, or adaptive jamming sources, which are becoming increasingly prevalent.

Spoofing is a threat that generates fake GNSS signals that can mislead the receiver into calculating incorrect positions. It is a distinct and sophisticated threat. Whereas jamming directly disrupts signal availability, and it is a quick and brute-force form of attack. Despite this distinction, both types of interference highlight the need for more resilient GNSS security measures.

To complement these conventional methods, the use of multi-frequency and multi-constellation GNSS receivers has grown. These receivers can mitigate ionospheric errors by comparing signals across different frequencies and reduce dependency on a single GNSS system (e.g., GPS) by leveraging signals from Galileo, GLONASS, and BeiDou (Wu et al., 2019). This diversification improves robustness, especially in environments where line-of-sight is frequently obstructed.

However, the increasing complexity and sophistication of GNSS threats—particularly those posed by modern jamming techniques—have exposed the limitations of traditional mitigation strategies. Many still rely heavily on fixed infrastructure or static algorithms and are not adaptive to evolving attack methods or dynamic environments (Chen et al., 2019). Consequently, recent research has begun exploring artificial intelligence (AI) and ML approaches to improve GNSS resilience (Dabove & Di Pietra, 2019). These methods enable systems to learn patterns of interference, predict potential errors, and adapt positioning computations in real time (Hu et al., 2023). For example, ML algorithms can analyze GNSS signal data to detect jamming attempts early or compensate for multipath distortions more effectively than classical filtering techniques.

Ultimately, while traditional techniques such as DGNSS, RAIM, SBAS, and anti-jamming filters remain foundational, they are increasingly supplemented by modern approaches like AI-based detection, sensor fusion, and high-level cryptography. The integration of these tools is essential to secure GNSS navigation, particularly in mission-critical and highly dynamic environments. Continued innovation in this field is necessary to ensure

GNSS can remain a reliable component in future transportation, defense, and autonomous systems (Wu et al., 2019).

2.4.2 Machine Learning Based Jamming Mitigation Techniques

ML has emerged as a powerful tool not only for GNSS error detection but also for mitigating signal degradation due to jamming, multipath, and environmental interference. Deep learning models such as feedforward neural networks and long short-term memory (LSTM) networks have shown high potential in learning patterns between GNSS signal parameters and their respective error sources (G. Li & Geng, 2019). These models are trained using large datasets to distinguish between genuine and altered signals, improving location accuracy—especially in complex urban environments where multipath effects are prevalent (Borhani-Darian et al., 2024). ML-based suppression of delayed signals leads to cleaner, more precise positioning critical for vehicle tracking and navigation.

Another significant area of ML application is in sensor fusion, where GNSS data is combined with inputs from inertial measurement units (IMUs), LiDAR, and cameras to improve accuracy and reliability. Traditional techniques such as Kalman filters have been extended by ML models that dynamically adjust sensor weights based on changing environmental conditions (Wu et al., 2019). Reinforcement learning and Bayesian inference are also being explored to create adaptive systems capable of maintaining positional accuracy in GNSS-denied environments like tunnels or dense cities. This is particularly relevant for autonomous vehicles and UAVs, where real-time, resilient navigation is essential.

ML models are also utilized for predictive error modeling, employing architectures like recurrent neural networks (RNNs) and transformer models to capture temporal dependencies in GNSS data (Ghanbarzadeh et al., 2025). These systems proactively predict and correct GNSS signal anomalies before they affect navigation accuracy. Furthermore, anti-jamming and anti-spoofing strategies have been enhanced using

adversarial learning techniques and generative adversarial networks (GANs), which simulate attack conditions and train robust detection models (Wen et al., 2020). As GNSS vulnerabilities continue to grow, such countermeasures are essential in securing critical navigation systems.

Looking forward, innovations such as quantum machine learning and federated learning are anticipated to revolutionize GNSS error mitigation (Szot et al., 2019). Quantum ML promises rapid real-time error corrections with enhanced computational power, while federated learning enables decentralized model training that ensures user privacy and data security. Combined with pattern recognition and unsupervised anomaly detection, these technologies will drive the future of secure and highly accurate GNSS systems, enabling their reliability even in dynamic, signal-challenging environments (Aggrey et al., 2020).

2.5 Smartphone Sensors and Sensor Fusion in GNSS Navigation

Modern smartphones are equipped with a wide array of sensors that significantly enhance GNSS-based navigation, particularly in environments where satellite signals are weak or unavailable. These sensors—including accelerometers, gyroscopes, magnetometers, barometers, and cameras—serve as complementary technologies to overcome GNSS limitations in areas like urban canyons, tunnels, or indoors. For example, accelerometers and gyroscopes support dead reckoning by tracking linear and angular motion when GNSS signals are blocked, although both are prone to drift errors over time and require sensor fusion for improved accuracy (Z. Li et al., 2022).

Magnetometers provide heading information and function as digital compasses, proving useful in orientation-dependent applications like pedestrian and automotive navigation. However, their performance can be affected by electromagnetic interference, especially in urban areas, necessitating calibration and integration with other sensor data (Robustelli et al., 2019). Barometers offer valuable altitude information, improving vertical accuracy in multi-level buildings and supporting use cases like emergency response and indoor navigation (Paziewski et al., 2019). Cameras, used in Visual SLAM,

have emerged as powerful localization tools, enabling the device to construct maps and determine positions simultaneously through computer vision and deep learning techniques (Chen et al., 2019).

In the absence of GNSS signals, especially indoors or underground, smartphones leverage alternative technologies such as Wi-Fi fingerprinting and Bluetooth beacons. These approaches rely on databases of signal characteristics to approximate user locations with relatively high precision (Wen et al., 2020). Additionally, inertial sensors combined with environmental maps can estimate movement in confined areas like subways or tunnels. This redundancy ensures navigation continuity when satellite-based systems are insufficient (Robustelli et al., 2019).

To further enhance navigation accuracy, sensor fusion techniques have become central. Kalman Filters are widely used to integrate GNSS with IMU data, allowing reliable navigation during temporary GNSS outages, such as in urban environments. Particle Filters provide advantages in nonlinear conditions by probabilistically estimating position based on diverse sensor inputs, making them suitable for indoor navigation scenarios. Recently, deep learning-based fusion techniques have gained traction, offering adaptability and robustness by learning complex patterns from multi-sensor inputs, supporting advanced applications in robotics and autonomous vehicles (Yi et al., 2022).

2.6 Chapter Summary and Research Gaps

GNSS jamming presents a serious threat to the integrity of navigation services, particularly in critical applications such as transportation, aviation, and emergency response. Traditional jamming detection techniques, which rely on signal strength, correlator outputs, and time-frequency analysis, are often limited by their reliance on static thresholds and their inability to detect sophisticated interference methods like chirp jamming. In contrast, ML techniques—especially supervised approaches such as SVMs and deep learning models like CNNs and LSTMs—offer enhanced adaptability and accuracy by learning complex patterns from signal data. Unsupervised and hybrid ML approaches also show promise in overcoming the challenge of limited labelled data.

However, most existing models rely on a combination of multiple signal features and are computationally intensive, posing difficulties for real-time deployment on consumer devices.

While prior studies have demonstrated the effectiveness of ML-based GNSS jamming detection using rich feature sets, little attention has been given to the potential of AGC data as a standalone input. Existing work rarely investigates the exclusive use of AGC—an inherently available and lightweight signal metric, for both supervised and unsupervised ML models. Furthermore, there is a lack of comparative studies evaluating the performance of these models in real-world, dynamic jamming scenarios using AGC data collected from consumer-grade GNSS devices. This research aims to address this gap by developing a scalable framework that uses only AGC data for GNSS jamming detection, with a focus on accuracy, robustness, and feasibility for real-time applications on resource-limited platforms.

3 Methodology

This chapter outlines the systematic approach employed in developing machine learning frameworks for detecting GNSS signal jamming in real-world scenarios using AGC data. The methodology is divided into several phases: research design, data collection, preprocessing, feature extraction, model development, and evaluation.

3.1 Research Design and Approach

The research aims to develop both unsupervised and supervised models capable of distinguishing between the normal and jammed GNSS signal conditions using AGC data collected from the mobile receiver. In addition to model development, the study provides a comprehensive comparison between the two approaches. The research follows an experiential design, incorporating real-world AGC data and model evaluation to ensure the framework captures realistic jamming scenarios and receiver behavior. Although the analysis is quantitative in nature, it contributes to a broader understanding of jamming detection methodologies. The overall workflow of the study is illustrated in **Figure 4**.

3.2 Data Collection

The dataset used in this study was collected during the *Jammertest* conducted in Norway under various controlled jamming, spoofing, and meaconing scenarios. The study focuses only on the jamming effect on GNSS signals, and the selected scenario involves mobile GNSS reception under multiple stationary jammers, representing a realistic and challenging detection environment. The vehicle root is an open sky path that promises that the other GNSS errors, such as multipath effects, have no effect on the GNSS signals. The **Figure 5 (a)** shows the environment of the path during the test.

