International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 3, pp 344-353, March-2024

https://doi.org/10.47001/IRJIET/2024.803053

Spoofer Chain: Detecting CAV Location Spoofing with Blockchain and Quantum Cryptography

[1]M.Shankar, [2]K.Deepan, [3]P.V.Dinesh, [4]A.Karthikeyan

[1]Assistant Professor, Department of Computer Science and Engineering, Erode Sengunthar Engineering College, Perundurai, Erode, Tamilnadu, India

[2,3,4]Student, Department of Computer Science and Engineering, Erode Sengunthar Engineering College, Perundurai, Erode, Tamilnadu, India

Abstract **- Connected and Autonomous Vehicles (CAVs) are a category of vehicles that combine connectivity, automation, and advanced technologies to enhance transportation efficiency, safety, and convenience. A CAV GPS spoofing attack refers to a type of cybersecurity threat aimed at Connected and Autonomous Vehicles (CAVs) by manipulating their Global Positioning System (GPS) navigation data. GPS spoofing involves transmitting fake GPS signals to mislead CAVs' onboard GPS receivers, causing them to make incorrect location and navigation decisions. This form of attack can have serious consequences, including altering the vehicle's route, causing it to deviate from its intended path, or even leading to accidents or safety issues. One of the primary challenges is the continual evolution of spoofing methods, with attackers employing increasingly sophisticated techniques. This constant innovation makes it difficult for existing algorithms to effectively detect and prevent GPS spoofing. The project aims to tackle these challenges by integrating blockchain technology for data integrity, LSTM algorithms for analysing GPS time series data, and quantum cryptography for secure communication. Through this integration, the goal is to detect and prevent location spoofing attacks and establish a secure and trustworthy framework for CAVs in a world where reliable GPS data is essential for their operation. This project introduces a multifaceted solution that combines cutting-edge technologies to safeguard CAVs from location spoofing attacks. The integration of blockchain technology ensures the integrity of GPS data by creating a tamper-resistant ledger of information. Long Short-Term Memory (LSTM) algorithms are employed to analyze GPS time series data, enhancing the system's ability to detect anomalies and attacks. Furthermore, the project leverages the power of quantum cryptography to establish secure and unbreakable communication channels between CAVs and data processing centers. Quantum cryptography utilizes the principles of quantum mechanics to encrypt and transmit data in a way that is practically immune to eavesdropping and hacking. By amalgamating these elements into the SpooferChain framework, the project aims to provide a holistic and resilient defense against location spoofing attacks on CAVs. This not only ensures the safety of passengers and the proper functioning of autonomous vehicles but also paves the way for a more secure and trustworthy environment for CAVs in the future.**

Keywords: Connected and Autonomous Vehicles (CAVs), GPS spoofing attack, Cybersecurity threat, Global Positioning System (GPS) manipulation, Fake GPS signals, Incorrect location and navigation decisions.

I. LITERATURE REVIEW

1.1) Title: 3D Radio Map-Based GPS Spoofing Detection and Mitigation for Cellular-Connected UAVs

Author: Yongchao Dang; Alp Karakoc;

Year: 2023

Reference Link: https://ieeexplore.ieee.org/document/10254521

Problem: The Author addresses the vulnerability of cellular-connected Unmanned Aerial Vehicles (UAVs) to GPS spoofing attacks due to their reliance on the unencrypted civil GPS services. These attacks can manipulate UAVs' locations and disrupt their missions, emphasizing the need for a secure navigation solution.

Objective: The objective is to leverage 3D radio maps and machine learning techniques to detect and mitigate GPS spoofing attacks in cellular-connected UAVs. This involves constructing a theoretical 3D radio map, employing machine learning methods (Multi-Layer Perceptrons, Convolutional Neural Networks, and Recurrent Neural Networks) to analyze Received Signal Strength (RSS) values, and applying the particle filter to relocate the UAV and mitigate GPS deviation when spoofing is detected.

Methodology: The methodology includes the use of ray tracing tools, deterministic channel models, and Kriging methods to create a theoretical 3D radio map. Machine

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 8, Issue 3, pp 344-353, March-2024
https://doi.org/10.47001/IRJIET/2024.803053

learning methods are then applied to analyze real-time RSS values reported by UAVs and base stations, comparing them to the theoretical RSS values derived from the radio map. A particle filter is used for GPS spoofing mitigation.

