COASTLINE COLLEGE

STORM Research Project

Machine Learning-Based Detection of GPS Spoofing in Autonomous Vehicles: Enhancing Navigation Security Through Deep Learning Models

Brian Stauffer

Abstract— Global Navigation Satellite Systems (GNSS), especially the Global Positioning System (GPS), are vital for the safe operation and navigation of autonomous vehicles (AVs). However, civilian GPS signals lack encryption and authentication, making them vulnerable to spoofing attacks that can deceive vehicles and create serious safety and security situations. This study examines the application of machine learning (ML) and deep learning models to detect GPS spoofing in AVs. We evaluate Long Short-Term Memory (LSTM) networks, Convolutional Neural Networks (CNNs), and Transformer-based architectures for their ability to identify anomalous signal features, such as irregular signal strength, Doppler shifts, and timing inconsistencies. Comparative analysis shows that LSTMs are effective in capturing sequential dependencies, CNNs excel in spatial feature extraction, and Transformers handle long-range interactions well, with hybrid models delivering superior performance across varying conditions. Results from recent studies indicate detection accuracies between 95% and 99%, highlighting the potential for integrating ML-based detection into AV navigation systems. Despite inherent challenges, such as limited real-world spoofing data, high computational requirements, and the need for adaptive retraining, ML-based detection remains the most promising approach for securing GPS-dependent systems against malicious attacks. This research concludes that hybrid deep learning models, combined with emerging technologies like Edge AI and quantum-enhanced processing, can greatly enhance AV navigation security against GPS spoofing threats.

Index Terms— GPS spoofing detection, autonomous vehicles (AVs), machine learning (ML), deep learning models (LSTM, CNN, Transformer), navigation security.

I. Introduction

On December 05, 2011, a significant event occurred, escalating the need for Global Navigation Satellite System (GNSS) signal integrity and security. Iran's military cyberwarfare unit brought down a U.S. hi-tech stealth military drone surveilling Iran's nuclear buildup capability. This was allegedly achieved by electronically hijacking, GPS spoofing, the drone (bbc.com, 2011). In an article published shortly after the incident by the Christian Science Monitor, an interview with an Iranian engineer working on the captured drone stated that this

electronic hijacking was accomplished by transmitting false GPS signal elevation coordinates, making the drone believe it was at a higher altitude than it was, along with false latitude/longitude coordinates. This caused the drone to change course, forcing it to descend until it eventually crash-landed in Iranian territory. The U.S. military denied this account and attributed the drone's grounding to a guidance system malfunction (Peterson and Faramarzi, 2011). Nonetheless, the geopolitical fallout from this incident was significant. Then Secretary of Defense Leon Panetta told Fox News, "the stakes are higher for such surveillance, now that Iran can apparently disrupt the work of U.S. drones".

The fallout from this incident, including the discord among U.S. government officials, further highlights the need to secure critical operations systems, especially GNSS. Moreover, emphasizing the vulnerabilities of GPS technology was crucial to advocating for increased GPS security worldwide in all applications relying on precise GPS signals. GPS spoofing is the intentional manipulation of GPS signals, resulting in the broadcast of false GPS signals to a receiver (Ghanbarzade and Soleimani, 2025). Specifically, spoofing occurs when RF waveforms mimic true signals in some ways but deny, degrade, disrupt, or deceive a receiver's operation when processed (U.S. DHS, 2017). The onset of these effects can be either immediate or delayed, and it is possible for these effects to persist even after the spoofing has ended (U.S. DHS, 2017). In autonomous vehicles (AVs) this can cause navigation failures and system disorientation, creating potentially dangerous conditions for passengers.

The increasing reliance on GNSS, especially GPS, highlights the urgent need to protect these technologies against hostile threats such as spoofing and jamming (Ghanbarzade and Soleimani, 2025). Civilian GPS signals are unencrypted and lack authentication features, making them prone to spoofing and hijacking (Abrar et al., 2024). Differentiating authentic signals from spoofed ones is crucial for maintaining system integrity. A standard metric for spoofed signal detection is measuring signal strength, expressed as C/N_0 (carrier-to-noise density ratio). Spoofed signals are generally stronger and more uniform than authentic signals since they are transmitted from a nearby ground source rather than satellites in space. This creates an anomalous power profile that detection algorithms can identify and flag. It is commonly stated that interference or jamming with received power 24 dB greater than the received power in authentic signals can disrupt operation of a C/A signal receiver (U.S. DHS, 2017). Using blocking antennas and redundant antennas can help reduce spoofing threats (U.S. DHS, 2017). Recent advancements in machine learning and deep learning offer promising opportunities for improving detection and mitigation strategies against these threats. (Ghanbarzade and Soleimani, 2025).