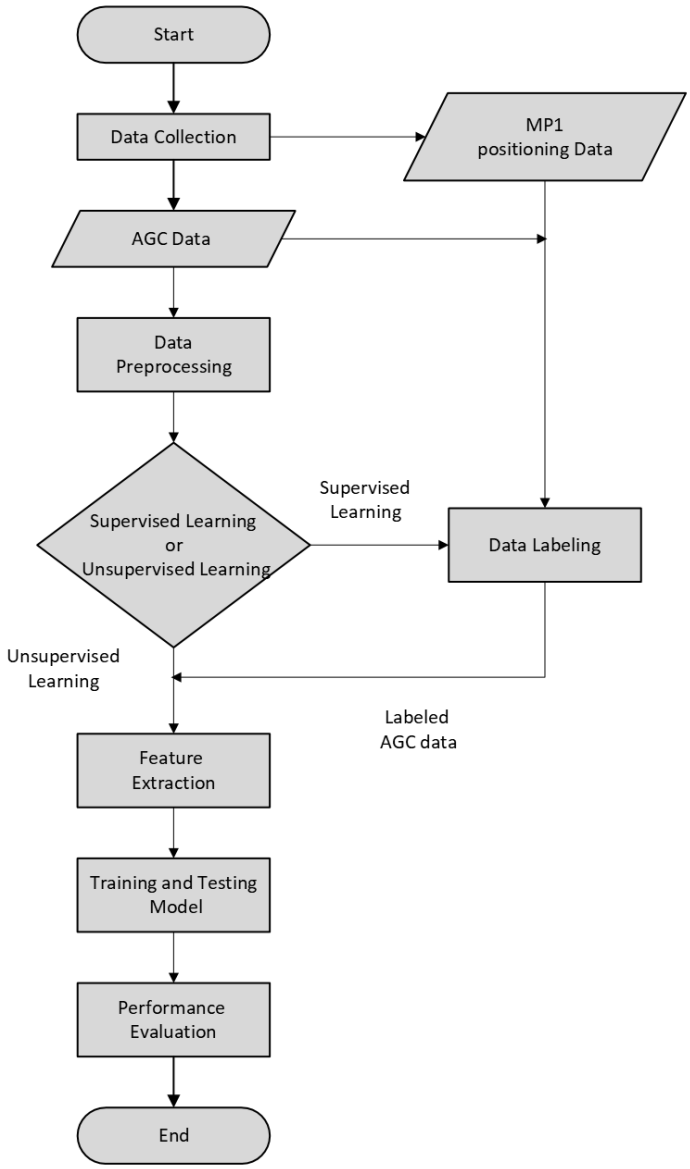

Figure 4: The Overall Workflow of the Study

3.2.1 Jammertest Setup

In the chosen test case, three jammers were deployed at fixed intervals along a 1-kilometer section of road between Nordmela and Stave. Each jammer was mounted on the roof of a stationary vehicle, with antennas oriented in distinct configurations. Specifically, all three jammers were positioned such that their antennas pointed upward toward a moving test vehicle equipped with GNSS receivers, or antennas were laid flat (i.e., facing downward toward the road surface).

The test vehicle is equipped with standard GNSS receivers and mobile phones to collect GNSS live data (e.g. ublox positioning, IMU, odometer, AGC). The geospatial layout of the jamming locations is illustrated in **Figure 5 (b)**.

a b

Figure 5: (a) The Test Environment (b) The Geospatial Layout of the Jamming Locations

3.2.2 Sensor Data Sources

Three handheld multi-band jammers, designated as H6.1, H6.2, and H6.3, were used during the test. These devices are battery-powered and user-operable via a simple interface, including an on/off button, LED indicators, and DIP switches to toggle between frequency bands.

- **H6.1**: This jammer transmits over six bands, but only two are relevant to GNSS. Both fall within the upper L-band ("L1-only"), thereby primarily affecting GPS L1/E1/B1C signals. The relevant antenna for GNSS interference is labelled "6". To limit unintentional disruption of non-GNSS signals, only this antenna was activated during the test.
- **H6.2 and H6.3**: These are also six-band jammers but have broader GNSS coverage. They transmit across the L1, L2, and L5 bands, affecting both upper and lower L-band frequencies. The active antennas for these devices are labelled "4" (L1), "5" (L5), and "6" (L2).

An overview of the jammer specifications, including output power and targeted GNSS bands, is provided in **Table 3**.

Table 3: An Overview of the Jammer Specifications

Jammer	Min Power (W)	Max Power (W)	Test Bands (As per Annex A)
H6.1 (Jammer 3)	0.631	0.631	G1, L1, E1, B1C
H6.2 (Jammer 2)	0.3981	1.000	L1, E1, B1C, E6, B3I, G2, L2, E5b, B2b, B2I, G3, L5, E5a, B2a
H6.3 (Jammer 1)	0.3981	1.000	L1, E1, B1C, E6, B3I, G2, L2, E5b, B2b, B2I, G3, L5, E5a, B2a

Jammer 1 and 2 can be categorized as broadband jammers because they affect all the bands. However, Jammer 3 can be identified as a narrowband jammer that affected only a single frequency band (L1). GNSS signal behaviour for each frequency band is shown in **Figure 6.**

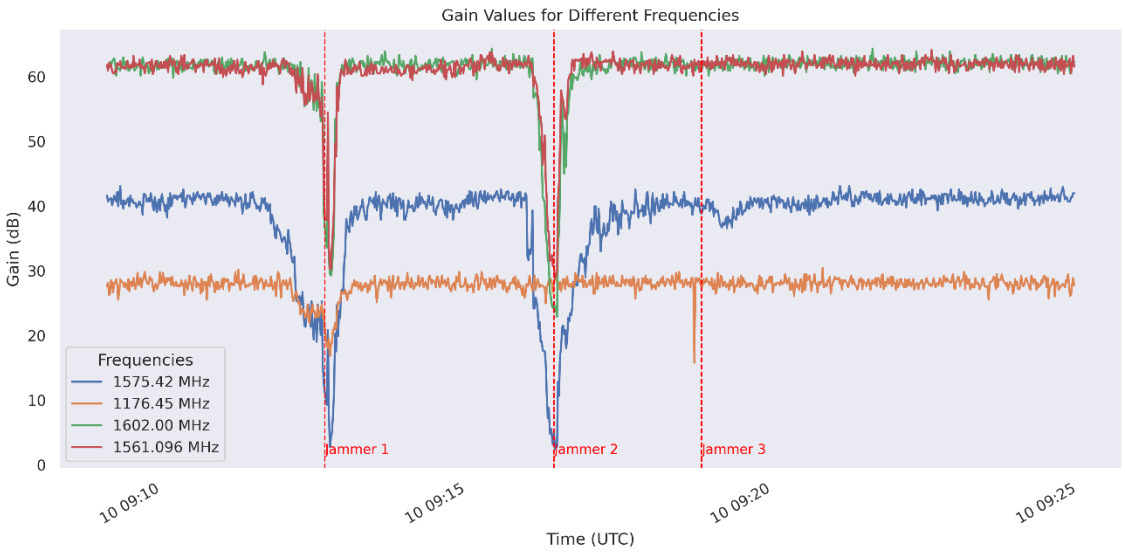

Figure 6: GNSS Signal Behaviour for Each Band

Based on the figure above, Jammers 1 and 2 appear to have impacted all observed frequency bands. In contrast, Jammer 3 primarily affected the 1575.42 MHz band and other frequencies have not responded to the Jammer 3.

3.2.3 Data Acquisition

The AGC data used in this study was collected using the GNSS Logger application installed on a Google Pixel smartphone. This application has captured raw positioning data, IMU data, and AGC data during the test period. The test data is stored in an HDF5 file, and the details about each test case have been stored in a separate metadata file. For the current analysis, the AGC data and positioning data are extracted and processed. However, positioning data is used only for the data labelling process.

AGC Data

AGC mechanism is significant in GNSS signal jamming detection because it dynamically adjusts the gain value of the receiver to maintain the same signal strength even with fluctuation of input power. As RFI, i.e., intentional jamming, is introduced in the GNSS band, thermal noise floor rises, and AGC consequently decreases gain in a bid to prevent signal saturation (Spens et al., 2022) The decrease reveals as a measurable reduction of AGC values, which itself can be utilized as a consistent metric of abnormal signal conditions. Because AGC reacts with an instant response to changes in the input's power within a specific range of frequencies, stable changes of its output, particularly steep decreases, can signify the presence and relative power of the jamming signals.

Figure 7 presents the AGC test data and positioning information collected during Test 2.2.3, in which the vehicle was driven toward Nordmela. The first three plots display the vehicle's geographical coordinates, north, east, and height. The fourth plot illustrates the quality factor (Q), an indicator of the reliability of satellite observations, and the number of visible satellites is in the fifth plot. The next plot is the velocity variations over time. Notably, data gaps appear in these plots as the vehicle passes near the jamming sources.