Algorithm: Algorithms mentioned include ray tracing, deterministic channel models, Kriging methods, Multi-Layer Perceptrons (MLP), Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and the particle filter.

Dataset: Simulation platform for cellular-connected UAVs in an urban canyon environment.

Merits:

- Effective spoofing detection using machine learning.
- Universal Kriging (UK) with an exponential kernel demonstrates low standard errors for radio map construction.
- MLP achieves high spoofing detection accuracy, robust to environmental impacts.
- CNN provides comparable accuracy with less training time, thanks to raw RSS data inputs.
- Particle filter-based GPS spoofing mitigation can relocate the UAV to its real position within an error of 10 meters using 100 particles.

Demerits:

- The proposed solution is specifically designed for cellular-connected UAVs in an urban canyon environment, limiting its applicability to different environments and connection types.
- Radio map construction consumes substantial computation and storage resources, making it challenging to build radio maps in large regions within an edge server.

1.2) Title: Reliable Detection of Location Spoofing and Variation Attacks
Author: Chiho Kim; Sang-Yoon Chang
Year: 2023
Reference Link: https://ieeexplore.ieee.org/document/10032501

Problem: Location spoofing is a critical attack in mobile communications, and previous studies in this area have limitations in performance and fail to consider emerging attack variations. The problem addressed by the Author is to develop a reliable methodology for detecting location spoofing attacks and their variations with improved accuracy and resilience to diverse types of spoofing attacks.

Objective: The objective is to reliably detect location spoofing and its variations by introducing a data-driven methodology. To achieve this, the Author introduces a new set of differential features that can check mobility constraints and inconsistencies, significantly improving detection accuracy and reliability compared to previous research. The objective also includes the establishment of a profiling-based detection approach for zero-day detection.

Methodology: The methodology is data-driven and utilizes a set of new features that are differential in nature. These features are used to check mobility constraints and inconsistencies in coordinate data. The Author also introduces a profiling-based detection approach, which refers only to legitimate coordinate data to enhance resilience to previously unseen attacks.

Algorithm: A data-driven methodology for detecting location spoofing attacks accurately and reliably. In particular, our scheme utilizes a new set of features, which is differential in nature and enables the checking of the mobility constraints and inconsistency. The profiling-based detection captures the characteristics of the Normal instances and then discriminates Spoofed samples deviating from the learned representation.

Dataset: The Author mentions the use of the "VeReMi dataset," which includes a collection of data instances with both original and spoofed coordinate information.

Merits:

- Significant improvement in detection accuracy and reliability compared to previous research.
- Introduction of a new set of features that enhance detection performance.
- Effective identification of diverse types of spoofing attacks and their variations, achieving up to 99.1% accuracy.

Demerits:

- Computational Resource Intensive: The methodology may require substantial computational resources, potentially limiting its practicality in resource-constrained settings.
- Security Against Adversarial Attacks: Resilience against potential adversarial attacks is not thoroughly considered, which is crucial for practical deployment.

1.3) Title: A Light-Weight Technique to Detect GPS Spoofing Using Attenuated Signal Envelopes
Author: (Author names not provided in the provided text)
Year: Publication year is not provided.
Reference Link: No reference link is provided.

Problem: GPS spoofing attacks are becoming more prevalent and effective, posing significant security risks. Existing

ISSN (online): 2581-3048
Volume 8, Issue 3, pp 344-353, March-2024
https://doi.org/10.47001/IRJIET/2024.803053

techniques for GPS spoofing detection suffer from computational complexity, hardware/software requirements, or lack of accuracy, and there is a need for a more efficient and accurate solution.

Objective: The objective of the Author is to propose a light-weight GPS spoofing detection method that leverages the distinctive transmission characteristics of fake GPS signal envelopes due to signal attenuation differences. The goal is to improve accuracy and reduce computational complexity in GPS spoofing detection.

Methodology: The proposed technique is based on an analytical model of the distribution of a signal's envelope. It focuses on the variance of the received signal's envelope, which exhibits significant differences in attack and legitimate scenarios. The technique uses a threshold for the variance of samples in a signal envelope and dynamically adjusts the threshold based on the dispersion value of the variance to maximize detection performance.