As more self-driving AV services, such as Waymo and Cruise, are introduced into large metropolitan areas, the potential for cyberattacks, especially remote takeovers, on these vehicles will increase due to their reliance on GPS, which inherently has weak signal security (Ghanbarzade and Soleimani, 2025). Threat actors will target these vehicles and their operators for ransomware attacks. This threat will become even more significant during major events like the upcoming 2028 Olympics in Los Angeles, California. Therefore, it is crucial to develop and implement advanced GPS spoofing detection strategies to ensure the high reliability and security of AV navigation.

A. Importance of Autonomous Vehicles in U.S. Critical Infrastructure

Autonomous ride-hailing services are just one area that relies on the deployment of AVs which can be susceptible to GPS spoofing attacks. Other applications include autonomous buses for public transit, autonomous heavy machinery for construction and mining, UAVs and autonomous combat vehicles for military and defense, automated forklifts and transport vehicles in manufacturing and warehousing, and autonomous aircraft and ships in aerospace and maritime operations. These areas of critical U.S. national infrastructure all have security implications regarding GPS signal security (U.S. DHS, 2022).

Table 1-1 maps AV applications across various industries to their relevant NIST (National Institute of Standards and Technology) Critical Infrastructure sectors. It demonstrates how AV technologies intersect with critical U.S. infrastructure domains, highlighting the cybersecurity and operational significance of AV deployments.

Table 1-1. AV Applications Mapped to NIST Critical Infrastructure Sectors

Industry	AV Applications/Usage	NIST Critical Infrastructure Sector Relationship
Transportation & Logistics	Self-driving trucks	Transportation Systems- Secure mobility & logistics
Ride-sharing & Mobility	Autonomous taxis & shuttles	Transportation Systems- Urban transit integration
Public Transit	Autonomous buses, harvesters	Food & Agriculture – Ensuring secure food production
Construction & Mining	Autonomous heavy machinery	Critical Manufacturing – Protecting Industrial Processes
Healthcare	Autonomous ambulances and medical delivery services	Healthcare & Public Health – Securing emergency response
Military & Defense	UAVs, autonomous combat vehicles	Defense Industrial Base – Securing strategic ops
Retail & Delivery	Autonomous delivery vehicles	Transportation Systems/Commercial – Secure supply chain
Manufacturing & Warehousing	Automated forklifts, transport vehicles	Critical manufacturing – Secure production and inventory
Aerospace & Maritime	Autonomous aircraft & ships	Transportation Systems – Secure navigation & transport

II. Research Methodology

A. Data Collection

This research employed a structured approach to gather information relevant to GPS spoofing detection and ML-based security methods for AVs. Publications and data were collected from a combination of academic databases, government publications, and open-source datasets. Searches were conducted using the UCLA Catalog Library Database, Google Scholar, Semantic Scholar, IEEE Xplore, and arXiv, as well as government and defense websites that publish technical reports on GNSS and GPS security. Data assets were supplemented by queries using AI-based research tools such as Gemini, Copilot, and ChatGPT. Prompts were focused on identifying

recent scholarly and technical publications related to GPS spoofing detection, autonomous vehicle security, machine learning models for spoofing detection, and the application of machine learning to AV security.

B. Sources

The primary sources for this study include peer-reviewed journal articles from engineering, computer science, and cybersecurity disciplines, thesis and dissertation research related to GPS vulnerabilities and ML-based spoofing detection. Additional sources used were government and military technical reports regarding GPS security, spoofing threats, and mitigation strategies, as well as open-source datasets relevant for training and testing machine learning models, along with industry reports and news articles documenting spoofing incidents and their impact on autonomous systems.

C. Time Frame

The primary reference window includes the years 2003–2025 to include the latest research in machine learning and GPS spoofing detection. Earlier publications, such as government standards, technical frameworks, and news reports, are also included if they are historically significant to GPS security.