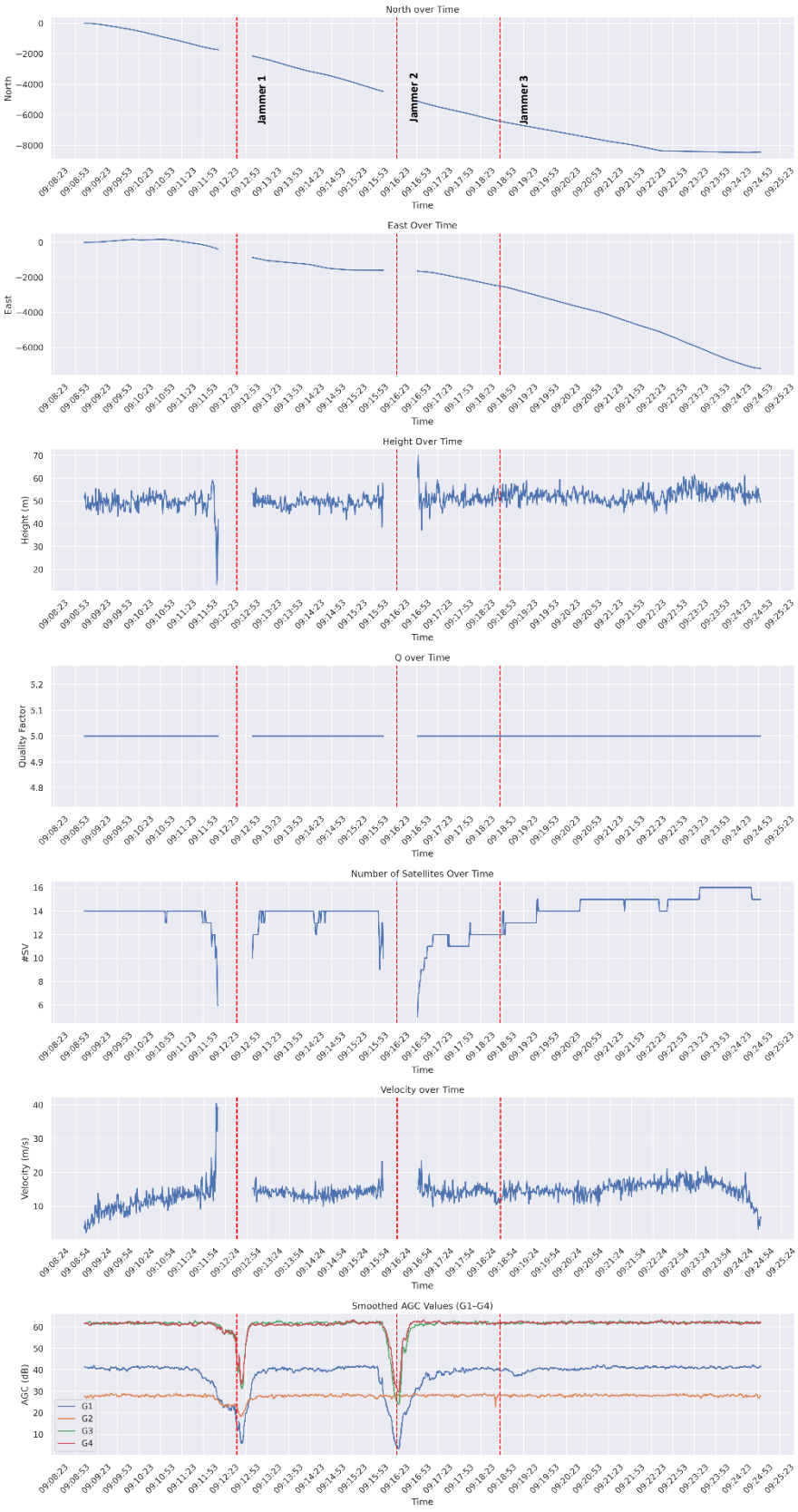

Figure 7: The Position and AGC Data over Time for Test Case 2.2.3.

The final graph shows variations in the AGC values over time. A sharp variation can be noted during the first two jamming periods, while the third jamming period does not show a significant effect on AGC data. Further, the impact on each band is also varied.

It can be observed that Jammer 1 and Jammer 2 significantly disrupted the positioning system, leading to a loss or degradation of the computed positional data. In contrast, Jammer 3 had no discernible impact on the integrity of the positioning information.

3.2.4 Impact of Jamming for Positioning and AGC Data

The impact of jamming on positioning accuracy and AGC data during the first jamming event is illustrated in **Figure 8**. A sudden loss of east and north values occurs as the vehicle approaches the jammer, and it takes approximately 20 seconds for the receiver to reacquire valid positioning data. The position values decrease smoothly during the normal (non-jammed) period. However, it is possible to observe a jump in height just before data loss, while there are minor variations under normal conditions; The quality factor is 5 under normal conditions, representing a single-point positioning solution. This parameter also drops as the vehicle enters the jamming zone.

As shown in the fifth plot, the number of visible satellites gradually decreases, and the jammer disrupts satellite visibility for more than one minute. A sudden spike in velocity is also observed just before data loss. Overall, the positioning data is unavailable for approximately 50 seconds during the jamming period, and this duration may vary from jammer to jammer depending on their signal strength.

The AGC data shows a gradual slope lasting about 25 seconds before falling sharply as the vehicle passes the jammer. The fall continues for approximately 10 seconds, after which the recovery in AGC values starts, returning to normal after a short delay. It can also be seen that jamming effects are not the same in all GNSS frequency bands.

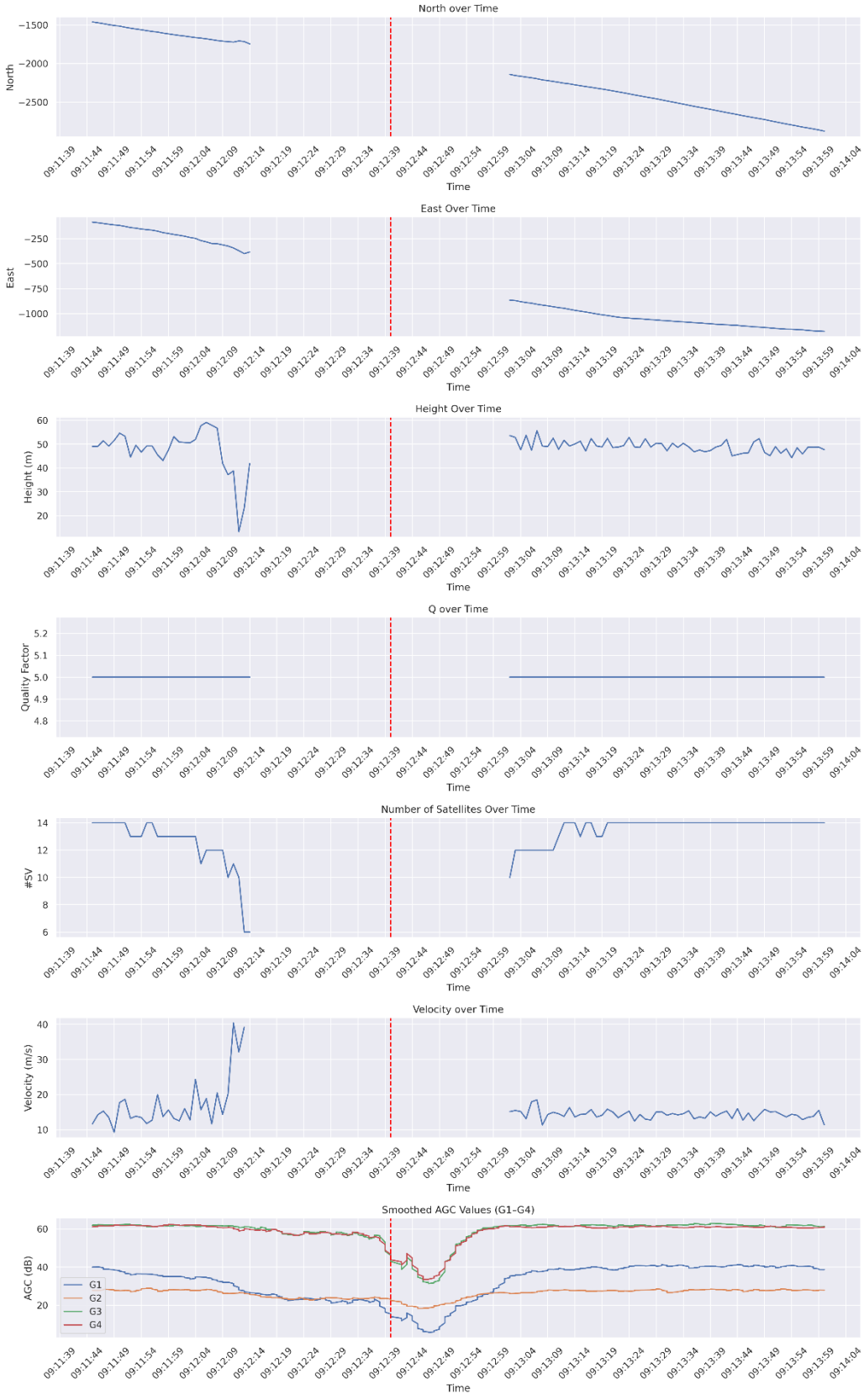

Figure 8: The Jamming Impact on Observed Data

3.2.5 The Vehicle Track in Geographical and ENU Coordinates Systems

The localization of the test vehicle in geographical and ENU coordinates systems are shown in **Figure 9**.

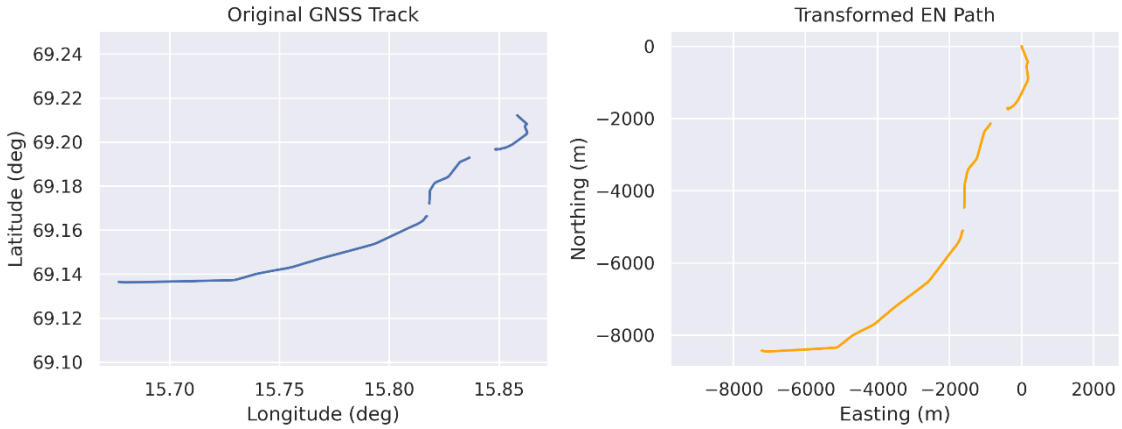

Figure 9: The vehicle track in geographical and ENU coordinates systems

3.3 Preprocessing and Labelling

3.3.1 Data Preprocessing

To enhance signal quality and reduce the impact of high-frequency noise, Exponential Moving Average (EMA) smoothing was applied to the AGC data before model training. EMA is a type of low-pass filter that assigns exponentially decreasing weights to older observations. This helps in capturing short-term trends effectively while preserving the overall shape of the signal (OpenAI, 2025).

Compared to simple moving averages, EMA responds more quickly to recent changes in the data, which is beneficial in detecting rapid changes caused by jamming events. By applying EMA smoothing, fluctuations due to random measurement noise are attenuated, allowing the machine learning models to focus on more meaningful variations in the AGC signal that are indicative of interference or normal conditions.