Algorithm:

- An analytical model for the distribution of a signal's envelope based on the distance between the transmitter and receiver.
- A light-weight threshold technique based on the distribution of signal envelopes to detect GPS spoofing attacks.
- A dynamic threshold selection mechanism based on the dispersion of variance of a signal's envelope.

Dataset: The Author mentions experiments based on actual GPS signals and hardware, but it does not provide specific information about the dataset used.

Merits:

- Introduces a light-weight GPS spoofing detection technique.
- Utilizes distinctive transmission characteristics of spoofed GPS signal envelopes.
- Improves accuracy and reduces computational complexity compared to existing techniques.
- Features a dynamic threshold based on the dispersion value of the variance.
- Achieves a probability of detection greater than 90%.

Demerits:

- Leads to significant reduction of the detection time in the proposed technique.
- Challenging to assess the validity and applicability of the proposed technique in real-world scenarios.

1.4) Title: A Slowly Varying Spoofing Algorithm Avoiding Tightly-Coupled GNSS/IMU With Multiple Anti-Spoofing Techniques

Author: Yangjun Gao; Guangyun Li
Year: 2022
Reference Link: https://ieeexplore.ieee.org/document/9772951

Problem: The problem addressed in this Author is the increasing threat of GNSS (Global Navigation Satellite System) spoofing attacks on vehicles and aircraft, particularly those equipped with tightly-coupled GNSS/IMU (Inertial Measurement Unit) systems. GNSS spoofing is a preferred method for spoofers due to its high concealment and potential for causing harm to navigation systems.

Objective: The Author aims to develop a spoofing algorithm that can gradually change the positioning results of tightly-coupled GNSS/IMU systems without being detected by multiple anti-spoofing techniques. It seeks to counter non-cooperative targets using GNSS spoofing and to provide a solution for implementing GNSS spoofing with high concealment.

Methodology: The methodology involves establishing a GNSS spoofing mathematical model and proposing a slowly varying spoofing algorithm. The algorithm is based on an analysis of the influence mechanism of spoofing on the positioning of tightly-coupled GNSS/IMU systems. It introduces a measurement deviation determination method to avoid various anti-spoofing techniques and manipulate the positioning results gradually.

Algorithm: The Author presents a "slowly varying spoofing algorithm" to manipulate the positioning results of tightly-coupled GNSS/IMU systems. Specific technical details about the algorithm are not provided in the text.

Dataset: Simulation

Merits:

- The algorithm is designed to gradually change the positioning of tightly-coupled GNSS/IMU systems within 30 seconds.
- The algorithm is effective in achieving a spoofing effect with high concealment.
- It avoids detection by anti-spoofing techniques, including least squares residual Receiver Autonomous Integrity Monitoring (RAIM) and parameter rationality checks.

Demerits:

- The Author lacks specific information about the practical applicability and scalability of the proposed approach.

ISSN (online): 2581-3048
Volume 8, Issue 3, pp 344-353, March-2024
https://doi.org/10.47001/IRJIET/2024.803053

- Ethical considerations, legal implications, and privacy concerns associated with GNSS spoofing are not discussed.
- The research directions mentioned for future work are general and lack specifics.

1.5) Title: Deep-Ensemble-Learning-Based GPS Spoofing Detection for Cellular-Connected UAVs
Author: Yongchao Dang; Chafika Benzaïd;
Year: 2022
Reference Link: https://ieeexplore.ieee.org/document/9845684

Problem: The Author addresses the problem of GPS spoofing in cellular-connected Unmanned Aerial Vehicles (UAVs). UAVs are vital for assisting cellular communications and IoT deployment, but they are vulnerable to GPS spoofing attacks, which can deviate them from their intended trajectories. The existing mobile positioning system can help verify UAV GPS locations for spoofing detection, but it requires a minimum of three base stations (BSs) simultaneously.

Objective: The objective is to propose a deep-ensemble-learning-based system for UAV monitoring and tracking to detect GPS spoofing in cellular-connected UAVs. The proposed method uses path losses between BSs and UAVs' communication to indicate UAV trajectory deviations caused by GPS spoofing. The goal is to achieve accurate detection while minimizing energy consumption on UAVs.

Methodology: The methodology involves using deep ensemble learning methods, particularly multilayer perceptron (MLP) neural networks, to analyze statistical features of path losses between BSs and UAVs. Statistical-MLP and multi-MLP ensemble algorithms are introduced to predict GPS spoofing probabilities at each BS and integrate these predictions using six different ML models. The Author also mentions the potential introduction of graphic neural networks (GNN) to support swarm spoofing detection.