D. Research Artifacts

The collected artifacts include technical publications, experimental datasets, and case studies that evaluate ML algorithms such as Long Short-Term Memory (LSTM) networks, Convolutional Neural Networks (CNNs), and Transformer models. These artifacts are used to compare the detection accuracy, adaptability, and limitations of each model in mitigating GPS spoofing threats in AVs.

III. Research Objectives

As global adversaries continue to adopt asymmetric warfare tactics across the battlefield, threat actors are also using these tactics as non-kinetic attack vectors. The results can be equally devastating. Large-scale attacks can significantly disrupt commercial travel, communications, military ops, and financial transactions (Isleyen, et al., 2024). Large mass transit fleets can be disabled and held for ransom. ML-based detection techniques are currently the most promising way to effectively prevent, detect, and disrupt adversarial GPS spoofing.

The key objectives of this research paper are to examine vulnerabilities in AV GPS systems and explore how machine learning (ML) can help identify these vulnerabilities, thus reducing risk and enhancing navigation safety in AVs. ML can analyze large datasets, detect anomalous patterns, and adapt to dynamic GPS spoofing techniques. This paper will focus on ML training models to detect anomalous GPS signal patterns, specifically deep learning algorithms, such as LSTM networks, CNNs, and Transformers. Other important anti-spoofing detection strategies include Sensor Fusion, Autonomous Navigation Adjustment, Positioning Algorithms (Shabbir, et al., 2023), Car-To-Everything Communication (C-V2X), and IoV (Internet of Vehicles) (Hakeem, et

al., 2025). This study will present a cogent evaluation and analysis of the current detection strategies for AV GPS anti-spoofing capabilities, available technology, and industry best practices.

Can ML-based detection techniques identify GPS spoofing attacks in AVs with a high degree of accuracy ($Pd \geq 95\%$ at $Pfa \leq 1\%$) to ensure safe navigation and operation? Researchers are currently exploring the extent to which ML can prevent threat actors from remotely disrupting or disabling AVs by interfering with onboard GPS systems. This study examines whether ML detection techniques can reliably identify GPS spoofing attacks in AVs with sufficient accuracy to ensure safe navigation and operation. This paper evaluates the current literature and presents a comparative analysis of deep learning architectures to assess their effectiveness and define requirements for practical AV deployment. The findings of this study will enhance AV navigation security by evaluating the most effective ML–based GPS spoofing detection models. Specifically, the results will guide AV navigation security engineering, inform dataset and benchmark design for GPS spoofing research, and specify practical deployment requirements such as model retraining and architecture selection. This study contributes to both academic development and critical infrastructure protection.

IV. Comparative Analysis of Models

A. Long Short-Term Memory (LSTM)

Machine learning can analyze large data sets, detect anomalous patterns, and adapt to dynamic GPS spoofing techniques (Isleyen and Bahtiyar, 2024). LSTM is a type of recurrent neural network (RNN) designed for analyzing sequential data. It is highly accurate in detecting signal inconsistencies by learning normal signal behavior and flagging deviations (Filippou et al., 2023). Recent research has examined LSTM-based models for spoofing detection, such as the LSTM-Detect model, which assesses distortions in the autocorrelation function of GPS signals (Filippou et al., 2023). Another approach combines inertial navigation system (INS) data with LSTMs to compare expected motion patterns against spoofed GPS signals (Chen et al., 2025).

These methods have demonstrated high detection accuracy, with some achieving over 98.5% success rates (Filippou et al., 2023). Existing solutions for detecting GPS spoofing attacks can be categorized into signal processing and data-driven approaches (Filippou et al., 2023). LSTM-based detection techniques represent a significant advancement over traditional GPS spoofing detection methods by leveraging deep learning, real-time data integration, and adaptive thresholding to improve both detection accuracy and speed (Chen et al., 2025).

The LSTM-based anomaly detection method provides a more practical and adaptable solution by eliminating the need for labeled data and focusing on learning normal operational patterns, making it suitable for real-world applications where labeled attack data is not readily available (Filippou et al., 2023).