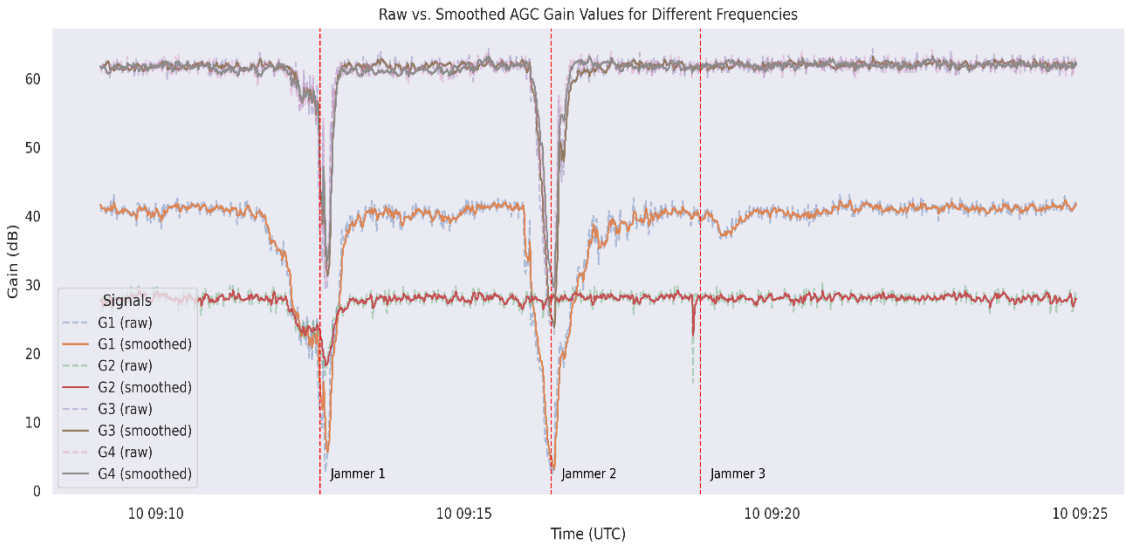

Figure 10: Effect of EMA Smoothing on AGC Data for Each Frequency

Figure 10 demonstrates how EMA smoothing enhances the AGC signal by reducing short-term fluctuations while preserving overall trends. The figure shows that the smoothed signals for each frequency band follow the same pattern as the original signals while reducing the unwanted spikes of the signal. It would be very useful to detect anomalies in the AGC data.

3.3.2 Data Labelling for Supervised Machine Learning Model

This study examines supervised and unsupervised machine learning algorithms for detecting jamming in GNSS. One of the biggest challenges is the absence of an explicit ground truth label for the data. The challenge has been addressed by using positioning data as a reference for labelling. Time slots during which positioning data, including latitude, longitude, quality indicator (Q), and number of visible satellites, are absent, are considered a potential jamming event. By contrast, data points containing valid positioning information are considered normal conditions. The AGC data in jamming period is labelled as **'1'**, and normal data are taken as **'0'**.

Figure 11 illustrates how the labelling process captures the jamming and normal period. The shaded green areas represent the normal period. The third jamming period is not taken as jamming since it does not affect the positioning.

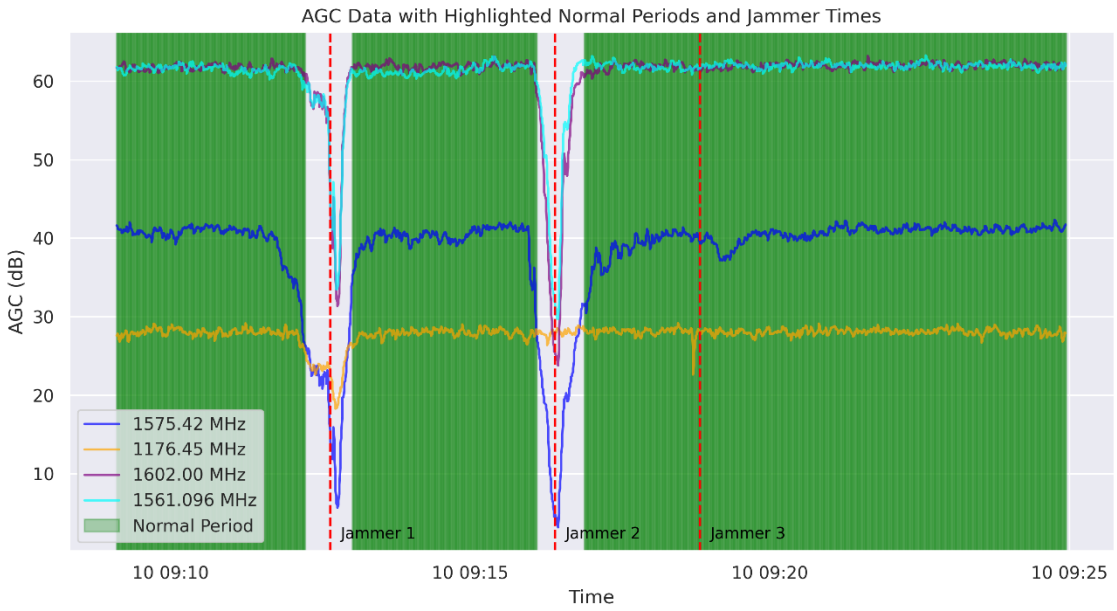

Figure 11: AGC Data with Highlighted Normal Period

3.4 Feature Selection and Extraction

Feature engineering is one of the most important steps in developing consistent machine learning models for GNSS signal anomaly detection. In this work, I focused on extracting temporal and statistical features from AGC data, a signal power metric, to detect the variations that are indicative of jamming. The same pipeline was used for supervised and unsupervised learning models.

3.4.1 Rationale for Using AGC Data

AGC values are actively controlled by GNSS receivers to maintain constant signal power. In normal operation conditions, AGC values should be within some expected range. However, in jamming conditions, artificial signal interference causes abnormal changes in signal power and results in prominent AGC adjustments. Therefore, fluctuations in AGC values are a robust method to determine probable interference, i.e., jamming.

3.4.2 Feature Selection

To effectively identify GNSS signal anomalies such as jamming, an underlying dynamics-based feature selection of the AGC signal is essential to ensure successful detection. For this study, domain expertise and empirical observation of the AGC during clear and jamming conditions guided feature selection. Since the values of the AGC respond to changes in the received signal power, features representing central tendency, extreme measurements, and temporal variability were identified as the most informative.

The selected features include:

- Mean: to capture the central value of the AGC in a window.
- Minimum and Maximum: to identify spike values potentially due to sudden variation of the signal.
- Range (max - min): as a measure of short-term signal volatility.

Other aspects, such as slope and standard deviation, were also explored, but were excluded from the final model upon initial performance evaluation and to reduce dimensionality, especially within the supervised environment. The selection is made for balancing computation with detection performance, especially when employed in the sliding-window method.

3.4.3 Feature Extraction

For feature capture extraction that indicates local deviations in the AGC signal typical of interference, a sliding window feature extraction was applied. The feature extraction has the capability to observe signal features over time locally by dividing the AGC data into overlapping windows of the same size (window size) and computing descriptive statistics for each window. The temporal resolution and overlap of the output feature set are governed by the sliding step (step size). The selection of window size and step size needs to be done carefully. The window size should be large enough to capture the meaningful features. However, it should be kept as small as possible to ensure that the window does not lag behind real data (G. Huang et al., 2022).

The AGC signal is captured in four unique frequency bands, which are G1, G2, G3, and G4 (*1575.42 MHz, 1176.45 MHz, 1602.00 MHz, and 1561.096 MHz, respectively*). They correspond to different GNSS signal carrier frequencies, and the AGC response is varied depending on the interference affecting each band. To preserve the separate temporal dynamics of each band, features were extracted separately for each AGC signal, creating a multidimensional feature space. For each frequency band in a given window, mean, maximum and minimum, and range were computed.

This results in a feature vector that includes the above metrics for each of the four bands. For example, with three features per band across four bands, each window yields a 12-dimensional feature vector (e.g., G1_mean, G1_min, G1_max, ..., G4_max).

In supervised learning scenarios, a label is also assigned to each window using the majority class (e.g., normal or jamming) present among the samples in that window. This allows the features to be used for both classification and unsupervised anomaly detection.

The multi-dimensional feature set retains the band-specific characteristics of the AGC signal, which is critical for distinguishing between normal variability and targeted interference affecting one or more frequency bands.

3.5 Machine Learning Model Development

This section outlines the machine learning models developed for GNSS jamming detection, covering both a supervised learning approach using Random Forest and an unsupervised method based on Isolation Forest. Each model was selected based on its suitability for the data characteristics and the nature of the detection problem.

3.5.1 Model Selection

To address the issue of GNSS signal anomaly detection, unsupervised and supervised learning approaches were employed to manage different labelling data situations. Two models were selected for their use in high-dimensional time-series features, noise resistance, and proven performance in anomaly detection issues:

Isolation Forest (Unsupervised)

For unsupervised anomaly detection, the Isolation Forest model was selected. The model is highly suitable for identifying infrequent and anomalous patterns in high-dimensional space without requiring ground truth. It operates by constructing random decision trees and isolating observations; anomalies tend to be easier to isolate and therefore have shorter average path lengths.

Isolation Forest was chosen due to the following advantages:

- No requirement for labelled data, so usable in early-stage or real-time detection where ground truth is absent.
- Efficient and scalable, applicable to large time-series datasets generated by AGC signals.
- Effective for high-dimensional feature sets, such as those derived from multiple frequency bands.

In this study, the model was trained on features extracted from presumed “normal” periods, and anomalies were detected during test windows by comparing their isolation depth against the learned distribution.

XGBoost (Supervised)

For the supervised learning scenario, the Extreme Gradient Boosting (XGBoost) algorithm was employed. XGBoost can be defined as a tree-based ensemble algorithm that builds additive models in a forward stage-wise manner and optimizes a differentiable loss function. Strong prediction performance, regularization, and management of class imbalance are the main advantages of the model.

XGBoost was chosen due to:

- High classification accuracy, especially with structured tabular features.
- Integrated missing value and outlier treatment, which is useful when exploring GNSS signal environments.
- Interpretability, via feature importance scores, to explore which AGC bands and metrics are most predictive of jamming.