Algorithm: Statistical-MLP and multi-MLP ensemble algorithms, no specific details provided for the ML models used.

Dataset: The Author does not specify the dataset used.

Merits:

- Achieves above 97% accuracy in GPS spoofing detection under two BSs.
- Maintains at least 83% accuracy under only one BS.
- Energy-efficient solution with no additional requirements and energy consumption on UAVs.
- Short testing time under various ML models.

Demerits:

- Designed for a single cellular-connected UAV and lacks consideration for UAV swarms.
- Running multiple spoofing detection models on MEC and edge cloud servers per UAV may lead to less cooperation among the detection procedures.
- Potential computational resource limitations when a large UAV swarm connects with a single BS.
- The Author mentions introducing GNN for swarm spoofing detection but does not provide detailed information.

1.6) Title: GANSAT: A GAN and SATellite Constellation Fingerprint-Based Framework for GPS Spoof-Detection and Location Estimation in GPS Deprived Environment
Author: Debashri Roy; Tathagata Mukherjee; Year: 2022
Reference Link: https://ieeexplore.ieee.org/document/9761924

Problem: Adversarial and natural disruptions in GPS signals, especially spoofing attacks.

Objective: Develop a robust system for mitigating GPS disruptions by combining a software-based defence mechanism against spoofing attacks using generative adversarial networks (GANs) and deep neural network models for inferring positioning information in GPS-degraded/denied environments.

Methodology: Unified framework combining GAN-based spoofing detection and satellite constellation fingerprinting. GANSAT neural networks implicitly learn hardware fingerprints of GPS satellites in the constellation. Raw GPS signals collected using software-defined radio (SDR) from five different locations in Florida, USA. Spoofing of GPS signals conducted in an uncontrolled laboratory environment using a GPS spoofer implemented with SDR.

Algorithm:

- Utilizes generative adversarial networks (GANs) for spoofing detection.
- Employs deep neural network models for location estimation.

Dataset: Raw GPS signals collected in real outdoor environments at five different locations in the Florida panhandle area of the United States.

Merits:

- Achieves ~99.5% accuracy for identifying and filtering spoofed GPS signals from real ones.
- Achieves ~100% accuracy for location estimation.

ISSN (online): 2581-3048
Volume 8, Issue 3, pp 344-353, March-2024
https://doi.org/10.47001/IRJIET/2024.803053

- Resilient to various spoofing attacks as it operates on the physical layer.
- Demonstrates efficacy through spatial correlations in GPS signal data.
- Compares favorably with other GPS spoofer detection schemes in terms of time complexity.

Demerits:

- Tested on data from only five locations, limiting generalizability.
- The Author discusses the feasibility of large-scale deployment but does not provide detailed plans for such deployments.
- The idea of temporal transfer learning is mentioned for adapting GANSAT models to real-time data, which may require industry-level collaboration for implementation and testing.

1.7) Title: Spoofer-to-Target Association in Multi-Spoofer Multi-Target Scenario for Stealthy GPS Spoofing
Author: Bethi Pardhasaradhi; Pathipati Srihari;
Year: 2021
Reference Link: https://ieeexplore.ieee.org/document/9495815

Problem: GPS receivers are vulnerable to spoofing, and this Author addresses the challenge of spoofing in a multi-spoofer multi-target (MSMT) scenario.

Objective: The objective of the Author is to develop a generalized mathematical model and centralized networking-based spoofing techniques to enhance spoofer-to-target association, improve hit ratios, and reduce position errors in GPS spoofing.

Methodology: The Author uses a mathematical model to describe the transmission and reception of GPS spoofed signals in MSMT scenarios. It formulates spoofer-to-target association as an optimization problem with unique mapping constraints. Three centralized networking-based spoofing techniques are proposed to overcome the challenges of spoofer-to-target association.

Algorithm:

- Global Nearest Neighbor (GNN) based centralized spoofing.
- Spoofers of opportunity-based centralized spoofing with GNN association.
- Tunable transmitting power-based centralized spoofing with the GNN association.

Dataset: Simulated Environment

Merits:

- The proposed algorithms outperform distributed spoofing methods.
- Improved spoofer-to-target association, hit ratios, and position accuracy.
- High spoofing efficiency, with 100% hit-ratio achieved with tunable power-based spoofing.
- The proposed algorithms are effective for spoofing both high precision and low precision GPS receivers.