Figure 1-1. LSTM GPS Signal Processing for Spoofing Detection

- **Raw GPS Signal:** Includes timing, location, and signal metadata.
- **Preprocessing:** Filters and normalizes the signal for model input.
- **LSTM Layers:** Captures temporal dependencies and patterns over time**.**
- **Temporal Feature Extraction:** Detects anomalies in signal behavior.
- **Classification:** Flags the signal as either "Spoofed" or "Authentic" (OpenAI, 2025a).

B. Convolutional Neural Networks (CNN)

CNNs are a type of deep learning model designed for processing structured, grid-like data, such as images. The accuracy of data processed by CNNs can be tested utilizing non-line-of-sight (NLOS) receptions (Zhang et al., 2023). CNNs are used in GPS spoofing detection by analyzing spatial patterns in GPS signal data to identify anomalies that can indicate GPS spoofing attacks (Zhang et al., 2023). CNNs are employed to extract spatial features from the data, effectively distinguishing between authentic and spoofed signals (Shabbir et al., 2023). CNN study results highlight superior performance compared to previous research, demonstrating high accuracy (99%) in detecting spoofing attacks across different datasets (Ghanbarzade and Soleimani, 2025).

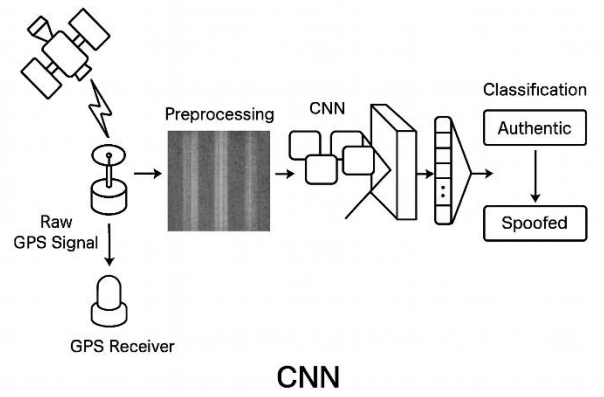

Figure 2-1. CNN GPS Signal Spoofing Detection

CNN Pipeline for GPS Signal Spoofing Detection

- **Input GPS Signal:** Raw satellite data including timestamps, signal strength, and location coordinates.
- **Preprocessing:** Normalization, noise filtering, and transformation into a format suitable for CNN input (e.g., spectrograms or time-series matrices).
- **Convolutional Layers:** Extract spatial and temporal patterns from the signal using filters.
- **Feature Extraction**: Identify anomalies or inconsistencies in signal behavior.
- **Classification:** Determine whether the signal is legitimate or spoofed.

- **Spoofing Detection Output:** Final decision- flagged as spoofed or authentic (OpenAI, 2025b).

C. Transformers

Transformers are a type of deep learning model designed to process sequential data efficiently. They are highly effective for tasks such as natural language processing (NLP), time series analysis, and geospatial data modeling (Niu et al., 2024). Transformers use attention weights to determine how much focus is given to each part of the input sequence when making predictions. For GPS spoofing detection, this means identifying which timestamps, satellite signals, or metadata points are most suspicious or informative. Transformers utilize these attention mechanisms via temporal focus, signal consistency checks, cross-satellite correlation, and contextual awareness to analyze GPS signals and determine whether the signal is spoofed or authentic (OpenAI, 2025c).

An authentic GPS signal sequence analyzed by LSTM can be represented, where $t_1 \ldots t_6$ denotes sequential data points, such as consecutive measurement intervals (e.g., every 1 second) containing GPS features such as carrier-to-noise density ratio (C/N_0), Doppler shift, or pseudo-range residuals. LSTM processes these time steps sequentially to detect anomalies that may indicate spoofing, as shown in the following signal sequence:

$[t_1, t_2, t_3, t_4, t_5, t_6]$

However, a spoofed signal might show a sudden jump at t_4. The resulting LSTM attention map, which indicates the model is heavily focusing on t_4 when analyzing t_6, suggests that t_4 contains anomalous behavior, an indication of spoofing:

Attention from $t_6 \rightarrow$ [0.1, 0.1, 0.2, **0.5**, 0.05, 0.05] (OpenAI, 2025c).

Transformer study results indicate over 95% detection accuracy under varying conditions, indicating its potential for improving navigation system security (Niu et al., 2024). Conclusive research data reiterates the Transformer model's effectiveness in spoofing detection and its potential for wide use in improving GPS security. It stresses the importance of balancing detection sensitivity and false alarm rates, suggesting future research and development directions (Niu et al., 2024).