The model was trained using the labelled data with the feature windows labelled as normal or jammed, depending on the ground truth derived from controlled jamming experiments. The XGBoost classifier gives a probability of jamming, which can be thresholded to generate binary predictions.

3.5.2 Training and Testing

The training and evaluation procedures were tailored for both supervised and unsupervised learning models, reflecting their respective assumptions about the availability of labelled data. Both models utilized a shared feature extraction process from a sliding window algorithm on AGC data.

Supervised Model: XGBoost Classifier

Training and testing of the XGBoost model were a standard supervised machine learning pipeline:

Feature Preparation

As outlined in Section 3.4, a sliding window technique was used to compute statistical features—including mean, minimum, maximum, range, and optionally slope—from each AGC frequency band. Each window received a binary label (jamming or normal) based on the most occurring ground truth value in the window.

Data Splitting

The dataset was divided into training and testing subsets using an 80/20 stratified split to preserve the class distribution, which is especially important in the case of class

imbalance. Stratification served to guarantee that both the normal and jamming cases were adequately represented in each subset.

Model Training

The XGBoost model was trained using binary logistic loss and default hyperparameters. This gradient-boosted decision tree algorithm is specifically suited for tabular data with a mix of distributions and was selected by virtue of high accuracy and resistance to overfitting.

Model Evaluation

The classifier was evaluated on the test set on the basis of accuracy, precision, recall, and F1-score, providing an overall indication of whether or not it can detect jamming instances correctly.

Unsupervised Model: Isolation Forest

The Isolation Forest model was trained on normal (not jamming) data alone and is hence particularly well-suited for anomaly detection scenarios where labelled anomaly data may not be easily available.

Feature Preparation

The same sliding window approach and statistical feature extraction were applied, as in the supervised case, to ensure consistency in feature representation.

Training and Testing Strategy

A known jamming interval was predefined based on the experimental setup, and all data outside this interval was considered normal. This normal subset was used to train the Isolation Forest, which learns the structure of typical AGC behavior by isolating observations through random partitioning.

Data Augmentation and Scaling

To enhance the model's generalization to unseen normal variations, data augmentation techniques were applied to the training set:

- Jittering introduced small random noise.
- Scaling altered the amplitude of features to simulate dynamic signal environments.
- All features were standardized using StandardScaler prior to model fitting.

Anomaly Detection

After training, the model was applied to the full dataset. Any feature window with a significantly short average path length (i.e., easy to isolate) was flagged as an anomaly. These were interpreted as potential jamming events.

3.5.3 Tools and Libraries

All data analysis, processing, and modeling were conducted using the **Python programming language**, thanks to its extensive data science and machine learning ecosystem. **Google Colab** provided a flexible platform to develop the models. The following frameworks and libraries were used throughout the study:

Scikit-learn

Used for both the development of the Isolation Forest and XGBoost models (via the sklearn.ensemble and xgboost interfaces, respectively) as well as feature scaling (StandardScaler), splitting data, and metrics for measuring performance.

Pandas and NumPy

Heavily utilized for data manipulation, pre-processing, and numerical computation. Pandas provided simple-to-use functionality for time-indexed AGC data manipulation and label sliding window manipulation, and NumPy provided support for high-speed numerical computations in feature extraction and augmentation.

Matplotlib and Seaborn

Employed to visualize AGC signal behavior, model predictions, and feature distributions. Further, the raw data visualization was done using these libraries. These libraries facilitated the generation of high-quality plots used for both exploratory analysis and result presentation.

Custom Python Functions

Several domain-specific functions were developed to support:

- Feature extraction from AGC signals using sliding windows.
- EMA smoothing to denoise raw AGC measurements.
- Data augmentation techniques (jittering and scaling) to enrich the training data for unsupervised learning.

These tools collectively enabled an efficient, reproducible, and scalable workflow for GNSS signal anomaly detection.

3.6 Performance and Evaluation Metrics

Quantitative comparison of the performance of supervised and unsupervised models was conducted through standard classification metrics. These metrics provided a comprehensive evaluation of how each model effectively detects GNSS signal anomalies and, more crucially, jamming events in various signal conditions.

3.6.1 Evaluation Metrics

The following performance indicators were employed:

- Accuracy: The proportion of correctly classified instances (both normal and jamming) over the total number of predictions.
- Precision: The proportion of correctly identified jamming instances out of all instances predicted as jamming (i.e., the ability to avoid false alarms).
- Recall: The proportion of actual jamming occurrences correctly identified, which means the ability to recognize actual jamming.

- F1-Score: Harmonic mean between precision and recall, providing a balanced measure, particularly useful in class-imbalanced situations.
- Confusion Matrix: Tabular summary reporting true positives, true negatives, false positives, and false negatives.

These values were calculated with the in-built functions of the scikit-learn library. The classification report and confusion matrix provided information regarding model strengths and failure modes.

3.6.2 Validation Approach

For the supervised model (XGBoost), performance was evaluated using 3-fold cross-validation on the training set to ensure robustness and reduce variance in the results. Final evaluation was performed on a held-out test set following cross-validation.
For the unsupervised model (Isolation Forest), normal (non-jammed) data alone was trained upon. Testing was performed on the full dataset, including known jamming intervals. For aligning predictions to ground truth labels:

- The prediction DataFrame (full_data) and the feature-label DataFrame (features_df) were merged based on timestamps to ensure alignment.
- Only matching entries were retained using an inner join.
- True labels and predicted labels were extracted and used to compute the confusion matrix, classification report, and accuracy.

This evaluation procedure ensured consistency and allowed for direct comparison between the predicted anomalies and the actual jamming events annotated in the dataset.

3.7 Summary

In this chapter, the methodology for the detection of GNSS jamming using supervised and unsupervised machine learning was presented. The process began with the preprocessing of AGC data, e.g., frequency-specific exponential moving average (EMA) smoothing, followed by feature engineering using a sliding window strategy. Key temporal and statistical features were extracted independently from four frequency bands, resulting in a multidimensional representation of signal behavior suitable for anomaly detection.

Two models were used: Isolation Forest in unsupervised and XGBoost for supervised classification. Both models underwent tailored training protocols. The Isolation Forest was trained on normal signal patterns alone, with jittering and scaling augmentation incorporated to improve generalization. The XGBoost model was trained on labelled data with a stratified train-test split and validated by 3-fold cross-validation to check the robustness.

Standard accuracy, precision, recall, and F1-score performance measures were utilized for model evaluation. Results were obtained by cross-referencing prediction outputs with ground truth labels using timestamp-based merging to enable the generation of a confusion matrix and classification report, and further thorough performance analysis.

Overall, this methodology provides a scalable and effective framework for GNSS signal anomaly detection, with potential applicability to real-time and embedded systems.

4 Analysis and Results

This chapter provides a detailed analysis of the performance of supervised and unsupervised ML models. It presents an overview of the experimental data set and the results obtained from each model. The chapter also includes the validation and feature importance.

4.1 Overview of the Dataset and Experimental Setup

This section outlines the dataset used for model training and evaluation. The data consists of AGC signal measurements collected from a smartphone GNSS receiver. The data are labelled to identify periods of normal operation and jamming. These labels served as the ground truth for the supervised learning model. The dataset was preprocessed using EMA smoothing to remove unwanted spikes, and feature extraction through sliding windows was employed to prepare the data for both supervised and unsupervised modeling. Additionally, data augmentation was used across the board to enhance the data.

Dataset Composition

The dataset used here was constructed from AGC measurements in a real-world vehicular GNSS environment. The sliding window approach was used to capture the dynamic character of AGC as it changes with varying signal conditions, as follows:

- Window size: 2 samples
- Step size: 1 sample (50% overlap)

Each window represents a short-term temporal snapshot of AGC behavior across four GNSS frequency bands. The increase in window size may lead to lag the window behind the real data, meaning that the jamming prediction occurs after the vehicle reaches its actual location. A large window size are not suitable for jamming detection. This process generated a total of 2846 labelled samples, used for both supervised and unsupervised learning models.

The dataset was annotated based on known time intervals of jamming, yielding a binary classification task:

- Label 0 – Normal: Signal windows without any known jamming interference.
- Label 1 – Jammed: Signal windows overlapping with confirmed jamming events.

From each window, a set of statistical features was extracted per frequency band. These include the mean, minimum, maximum, and range, which collectively capture both signal amplitude and variation trends over time. The resulting feature space is multidimensional, reflecting the behavior of the AGC across each of the four frequency bands independently. This allows the models to leverage frequency-specific signal behavior in order to better detect anomalies.

Table 4: Dataset Characteristics

Property	**XGBoost**	**Isolation Forest**
Total number of samples	2846	2846
Number of Training Samples	80% of total samples	Normal data
Number of testing samples	20% of total samples	All data
Sampling Frequency	8 Hz	8 Hz
Duration of the dataset	15 min 52 sec	15 min 52 sec
Window size	2	2
Step size	1 (50% overlap)	1 (50% overlap)
Feature extracted per window	Mean, Min, Max, Range	Mean, Min, Max, Range
Total features per sample	16 (4 x 4)	16 (4 x 4)
Label for Training	Yes	No

4.2 Performance Evaluation

The detailed assessment of both models, which are trained for jamming detection in GNSS, is discussed in this section. Performance was tested out using a combination of classification evaluation metrics, including accuracy, precision, recall, F1-score, and confusion matrices, along with visual checks of predicted vs. actual labels for Isolation Forest. Additionally, 3-fold cross-validation was also applied for the supervised model to evaluate model robustness.

4.2.1 Supervised Model (XGBoost)

The XGBoost model was trained using labelled AGC features extracted as detailed in Section 3.4. The dataset was split into 80% training and 20% test subsets. In addition, 3-fold cross-validation was done during training to ensure model stability and reduce the risk of overfitting.

The confusion matrix for the XGBoost model is given in the **Table 5**.

Table 5: The Confusion matrix for the XGBoost Model.