Demerits:

- Assumes line of sight (LOS) for spoofer-to-target association, which may not always hold.
- Focuses on static targets and spoofers; dynamic scenarios are not addressed.
- Assumes an omni-directional antenna-based framework, which may not apply to scenarios with directional antennas or urban environments.

1.8) Title: Detecting Signal Spoofing Attack in UAVs Using Machine Learning Models
Author: Arslan Shafique; Abid Mehmood
Year: 2021
Reference Link: https://ieeexplore.ieee.org/document/9456965

Problem: Due to advancements in interactive multimedia systems and technologies, the security of autonomous systems like Unmanned Aerial Vehicles (UAVs) has become a major concern. UAVs are vulnerable to various hacking techniques, including spoofing, which involves injecting fake signals into their sensors. This Author focuses on protecting UAVs from GPS signal spoofing attacks.

Objective: The objective of this Author is to propose a methodology that incorporates machine learning (ML) algorithms, specifically the Support Vector Machine (SVM), to detect counterfeit GPS signals that are spoofed to deceive UAVs. The Author also conducts a detailed analysis of various learning algorithms to select the most suitable one.

Methodology: The proposed methodology uses machine learning models to classify received signals from UAVs as either spoofed or authentic. Multiple ML algorithms are evaluated to choose the best classification algorithm. Signal characteristics of GPS signals, including features such as jitter, shimmer, and frequency modulation, are used to train the model. K-fold cross-validation analyses are performed to create multiple K-learning models, which are used for voting to enhance the model's accuracy. Both soft and hard voting techniques are applied to assign classes to unseen or test data. The Author also conducts experiments to evaluate the model's

ISSN (online): 2581-3048
Volume 8, Issue 3, pp 344-353, March-2024
https://doi.org/10.47001/IRJIET/2024.803053

performance, considering metrics like accuracy, precision, recall, and F1-score.

Algorithm: The primary algorithm used in the proposed methodology is the Support Vector Machine (SVM). The Author evaluates various ML algorithms as part of the methodology.

Dataset: Dataset that consists of different characteristics of GPS signal such as jitter, jitter (absolute), jitter (local), jitter (RAP), jitter (ppq5), shimmer, shimmer(local), shimmer(dB), shimmer(apq3) and shimmer (apq5).

Merits:

- The proposed model effectively detects counterfeit GPS signals.
- Multiple ML algorithms are evaluated to select the most suitable one.
- K-fold cross-validation and voting techniques enhance model accuracy.
- Comparative analysis with existing methods shows the superiority of the proposed model.

Demerits:

- The Author suggests improvements with deep learning algorithms but does not implement them in this work.

1.9) Title: SCER Spoofing Attacks on the Galileo Open Service and Machine Learning Techniques for End-User Protection
Author: Francisco Gallardo;
Year: 2020
Reference Link: https://ieeexplore.ieee.org/document/9085417

Problem: The Author addresses the issue of spoofing attacks on Global Navigation Satellite Systems (GNSS), particularly Secure Code Estimation and Replay (SCER) spoofing attacks. SCER attacks are considered challenging and problematic for GNSS protection systems, necessitating complementary protection techniques.

Objective: The objective of the Author is to analyze SCER spoofing attacks on GPS and Galileo, discuss the role of Galileo's Pseudorandom Noise (PRN) intra-satellite non-orthogonality distortion term, and propose a machine learning-based detection method for end-user receivers to counteract SCER attacks.

Methodology: The Author utilizes detailed analysis of SCER attacks, simulation of SCER attack quality curves for GPS and Galileo, and the development of a machine learning-based detection method using features extracted from the receiver search space.

Algorithm: Machine learning techniques, specifically Decision Trees, are employed for SCER spoofing detection.

Dataset: The datasets used for experimentation were generated with various combinations of Doppler shifts and time delays.

Merits:

- Detailed analysis of SCER spoofing attacks, especially on Galileo.
- Comparison of SCER attack quality curves between GPS and Galileo.
- Proposal of a machine learning-based detection method with high accuracy.
- Enhancement of false alarm rates for specific scenarios.