V. Findings

This research investigates the vulnerabilities of GPS systems in AVs and explores how ML can enhance GPS signal spoofing detection to improve navigation safety and security. It employs literature reviews of deep ML models, including LSTM networks, CNNs, and Transformers, to identify anomalous GPS signal patterns. A comparative analysis shows that LSTMs detect signal inconsistencies with 98.5% accuracy, CNNs with 99%, and Transformers with over 95% accuracy. A detailed analysis of this data demonstrates that hybrid ML architectures combining sequential and spatial feature extraction achieve superior performance in GPS spoofing detection, offering

safer and more reliable AV operations. CNNs can be integrated with LSTMs for spatial-temporal analysis, while Transformers weigh GPS data points for anomaly detection.

Table 2-1 offers a detailed comparison of the three ML architectures: LSTM, CNN, and Transformer. Each model is assessed based on attributes such as accuracy, real-world applicability, parallelization capability, and hybrid integration potential.

Table 2-1. ML Model Comparison

Feature / Attribute	**LSTM (Long Short-Term Memory)**	**CNN (Convolutional Neural Network)**	**Transformer**
Type	Recurrent Neural Network (RNN)	Deep Learning model for spatial data	Attention-based deep learning model for sequential/spatial data
Primary Strength	Excellent at capturing temporal/sequential patterns	Strong at spatial feature extraction	Handles long-range dependencies via self-attention
Detection Accuracy	>98.5% in some studies	Up to 99% accuracy across datasets	Over 95% accuracy under varying conditions
Parallelization	Limited due to sequential nature	Highly parallelizable	Highly parallelizable
Best Use Case	Learning GPS signal time-series anomalies and comparing with INS data	Analyzing spatial patterns like signal distributions or NLOS detection	Modeling complex GPS data interactions and long-term dependencies
Weakness	Struggles with very long sequences and high parallelism	Not ideal for sequential dependencies	May require more training data and compute resources
Hybrid Potential	Can be enhanced with Transformer-style attention for better generalization	Can be fused with LSTM for spatial-temporal analysis	Ideal for hybrid models combining spatial and temporal features
Real-World Readiness	Suitable for real-time anomaly detection with no need for labeled attacks	Suitable for image-like signal patterns (e.g., RF heatmaps)	Promising for real-time GPS spoofing detection with efficient scaling

Table 2-2 summarizes the three models' attributes.

Table 2-2. ML Model Attribute Summary

Feature / Attribute	LSTM (Long Short-Term Memory)	CNN (Convolutional Neural Network)	Transformer
Type	Recurrent Neural Network (RNN)	Deep learning model for spatial data	Attention-based deep learning model for sequential/spatial data
Detection Accuracy	>98.5% in some studies	Up to 99% accuracy across datasets	Over 95% accuracy under varying conditions
Hybrid Potential	Can be enhanced with Transformer-style attention	Can be fused with LSTM for spatial-temporal analysis	Ideal for hybrid models combining spatial and temporal features

VI. Contributions

This research makes several important contributions to the field of GPS spoofing detection and autonomous vehicle security:

1. Comparative Analysis of Deep Learning Models
    - Provides a structured evaluation of LSTMs, CNNs, and Transformer architectures, highlighting their strengths, limitations, and applications for GPS spoofing detection in AVs.
2. Hybrid Detection Framework Proposal
    - Demonstrates the potential of combining sequential (LSTM), spatial (CNN), and attention-based (Transformer) architectures to achieve superior detection accuracy (>95–99%) and reliability across various spoofing scenarios.
3. Operational Integration for AVs
    - Outlines practical considerations for deploying ML-based spoofing detection in AVs, including real-time latency constraints, Edge AI feasibility, and retraining requirements.
4. Future-proofing Through Emerging Technologies
    - Discusses how Quantum Machine Learning (QML), quantum cloud/cluster computing, and Edge AI can be integrated to enhance spoofing detection, fleet-wide retraining, and GPS signal authentication over time.
5. Contribution to GPS Security Research and Policy
    - Provides technical insights that can guide GPS spoofing benchmarks, dataset design, and development of government and industry standards for securing autonomous navigation systems used in critical infrastructure protection.