	Predicted Normal	**Predicted Jammed**
Actual Normal	514	1
Actual Jammed	1	54

The classifier achieved an overall accuracy of **99.65%,** correctly identifying most instances of both normal and jammed conditions.

Table 6: Classification Metrics for XGBoost Model.

Class	**Precision**	**Recall**	**F1-Score**
Normal (0)	1.00	1.00	1.00
Jammed (1)	0.98	0.98	0.98

Moreover, the mean cross-validation score is **98.21%**, which indicates that the model is robust for overfitting.

Interpretation

- High Recall (0.98): The model successfully detects 94% of actual jamming events, which is crucial for maintaining GNSS navigation security.
- High Precision (1.00): Few normal signals are mistakenly classified as jamming, indicating a low false positive rate.
- Strong F1-Score (0.98): Shows a well-balanced trade-off between precision and recall for the jammed class.
- Robust Performance: Despite class imbalance, the model performs well on both classes, with particularly strong generalization to the minority (jammed) class.

4.2.2 Unsupervised Model (Isolation Forest)

For the unsupervised scenario, the Isolation Forest model was trained using only normal-labelled samples, in a real-world anomaly detection application where jamming patterns are unknown at training time. labelled samples were used for evaluating the model, not for training purposes.

Data Handling Strategy:

- Only normal data samples were used for training, as the model needs to detect outliers.
- Jammed windows were added in the test set to evaluate anomaly detection performance.
- Feature standardization (with StandardScaler) and data augmentation (jittering and scaling) were employed to introduce robustness.

The confusion matrix and Classification matrix for the Isolation Forest model are given in the **Table 7** and **Table 8** respectively.

Table 7: The Confusion matrix for the Isolation Forest Model.

	Predicted Normal	**Predicted Jammed**
Actual Normal	2548	24
Actual Jammed	9	265

Table 8: Classification Metrics for Isolation Forest Model.

Class	**Precision**	**Recall**	**F1-Score**
Normal (0)	1.00	0.99	0.99
Jammed (1)	0.92	0.94	0.94

Although they were trained on unlabelled jamming images, Isolation Forest accurately detected unusual patterns of AGC behavior that overlapped with well-known periods of jamming. The relatively good recall indicates good sensitivity but at the cost of some false positives (true, regular samples incorrectly identified as anomalies)—a trade-off to be expected in unsupervised anomaly detection. The contamination value needs to be selected carefully to get better performance.

Visual Investigation of IF Results

The visual representation of the IF model predictions and the positioning data during the jamming period are shown in **Figure 12**. The topmost plot shows the AGC data with predicted jamming points (red ‘x’), and the jamming windows based on the model predictions are indicated by shaded time intervals. The other plots correspond to positioning data, including latitude, longitude, height, quality factor, number of satellites, and velocity. The results highlight that the shaded period is bigger than the period in which the positioning data is lost. However, the model has captured the sudden variations of height, number of satellites, and velocity.

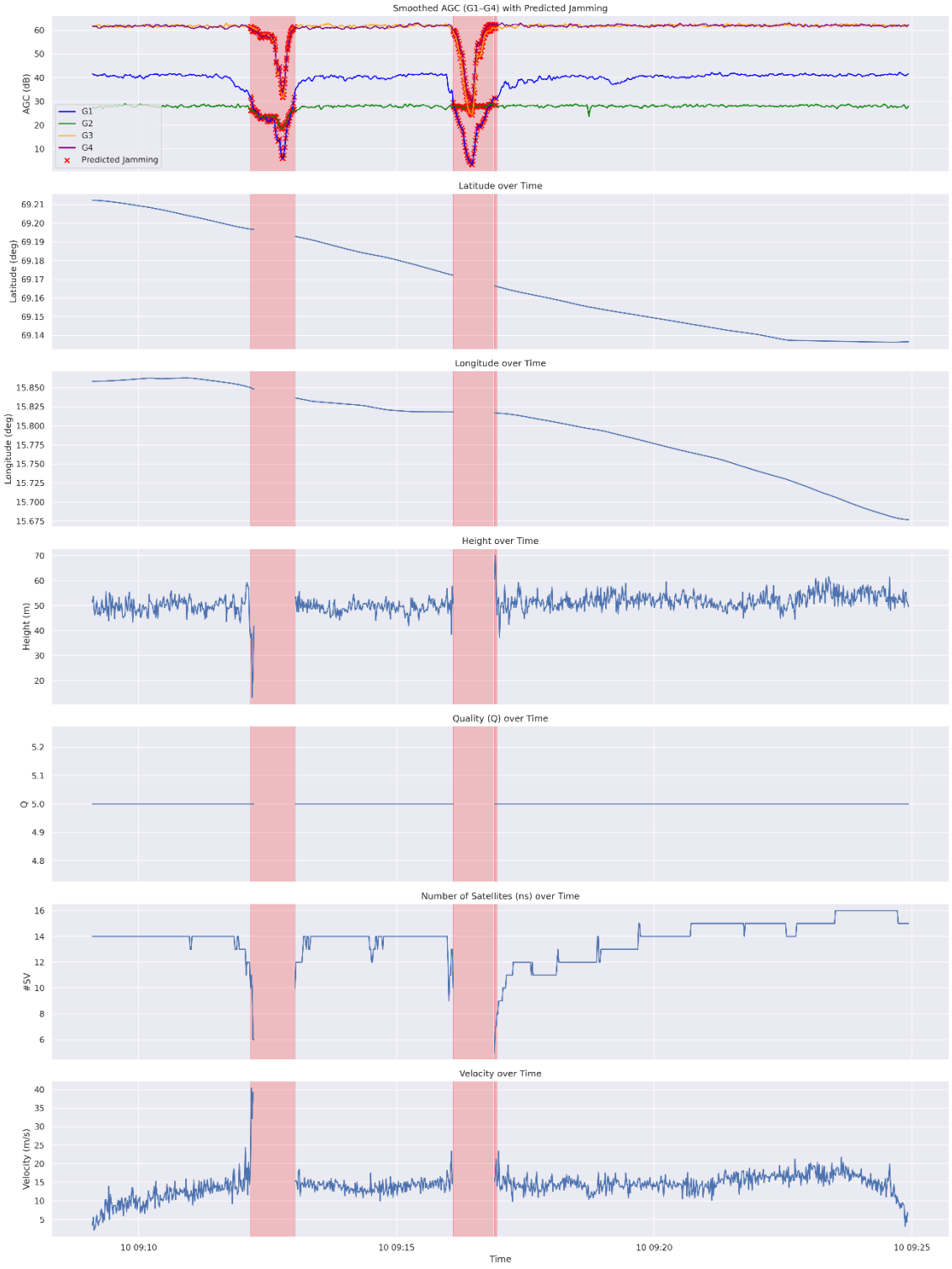

Figure 12: Visualization of IF Model Predictions and GNSS Positioning Parameters During Detected Jamming Events.

4.3 Feature Importance for XGBoost Model

The supervised XGBoost classifier provides intrinsic feature importance scores, allowing us to identify which AGC-based features contribute the most to the classification task. The relative importance of each feature from different AGC signal bands (G1–G4) is shown in the bar chart of **Figure 13**.

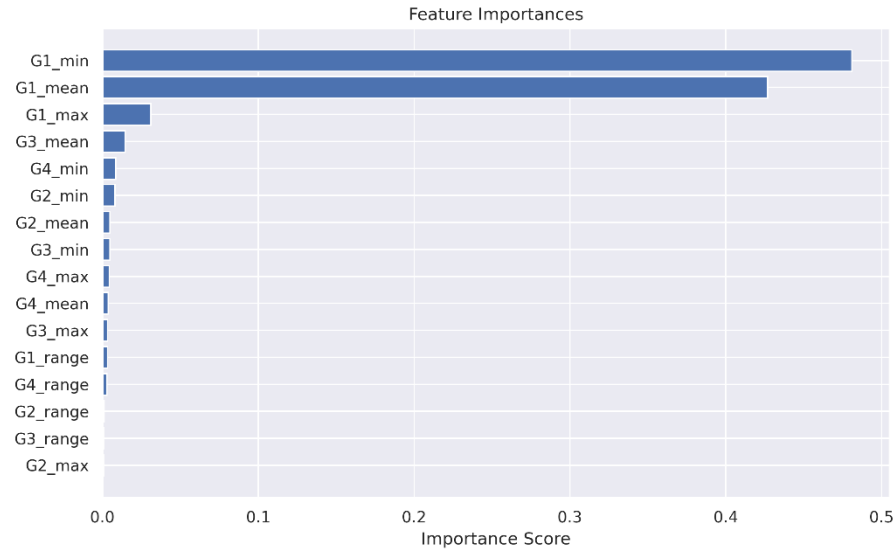

Figure 13: Feature importance plot from the trained XGBoost model.

Key Observations

- Dominant Features:

  The two most influential features were G1_min and G1_mean, contributing approximately 48% and 43%, respectively, to the model's decision-making process. This suggests that minimum and average AGC values from the G1 band are highly indicative of jamming events, likely due to G1's sensitivity to power disruptions.

- Moderate Importance:

  G1_max and G3_mean exhibited marginal importance, indicating that other bands contribute to the classification, albeit less significantly.

- Low-Impact Features:

  Most features derived from bands G2, G3, and G4—including range, max, and mean—had negligible importance scores. This implies that AGC anomalies caused by jamming predominantly manifest in the G1 band, which could relate to the receiver's frequency handling or antenna configuration.

Implications for Model Simplification

These results suggest that a dimensionality reduction approach may be viable without significant performance loss. For instance, feature engineering could prioritize G1 statistics in future iterations, reducing complexity and improving interpretability.

4.4 Summary

This chapter provided a comprehensive evaluation of machine learning models for GNSS jamming detection based on AGC signal features. The dataset of 2846 time-window samples labelled by a sliding window method was utilized as the basis for training and testing supervised and unsupervised models.

The XGBoost classifier under supervision worked extremely well with respect to prediction accuracy of 99.6%, precision of 0.98, recall of 0.98, and an F1-score of 0.98 for jamming detection. Analysis of feature importance revealed that G1_min and G1_mean statistics of AGC from the G1 frequency band were the most significant in performing the classification.