Demerits:

- Specific details about the dataset and its practical applications are limited.
- The effectiveness of the proposed method may be compromised if the attacker can nullify the original satellite signal.

1.10) Title: Detection of Spoofing Attacks in WLAN-Based Positioning Systems Using WiFi Hotspot Tags
Author: Ayong Ye; Qing Li
Year: 2020
Reference Link: https://ieeexplore.ieee.org/document/9007700

Problem: The problem addressed in this Author is the vulnerability of WLAN-based positioning systems to location spoofing attacks. These attacks can raise significant privacy concerns, particularly in the context of Mobile Social Network Services (MSNS).

Objective: The objective is to develop a defense mechanism to detect and prevent spoofing attacks in WLAN-based positioning systems. The proposed mechanism is based on the use of WiFi hotspot tags (BS tags) to authenticate the spatial-temporal properties of geolocations.

Methodology: The methodology involves the following key steps: Creation of a privacy attack model based on spoofing attacks in MSNS.Development of a defence mechanism using BS tags for spatial-temporal authentication. Introduction of bloom filters to compress portions of real-time hotspot frames while maintaining high entropy. Design of a tag verification algorithm based on fuzzy extractors to adapt to high bit-error rates in wireless transmission. Verification of the safety and feasibility of the proposed mechanism through theoretical and experimental analysis.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 3, pp 344-353, March-2024

https://doi.org/10.47001/IRJIET/2024.803053

Algorithm: The Author describes a "tag verification algorithm based on fuzzy extractors" to authenticate geolocations. Specific technical details about the algorithm are not provided in the text.

Dataset: Simulation.

Merits:

- Development of a defence mechanism to detect and prevent spoofing attacks in WLAN-based positioning systems.
- Use of WiFi hotspot tags for spatial-temporal authentication.
- Introduction of bloom filters to reduce storage overhead and tolerate channel errors.
- Design of a tag verification algorithm to adapt to high bit-error rates in wireless transmission.

Demerits:

- Need to evaluate other signal features, trying to reduce the computational load of the extraction step.
- Multipath simulation will be considered and more sophisticated RFI detection methods will be evaluated, too.

II. COMPARITIVE TABLE

No	Author Info	Methodology	Algorithm	Merits	Demerits
1	Title: 3D Radio Map-Based GPS Spoofing Detection and Mitigation for Cellular-Connected UAVs. Author: Yongch o Dang; Alp Karakoc; Year:2023	Utilizes ray tracing tools, deterministic channel models, Kriging methods for 3D radio map construction. Employs Multi-Layer Perceptrons (MLP) for spoofing detection.	Ray tracing, deterministic channel models, Kriging methods, MLP, CNN, RNN, particle filter.	Universal Kriging (UK) with exponential covariance function results in low standard errors for radio map construction.	The proposed solution is specifically designed for cellular-connected UAVs in an urban canyon environment
2	Title: Reliable Detection of Location Spoofing and Variation Attacks. Author: Chiho Kim;Sang-Yoon Chang Year:2023	Utilizes a data-driven methodology with a new set of differential features to check mobility constraints and inconsistencies.	Profiling-based detection	Feasibility of the new features for identifying diverse types of spoofing attacks and their variations.	Spoofed samples deviating from the learned representation
3	Title: A Light-Weight Technique to Detect GPS Spoofing Using Attenuated Signal Envelopes. Author: Xiao Wei; Year:2023	The Author presents a technique based on an analytical model of signal envelope distribution.	Analytical model, light-weight threshold technique	Improves accuracy and reduces computational complexity compared to existing techniques.	Challenging to assess the validity and applicability of the proposed technique in real-world scenarios.
4	Title: A Slowly Varying Spoofing Algorithm Avoiding Tightly-Coupled GNSS/IMU With Multiple Anti-Spoofing Techniques. Author: Yangjun Gao;	The methodology includes establishing a GNSS spoofing mathematical model and proposing a slowly varying spoofing algorithm.	GNSS spoofers, poofing algorithm	Provides an effective solution for non-cooperative targets with tightly-coupled GNSS/IMU	Exceed the alarm threshold

ISSN (online): 2581-3048
Volume 8, Issue 3, pp 344-353, March-2024
https://doi.org/10.47001/IRJIET/2024.803053