VII. Conclusion

Based on these results, each ML model offers individual advantages in GPS detection. However, a hybrid Transformer model that combines CNNs and LSTMs would deliver the best performance for GPS signal spoofing detection. This hybrid model would provide optimal GPS spoofing detection and supply live data feeds to sensors and other input systems to correct for erroneous signals, ensuring safe operation for AVs. Additionally, this hybrid model can be applied to other GPS-dependent systems, including military, industrial, agricultural, aeronautical, space, IoT, IIoT, financial, and cybersecurity applications.

A. Challenges and Limitations

Challenges and limitations identified in this research include data quality and availability, real-time processing, and threat actor evasion and detection. Given the lack of real-world spoofing attack data, most datasets in the current literature are based on computer models. Therefore, generalizing data results to real-world scenarios has inherent limitations. In a computer model simulation, some variables cannot be introduced, such as signal noise, environmental interference, and unpredictable behavior. The ability to extrapolate these lab-controlled results and deploy them in real-world AV scenarios is cautionary, as they may lead to failures and jeopardize passenger safety and navigation reliability. However, the technological data results of specific processes involved are concrete and of high value for current and future research.

During actual spoofing attacks, real-time processing of machine learning models is complex. Deep learning models are resource-intensive; therefore, on-board processing of this data may be limited by native, out-of-the-box systems. This limitation matters because missed detections can lead to critical system compromise. Furthermore, threat actors may exploit time gaps caused by data processing latency from native systems.

Static ML models are a safety concern and require continuous adaptive retraining. As detection techniques advance, threat actor methods, tactics, and techniques will advance as well. To address this challenge, implementing dynamic detection approaches that include adaptation and retraining of ML models is essential. Without this, false negative detection will increase, leading to operational vulnerabilities.

B. The Future of Machine Learning and GPS Security

As newer LLMs are developed, such as the current transformer model, GPS systems must be updated with these models to ensure they are protected against evolving, dynamic GPS spoofing tactics and techniques. As technology advances, threat actors continue to develop more sophisticated GPS spoofing capabilities. Researchers should aim not only to match adversaries' abilities but to exceed them, thereby ensuring the continued safety of AV navigation in the future.

Based on the research challenges and limitations presented, a recommendation for future research is to increase on-board AV processing capabilities. This is a technology-only limitation. As technology advances, the ability to integrate and leverage higher-level processing functions will become possible. With the development of quantum computing and quantum-like chip sets, research in this area will achieve significant progress in processing power and enable GPS systems

to overcome current limitations in data handling and latency. Cloud-Quantum GPS systems could enable high-dimensional data processing across multiple satellites, enabling multi-signal entanglement analogies, as well as accelerated ML training and retraining (Google, 2025). Quantum Machine Learning (QML) could advance spoofing detection by increasing anomaly detection sensitivity. Quantum-enhanced cryptography would enable unbreakable authentication keys for GPS signals with quantum key distribution (QKD) (Google, 2025), fortifying GPS signal encryption, which is currently absent from civilian systems.

Although Edge AI is currently in use in AVs, it is limited to processing camera data, LiDAR, and radar, such as Tesla's FSD computer, NVIDIA's Drive AGX Pegasus/Orin, and the Mobileye EyeQ chips (Microsoft, 2025). They are also used for lane keep assist, adaptive cruise control, and pedestrian detection (Microsoft, 2025). Extending Edge AI to GPS spoofing detection will significantly enhance AV navigation and safety. Furthermore, having lightweight models on GPS receivers for onboard signal spoofing detection will enable a mass defense strategy, especially for large AV fleets. Combining QML with Edge AI would create an "iron dome" defense against GPS spoofing with quantum cloud/cluster providing high-dimensional data, OTA updates, and global retraining, while Edge AI manages the lightweight, on-board data processing and spoofing detection.

On August 12, 2025, the United States Space Force launched a satellite designed to test systems for simultaneous GPS signal broadcast and receipt, autonomous operations, and anti-spoofing signals. It will experiment with new positioning, navigation, and timing (PNT) signals and payloads that could be used on future GPS satellites and help enhance capabilities for GPS-reliant systems (defensenews.com, 2025). These PNT tests will be the first of their kind since 1977, which today's GPS satellite systems rely on.