The Isolation Forest model (unsupervised) also distinguished well jamming conditions from normal conditions at a rate of accuracy of 98% and balanced the detection of anomalies when trained solely on normal data. The model has captured not only the position data loss period but also the sudden variation of some positioning data.

These findings verify the efficacy of using AGC-based features in jamming detection and certify both learning paradigms to function effectively in practical signal environments. The comparative examination of model performance and deployment implications are discussed in the next chapter.

5 Discussion

This chapter discusses the results obtained from both supervised and unsupervised models and key findings. It also includes the discussion of results over previous works and applicability of models.

Supervised and unsupervised machine learning models were developed for GNSS jamming detection using AGC data in this study. The supervised XGBoost model has achieved a high classification accuracy of 99.65% which indicates that the model has correctly classified nearly all samples. The precision and recall scores of 0.98 for the jammed class demonstrate the model's strong ability to accurately detect jamming conditions. The confusion matrix revealed only two misclassifications out of over 500 samples, showing strong reliability in differentiating between normal and jammed conditions. The model also demonstrated good generalization even with minority jamming samples, achieving a cross-validation mean accuracy of 98.21%, indicating robustness and minimal overfitting.

The unsupervised Isolation Forest model is trained with normal data, and it showed 98% accuracy with the complete test set. Despite not having seen jamming examples during training, it achieved a recall of 0.94 and a precision of 0.92, effectively identifying abnormal patterns. However, the visual comparison of predictions of IF with the positioning data demonstrated stimulating result; the model has captured not only the data absence period but also the data degradation intervals. Therefore, the reason behind false predictions of this unsupervised model can be a problem with the labelling algorithm.

Feature importance analysis from the XGBoost model revealed that G1_min and G1_mean were the most influential features, which contribute over 90% of the model's predictive power. This suggests that the G1 frequency band is most sensitive to jamming effects and can be prioritized in future models for better performance and efficiency.

With the above result, the supervised learning method, XGBoost, is highly effective in controlled environments where explicit ground truth is available. The model performs well in real-time jamming detection scenarios where historical patterns of normal and jammed signals can be used to train reliable classifiers. The model is suitable for applications such as transportation systems where the performance tracking and data labelling are feasible.

The unsupervised model, IF, is well-suited for situations where the absence or unreliability of ground truth is present. Further, it is applicable for early jamming detection purposes. This model can be highly recommended for real-time applications, such as autonomous driving, for early warning of jamming. However, the IF model can be unreliable in high-noisy environments because it may lead to false predictions.

Authors, Ghanbarzadeh et al., (2025) have carried out a comprehensive analysis of GNSS jamming detection and classification using machine learning methods. They achieved an accuracy of 98.93% with the ResNet18 model using transfer learning, while the XGBoost model developed in this study achieved 99.65% accuracy. Furthermore, they have utilized various signal parameters to train the model, whereas my research focuses solely on AGC data. Moreover, the model has been improved by 0.45% in accuracy compared to the detection method developed by Z. Li et al., (2025).

Y. Huang et al., (2023) have developed an early GNSS jamming method using a non-GNSS signal channel by keeping AGC at a fixed gain value. They calibrated a threshold in the non-jamming environment, and as the parameter increases, the threshold enables the model to provide early warning. However, the proposed isolation forest model has the capability of early jamming detection without requiring a threshold calibration and with variation in AGC values. Moreover, this fixed threshold has been calibrated under a specific GNSS frequency band, and the IF model can handle all GNSS frequency bands.

An entropy-based GNSS jamming detection method is carried out by Sakorn & Supnithi, (2021b) using AGC and C/N0 data. The method is tested under specific conditions and

only for the L1 frequency band. The threshold has been defined at 100 m distance and needs prior labelling to identify jamming. However, this threshold can be varied with jammers, and the proposed IF model in this study can dynamically identify jamming, thereby detecting signal degradation. Furthermore, the IF model can handle multiple GNSS frequency bands without prior labelling when compared to previous work. Moreover, the XGBoost model also performed well without a complex analysis than this entropy-based method.

6 Conclusions and Future Works

This thesis presents supervised and unsupervised machine learning models for GNSS jamming detection, based on the characteristics of the AGC signal. In conclusion, both models exhibit high performance values and can effectively handle multidimensional features. The cross-validation method has proven that the XGBoost model is robust against overfitting. Furthermore, it can be stated that the reason for the false predictions of the IF model may be an issue with the labelling algorithm, as it is evident that the model has also captured the signal degradation period as jamming. Moreover, AGC data collected from consumer-grade GNSS receivers can be effectively used for jamming detection as a standalone parameter.

Future work directions include advancing the labelling algorithm to provide a reliable ground truth for supervised model training. Another possible approach is the development of hybrid learning systems that incorporate both supervised and unsupervised learning, enabling them to identify both labelled and unlabeled scenarios. Future studies can be expanded by incorporating additional measurements, such as SNR, frequency spectrum, C/N0, as well as pseudorange residuals, in addition to AGC data, to enhance performance further. The models can be improved in detecting other intentional RFIs, including spoofing and meaconing. Finally, deploying light-weight versions of these models on embedded GNSS receivers to perform real-time processing.

References

Aggrey, J., Bisnath, S., Naciri, N., Shinghal, G., & Yang, S. (2020). Multi-GNSS precise point positioning with next-generation smartphone measurements. *Journal of Spatial Science*, *65*(1). https://doi.org/10.1080/14498596.2019.1664944

Borhani-Darian, P., Li, H., Wu, P., & Closas, P. (2024). Detecting GNSS spoofing using deep learning. *Eurasip Journal on Advances in Signal Processing*, *2024*(1), 1–19. https://doi.org/10.1186/S13634-023-01103-1/FIGURES/9

Broumandan, A., & Lachapelle, G. (2018). Spoofing Detection Using GNSS/INS/Odometer Coupling for Vehicular Navigation. *Sensors 2018, Vol. 18, Page 1305*, *18*(5), 1305. https://doi.org/10.3390/S18051305

Caputo, G. (n.d.). *AI-Based GNSS Jamming and Spoofing Detection and Classification*.

Chen, B., Gao, C., Liu, Y., & Sun, P. (2019). Real-time Precise Point Positioning with a Xiaomi MI 8 Android Smartphone. *Sensors 2019, Vol. 19, Page 2835*, *19*(12), 2835. https://doi.org/10.3390/S19122835

Dabove, P., & Di Pietra, V. (2019). Single-Baseline RTK Positioning Using Dual-Frequency GNSS Receivers Inside Smartphones. *Sensors 2019, Vol. 19, Page 4302*, *19*(19), 4302. https://doi.org/10.3390/S19194302

Dovis, Fabio. (2015). *GNSS interference threats and countermeasures*. 217. https://books.google.com/books/about/GNSS_Interference_Threats_and_Counterme a.html?id=XIcTBwAAQBAJ

Elghamrawy, H., Karaim, M., Korenberg, M., & Noureldin, A. (2022). High-Resolution Spectral Estimation for Continuous Wave Jamming Mitigation of GNSS Signals in Autonomous Vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *23*(7), 7881–7895. https://doi.org/10.1109/TITS.2021.3074102

Elghamrawy, H., Karaim, M., Tamazin, M., & Noureldin, A. (2020). Experimental Evaluation of the Impact of Different Types of Jamming Signals on Commercial GNSS Receivers. *Applied Sciences 2020, Vol. 10, Page 4240*, *10*(12), 4240. https://doi.org/10.3390/APP10124240

Elghamrawy, H., & Noureldin, A. (2023). Narrowband Jamming Mitigation Based on Multi-Resolution Analysis for Land Vehicles. *IEEE Transactions on Intelligent Vehicles*, *8*(4), 3083–3095. https://doi.org/10.1109/TIV.2021.3134494

Ferre, R. M., Fuente, A. D. La, & Lohan, E. S. (2019). Jammer Classification in GNSS Bands Via Machine Learning Algorithms. *Sensors 2019, Vol. 19, Page 4841*, *19*(22), 4841. https://doi.org/10.3390/S19224841

Ghanbarzadeh, A., Soleimani, M., & Soleimani, H. (2025). *GNSS/GPS Spoofing and Jamming Identification Using Machine Learning and Deep Learning*. https://github.com/alicmu2024/GNSS-Jamming-Detection-

Hu, J., Yi, D., & Bisnath, S. (2023). A Comprehensive Analysis of Smartphone GNSS Range Errors in Realistic Environments. *Sensors 2023, Vol. 23, Page 1631*, *23*(3), 1631. https://doi.org/10.3390/S23031631

Huang, G., Wang, D., Du, Y., Zhang, Q., Bai, Z., & Wang, C. (2022). Deformation Feature Extraction for GNSS Landslide Monitoring Series Based on Robust Adaptive Sliding-Window Algorithm. *Frontiers in Earth Science*, *10*, 884500. https://doi.org/10.3389/FEART.2022.884500/BIBTEX

Huang, Y., Xu, R., Weng, D., & Chen, W. (2023). Early Detection of GNSS jamming Interference Based on Statistical Test in Receiver Non-satellite Channel. *Proceedings - 2023 7th International Symposium on Computer Science and Intelligent Control, ISCSIC 2023*, 151–154. https://doi.org/10.1109/ISCSIC60498.2023.00040

Kaplan, E. D. ., & Hegarty, C. . (2017). *Understanding GPS/GNSS : principles and applications*. 993.