	Guangyun Li Year:2022			systems.	
5	Title:Deep Ensemble-Learning-Based GPS Spoofing Detection for Cellular-Connected UAVs. Author: Yongchao Dang; Chafika Benzaïd Year:2022	Utilizes path losses between base stations (BSs) and UAVs' communication to indicate UAV trajectory deviations due to GPS spoofing.	Statistical-MLP algorithm, multi-MLP ensemble algorithm for integration.	Achieves above 97% accuracy in GPS spoofing detection under two BSs.	Designed for a single cellular-connected UAV and lacks consideration for UAV swarms.
6	Title: GANSAT: A GAN and SATellite Constellation Fingerprint-Based Framework for GPS Spoof-Detection and Location Estimation in GPS Deprived Environment. Author: Debashri Roy Year:2022	Combines GAN-based spoofing detection with deep neural network models for location estimation. GANSAT neural networks learn satellite constellation fingerprints to identify spoofed GPS Signals.	Utilizes generative adversarial networks (GANs) for spoofing detection and deep neural network models for location estimation.	Achieves ~99.5% accuracy for identifying and filtering spoofed GPS signals from real ones. Resilient to various spoofing attacks as it operates on the physical layer.	Tested on data from only five locations, limiting generalizability.
7	Title: Spoofer-to-Target Association in Multi-Spoofer Multi-Target Scenario for Stealthy GPS Spoofing. Author: Bethi Pardhasaradhi; Pathipati Srihari; Year:2021	The Author presents a mathematical model for multi-spoofer multi-target scenarios, spoofer management, and spoofer-to-target association.	GNN-based centralized spoofing, Spoofers of Opportunity-based centralized spoofing, and Tunable Transmitting Power-based centralized spoofing.	Proposed algorithms outperform distributed spoofing.	GNN-based centralized spoofing has lower hit ratios, limitations in the installation of more spoofers
8	Title: Detecting Signal Spoofing Attack in UAVs Using Machine Learning Models. Author: Arslan Shafique; Abid Mehmood Year:2021	A machine learning model is proposed to classify spoofed and authentic signals received by UAVs.	Support Vector Machine (SVM) and multiple machine learning algorithms are evaluated.	The proposed model effectively detects counterfeit GPS signals with a high level of accuracy.	The Author suggests further improvemen with deep learning (DL) algorithms, but these are not implemented in this work.
9	Title: SCER Spoofing Attacks on the Galileo Open Service and	The Author conducts a detailed analysis of SCER attacks on GPS and Galileo,	Decision Trees, for the proposed SCER spoofer	Provides quality curves for SCER attacks on	it may not be effective if the attacker can null

ISSN (online): 2581-3048
Volume 8, Issue 3, pp 344-353, March-2024
https://doi.org/10.47001/IRJIET/2024.803053

	Machine Learning Techniques for End-User Protection. Author: Francisco Gallardo; Year:2020	focusing on the role of the Galileo PRN distortion term.	detection method.	Galileo.	the original satellite signal.
10	Title: Detection of Spoofing Attacks in WLAN-Based Positioning Systems Using WiFi Hotspot Tags. Author: Ayong Ye; Qing Li; Year:2020	The Author presents a defense mechanism based on WiFi hotspot tags (BS tags) to authenticate the spatial-temporal	bloom filter, fuzzy extractors	Prevent spoofing attacks in WLAN-based positioning systems.	storage and communication overhead

III. CONCLUSION

In conclusion, the survey papers on GPS spoofing attack detection and prevention highlight the critical importance of securing the navigation systems of connected and autonomous vehicles. As these technologies become increasingly integrated into our daily lives, the potential threats posed by GPS spoofing attacks cannot be underestimated. The papers delve into various existing algorithms, techniques, and emerging technologies aimed at countering these threats. Despite the progress made in GPS spoofing detection, numerous challenges persist. The dynamic and innovative nature of spoofing attacks, limited training data, environmental variability, resource constraints, and privacy concerns pose significant hurdles. Addressing these challenges requires adaptability, robustness, and scalability in detection algorithms, all while adhering to legal and ethical standards. As we move forward, the integration of blockchain and quantum cryptography emerges as a promising approach to enhance security. These technologies offer new layers of protection and data integrity, fostering trust in the increasingly interconnected world of connected and autonomous vehicles.