Acknowledgements

The author would like to express sincere gratitude to Dr. Aeron Zentner, D.B.A. and Dr. Tobi West, Ph.D., of Coastline College for their invaluable mentorship and guidance throughout the development of this research project. Their expertise, encouragement, and thoughtful feedback played a vital role in shaping both the technical direction and scholarly quality of this work.

References

Abrar, M. M., Youssef, A., Islam, R., Satam, S., Latibari, B. S., Hariri, S., & Satam, P. (2024). Gps-ids: An anomaly-based gps spoofing attack detection framework for autonomous vehicles. *arXiv preprint arXiv:2405.08359*.

Albon, C. https://www.defensenews.com/space/2025/08/13/space-force-launches- satellite-to-explore-new-gps-technology/, 2025

British Broadcasting Corporation www.bbc.com/news/world-middle-east-16098562, 2011

Chen, Q., Li, G., Liu, P., & Wang, Z. (2025). "Anomaly Detection and Secure Position Estimation Against GPS Spoofing Attack: A Security-Critical Study of Localization in Autonomous Driving," in IEEE Transactions on Vehicular Technology, vol. 74, no. 1, pp. 87-99, Jan. 2025, doi: 10.1109/TVT.2024.3454416.

Department of Homeland Security: Resilient Positioning, Navigation, and Timing (PNT) Conformance Framework, https://www.dhs.gov/publication/st-resilient-pnt-conformance-framework, 2022.

Department of Homeland Security. "Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure". Retrieved November 12, 2017.

Filippou, S., Achilleos, A., Zukhraf, S. Z., Laoudias, C., Malialis, K., Michael, M. K., & Ellinas, G. (2023). "A Machine Learning Approach for Detecting GPS Location Spoofing Attacks in Autonomous Vehicles," 2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring), Florence, Italy, 2023, pp. 1-7, doi: 10.1109/VTC2023-Spring57618.2023.10200857.

Ghanbarzade, A., & Soleimani, H. (2025). GNSS/GPS Spoofing and Jamming Identification Using Machine Learning and Deep Learning. *arXiv preprint arXiv:2501.02352*.

Google Gemini. (2025). (Version 2.5) [Large language model]. https://gemini.google.com/

Hakeem, S. A. A. & Kim, H. (2025). "Advancing Intrusion Detection in V2X Networks: A Comprehensive Survey on Machine Learning, Federated Learning, and Edge AI for V2X Security," in IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2025.3558849.

Işleyen, E. & Bahtiyar, S. (2024). "GPS Spoofing Detection on Autonomous Vehicles with XGBoost," 2024 9th International Conference on Computer Science and Engineering (UBMK), Antalya, Turkiye, 2024, pp. 500-505, doi: 10.1109/UBMK63289.2024.10773593.

Microsoft Copilot. (2025, August 14). [Large language model]. https://copilot.microsoft.com

Niu, B., Zhuang, X., Lin, Z., Zhang, L., (2024). "Navigation spoofing interference detection based on Transformer model", Advances in Space Research, Volume 74, Issue 10, 2024, Pages 5156-5171, ISSN 0273-1177, https://doi.org/10.1016/j.asr.2024.07.016.

OpenAI. (2025a). *ChatGPT-5* (Aug 13 version) [Large language model]. https://chat.openai.com/chat

OpenAI. (2025b). *ChatGPT-5* (Aug 13 version) [Large language model]. https://chat.openai.com/chat

OpenAI. (2025c). *ChatGPT-5* (Aug 13 version) [Large language model]. https://chat.openai.com/chat

Peterson & Faramarzi, https://www.csmonitor.com/World/Middle-_East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer, 2011

Shabbir, M., Kamal, M., Ullah, Z. & Khan, M. M. (2023). "Securing Autonomous Vehicles Against GPS Spoofing Attacks: A Deep Learning Approach," in IEEE Access, vol. 11, pp. 105513-105526, 2023, doi: 10.1109/ACCESS.2023.3319514.

Zhang, H., Wang, Z. & Vallery, H. (2023). "Learning-based NLOS Detection and Uncertainty Prediction of GNSS Observations with Transformer-Enhanced LSTM Network," 2023 IEEE 26th International Conference on Intelligent Transportation Systems (ITSC), Bilbao, Spain, 2023, pp. 910-917, doi: 10.1109/ITSC57777.2023.10422672.