Kreuzer, D., & Munz, M. (2021). Deep Convolutional and LSTM Networks on Multi-Channel Time Series Data for Gait Phase Recognition. *Sensors 2021, Vol. 21, Page 789*, *21*(3), 789. https://doi.org/10.3390/S21030789

Lachapelle, G., Gratton, P., Horrelt, J., Lemieux, E., & Broumandan, A. (2018). Evaluation of a Low Cost Hand Held Unit with GNSS Raw Data Capability and Comparison with an Android Smartphone. *Sensors 2018, Vol. 18, Page 4185*, *18*(12), 4185. https://doi.org/10.3390/S18124185

Li, G., & Geng, J. (2019). Characteristics of raw multi-GNSS measurement error from Google Android smart devices. *GPS Solutions*, *23*(3). https://doi.org/10.1007/s10291-019-0885-4

Li, Z., Wang, L., Wang, N., Li, R., & Liu, A. (2022). Real-time GNSS precise point positioning with smartphones for vehicle navigation. *Satellite Navigation*, *3*(1), 1–22. https://doi.org/10.1186/S43020-022-00079-X/TABLES/7

Li, Z., Zheng, L., Zhang, Q., Wang, H., Du, Z., & Liu, J. (2025). GNSS Jamming Attacks Recognition Based on Dual GCN with Adaptive Weight Learning. *IEEE Sensors Journal*. https://doi.org/10.1109/JSEN.2025.3571189

Liu, C., Ren, B., Xie, Y., & Chen, F. (2025). Deep learning-based GNSS composite jamming detection and recognition technology. *Frontiers in Signal Processing*, *5*, 1567926. https://doi.org/10.3389/FRSIP.2025.1567926/BIBTEX

Liu, W., Shi, X., Zhu, F., Tao, X., & Wang, F. (2019). Quality analysis of multi-GNSS raw observations and a velocity-aided positioning approach based on smartphones. *Advances in Space Research*, *63*(8), 2358–2377. https://doi.org/10.1016/J.ASR.2019.01.004

Mehr, I. E., & Dovis, F. (2025). A Deep Neural Network Approach for Classification of GNSS Interference and Jamming. *IEEE Transactions on Aerospace and Electronic Systems*, *61*(2), 1660–1676. https://doi.org/10.1109/TAES.2024.3462662

Odolinski, R., Teunissen, P. J. G., & Zhang, B. (2020). Multi-GNSS processing, positioning and applications. *Journal of Spatial Science*, *65*(1), 3–5. https://doi.org/10.1080/14498596.2020.1687170

OpenAI. (2025). *ChatGPT* (April 2 version) [Large language model]. https://chat.openai.com/chat

Paziewski, J., Sieradzki, R., & Baryla, R. (2019). Signal characterization and assessment of code GNSS positioning with low-power consumption smartphones. *GPS Solutions*, *23*(4), 1–12. https://doi.org/10.1007/S10291-019-0892-5/TABLES/2

Previous jammertests. (n.d.). Retrieved May 28, 2025, from https://jammertest.no/previous-jammertests/

Qin, W., & Dovis, F. (2022). Situational Awareness of Chirp Jamming Threats to GNSS Based on Supervised Machine Learning. *IEEE Transactions on Aerospace and Electronic Systems*, *58*(3), 1707–1720. https://doi.org/10.1109/TAES.2021.3135014

Radoš, K., Brkić, M., & Begušić, D. (2024). Recent Advances on Jamming and Spoofing Detection in GNSS. In *Sensors* (Vol. 24, Issue 13). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/s24134210

Realini, E., Caldera, S., Pertusini, L., & Sampietro, D. (2017). Precise GNSS Positioning Using Smart Devices. *Sensors 2017, Vol. 17, Page 2434*, *17*(10), 2434. https://doi.org/10.3390/S17102434

Reda, A., Mekkawy, T., Tsiftsis, T. A., & Mahran, A. (2024). Deep Learning Approach for GNSS Jamming Detection Based PCA and Bayesian Optimization Feature Selection Algorithm. *IEEE Transactions on Aerospace and Electronic Systems*. https://doi.org/10.1109/TAES.2024.3429049

Robustelli, U., Baiocchi, V., & Pugliano, G. (2019). Assessment of Dual Frequency GNSS Observations from a Xiaomi Mi 8 Android Smartphone and Positioning Performance Analysis. *Electronics 2019, Vol. 8, Page 91*, *8*(1), 91. https://doi.org/10.3390/ELECTRONICS8010091

Sakorn, C., & Supnithi, P. (2021a). Calculating AGC and C/N0 thresholds of mobile for jamming detection. *ECTI-CON 2021 - 2021 18th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology: Smart Electrical System and Technology, Proceedings*, 268–271. https://doi.org/10.1109/ECTI-CON51831.2021.9454850

Sakorn, C., & Supnithi, P. (2021b). Calculating AGC and C/N0 thresholds of mobile for jamming detection. *ECTI-CON 2021 - 2021 18th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology: Smart Electrical System and Technology, Proceedings*, 268–271. https://doi.org/10.1109/ECTI-CON51831.2021.9454850

Samalla, K., & Naveen Kumar, & P. (2024). *Global Navigation Satellite System in the Civil Surveillance*. *4*(1). https://doi.org/10.34293/acsjse.v4i1.100

Siemuri, A., Selvan, K., Kuusniemi, H., Valisuo, P., & Elmusrati, M. S. (2022). A Systematic Review of Machine Learning Techniques for GNSS Use Cases. In *IEEE Transactions on Aerospace and Electronic Systems* (Vol. 58, Issue 6). https://doi.org/10.1109/TAES.2022.3219366

Spanghero, M., Geib, F., Panier, R., & Papadimitratos, P. (2025). GNSS jammer localization and identification with airborne commercial GNSS receivers. *IEEE Transactions on Information Forensics and Security*. https://doi.org/10.1109/TIFS.2025.3550050

Specht, M., Specht, C., Wilk, A., Koc, W., Smolarek, L., Czaplewski, K., Karwowski, K., Dąbrowski, P. S., Skibicki, J., Chrostowski, P., Szmagliński, J., Grulkowski, S., & Judek, S. (2020). Testing the Positioning Accuracy of GNSS Solutions during the Tramway Track Mobile Satellite Measurements in Diverse Urban Signal Reception Conditions. *Energies 2020, Vol. 13, Page 3646*, *13*(14), 3646. https://doi.org/10.3390/EN13143646

Spens, N., Lee, D.-K., Nedelkov, F., & Akos, D. (2022). *Detecting GNSS Jamming and Spoofing on Android Devices*. https://doi.org/10.33012/navi.537

Sun, K., Yu, B., Elhajj, M., Ochieng, W. Y., Zhang, T., & Yang, J. (2021). A Novel GNSS Interference Detection Method Based on Smoothed Pseudo-Wigner–Hough Transform. *Sensors 2021, Vol. 21, Page 4306*, *21*(13), 4306. https://doi.org/10.3390/S21134306

Sun, K., Zhang, M., & Yang, D. (2016). A New Interference Detection Method Based on Joint Hybrid Time-Frequency Distribution for GNSS Receivers. *IEEE Transactions on Vehicular Technology*, *65*(11), 9057–9071. https://doi.org/10.1109/TVT.2016.2515718

Szot, T., Specht, C., Specht, M., & Dabrowski, P. S. (2019). Comparative analysis of positioning accuracy of Samsung Galaxy smartphones in stationary measurements. *PLOS ONE*, *14*(4), e0215562. https://doi.org/10.1371/JOURNAL.PONE.0215562

Test Catalogue. (2024).

Viana, J., Farkhari, H., Campos, L. M., Sebastiao, P., Cercas, F., Bernardo, L., & Dinis, R. (2022). Two methods for Jamming Identification in UAV Networks using New

Synthetic Dataset. *IEEE Vehicular Technology Conference*, *2022-June*. https://doi.org/10.1109/VTC2022-SPRING54318.2022.9860816

Wen, Q., Geng, J., Li, G., & Guo, J. (2020). Precise point positioning with ambiguity resolution using an external survey-grade antenna enhanced dual-frequency android GNSS data. *Measurement*, *157*, 107634. https://doi.org/10.1016/J.MEASUREMENT.2020.107634

Wu, Q., Sun, M., Zhou, C., & Zhang, P. (2019). Precise Point Positioning Using Dual-Frequency GNSS Observations on Smartphone. *Sensors 2019, Vol. 19, Page 2189*, *19*(9), 2189. https://doi.org/10.3390/S19092189

Yi, D., Yang, S., & Bisnath, S. (2022). Native Smartphone Single- and Dual-Frequency GNSS-PPP/IMU Solution in Real-World Driving Scenarios. *Remote Sensing 2022, Vol. 14, Page 3286*, *14*(14), 3286. https://doi.org/10.3390/RS14143286

Zangenehnejad, F., & Gao, Y. (2021). GNSS smartphones positioning: advances, challenges, opportunities, and future perspectives. *Satellite Navigation*, *2*(1), 1–23. https://doi.org/10.1186/S43020-021-00054-Y/TABLES/5

Zhou, W., Lv, Z., Li, G., Jiao, B., & Wu, W. (2024). Detection of Spoofing Attacks on Global Navigation Satellite Systems Using Kolmogorov-Smirnov Test-Based Signal Quality Monitoring Method. *IEEE Sensors Journal*, *24*(7), 10474–10490. https://doi.org/10.1109/JSEN.2024.3354110

Appendices

Appendix A. GNSS Systems Overview with Signal Notation and Frequency

Table 9: GNSS Systems Overview with Signal Notation and Frequency (Test Catalogue, 2024).

GNSS System	Signal Notation	Signal Frequency (MHz)
GPS	L1 C/A	1575.42
	L1C	1575.42
	L2 C	1227.6
	L2 P	1227.6
	L5	1176.45
GLONASS	L1 C/A	1598.0625 – 1609.3125
	L2 C	1242.9375 – 1251.6875
	L2 P	1242.9375 – 1251.6875
	L3 OC	1202.025
Galileo	E1	1575.42
	E5a	1176.45
	E5b	1207.14
	E5 AltBOC	1191.795
	E6	1561.098
BeiDou	B1I	1561.098
	B2I	1207.14
	B3I	1268.52
	B1C	1575.42
	B2a	1176.45
	B2b	1207.14
NAVIC	L5	1176.45
SBAS	L1	1575.42
	L5	1176.45
QZSS	L1 C/A	1575.42
	L1 C	1575.42
	L1S	1575.42
	L2C	1227.6
	L5	1176.45
	L6	1278.75