REFERENCES

[1] S. Filippou, A. Achilleos, S. Z. Zukhraf, C. Laoudias, K. Malialis, M. K. Michael, and G. Ellinas, ‘‘A machine learning approach for detecting GPS location spoofing attacks in autonomous vehicles,’’ in Proc. IEEE 97th Veh. Technol. Conf., Jun. 2023, pp. 1–7.

[2] N. Souli, P. Kolios, and G. Ellinas, ‘‘Online relative positioning of autonomous vehicles using signals of opportunity,’’ IEEE Trans. Intell. Vehicles, vol. 7, no. 4, pp. 873–885, Dec. 2022.

[3] H. Sathaye, G. LaMountain, P. Closas, and A. Ranganathan, ‘‘SemperFi: Anti-spoofing GPS receiver for UAVs,’’ in Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS), 2022, pp. 1–17.

[4] D. Y. Jeon, T. Gaybullaev, J. H. Noh, J. M. Joo, S. J. Lee, and M.-K. Lee, ‘‘Performance analysis of authentication protocols of GPS, Galileo and BeiDou,’’ J. Positioning, Navigat., Timing, vol. 11, no. 1, pp. 1–9, 2022.

[5] M. Jayaweera, ‘‘A novel deep learning GPS anti-spoofing system with DOA time-series estimation,’’ in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2021, pp. 1–6.

[6] E. Basan, A. Basan, A. Nekrasov, C. Fidge, N. Sushkin, and O. Peskova, ‘‘GPS-spoofing attack detection technology for UAVs based on Kullback–Leibler divergence,’’ Drones, vol. 6, no. 1, p. 8, Dec. 2021.

[7] E. Ranyal and K. Jain, ‘‘Unmanned aerial vehicle’s vulnerability to GPS spoofing a review,’’ J. Indian Soc. Remote Sens., vol. 49, no. 3, pp. 585–591, Mar. 2021, doi: 10.1007/s12524-020-01225-1.

[8] Z. Wu, Y. Zhang, and R. Liu, ‘‘BD-II NMA&SSI: An scheme of antispoofing and open BeiDou II D2 navigation message authentication,’’ IEEE Access, vol. 8, pp. 23759–23775, 2020.

[9] Y. Dang, C. Benzaïd, Y. Shen, and T. Taleb, ‘‘GPS spoofing detector with adaptive trustable residence area for cellular based-UAVs,’’ in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2020, pp. 1–6.

[10] S. Semanjski, I. Semanjski,W. DeWilde, and A. Muls, ‘‘Use of supervised machine learning for GNSS signal spoofing detection with validation on real-world

ISSN (online): 2581-3048
Volume 8, Issue 3, pp 344-353, March-2024
https://doi.org/10.47001/IRJIET/2024.803053

meaconing and spoofing data—Part I,'' Sensors, vol. 20, no. 4, p. 1171, Feb. 2020.

[11] W. Liang, K. Li, and Q. Li, ''Anti-spoofing Kalman filter for GPS/rotational INS integration,'' Measurement, vol. 193, Apr. 2022, Art. no. 110962. 48

[12] S.-H. Seo, G.-I. Jee, and B.-H. Lee, ''Spoofing signal generation based on manipulation of code delay and Doppler frequency of authentic GPS signal,'' Int. J. Control, Autom. Syst., vol. 19, no. 2, pp. 1026–1040, Feb. 2021.

[13] N. Linty, A. Farasin, A. Favenza, and F. Dovis, ''Detection of GNSS ionospheric scintillations based on machine learning decision tree,'' IEEE Trans. Aerosp. Electron. Syst., vol. 55, no. 1, pp. 303–317, Feb. 2019.

[14] Chao Sun;, Joon Wayn Cheong;," GNSS Spoofing Detection Using Static or Rotating Single-Antenna of a Static or Moving Victim", IEEE Trans, GPS, Nov 2022.

[15] Garima Chopra; Rakesh Kumar Jha;" TPA: Prediction of Spoofing Attack Using Thermal Pattern Analysis in Ultra Dense Network for High-Speed Handover Scenario", IEEE, Trans, intel vehicle, Jun 2021.

Citation of this Article:

M.Shankar, K.Deepan, P.V.Dinesh, A.Karthikeyan, "Spoofer Chain: Detecting CAV Location Spoofing with Blockchain and Quantum Cryptography", Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 8, Issue 3, pp 344-353, March 2024. Article DOI https://doi.org/10.47001/IRJIET/2024.803053

****

