



# Blockchain Integrated Framework To Detect And Prevent CAV Location Spoofing Attacks Using GPS Time Data Learning And Quantum Cryptography

Nazeeb M

*PG Scholar, Department of Master of Computer Applications,  
Vidyaa Vikas College of Technology, Tirucengode, Tamilnadu, India*

Dr.S. Roshni

*Associate professor, Department of Computer Science Engineering,  
Vidyaa Vikas College of Technology, Tirucengode, Tamilnadu, India*

Dr.G. Lalitha

*Assistant Professor, Department of Master of Computer Applications,  
Vidyaa Vikas College of Technology, Tirucengode, Tamilnadu, India*

Date of Submission: 03-06-2024

Date of Acceptance: 13-06-2024

## 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. These vehicles rely heavily on accurate GPS data for navigation and operation. A CAV GPS spoofing attack refers to a type of cybersecurity threat aimed at CAVs by manipulating their GPS navigation data, involving the transmission of fake GPS signals to mislead onboard GPS receivers and cause 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.

## I. INTRODUCTION

The evolution of Connected and Autonomous Vehicles (CAVs) marks a pivotal shift in the transportation sector, promising unprecedented advancements in safety, efficiency, and user convenience. Central to the functionality of CAVs is their reliance on Global Positioning System (GPS) data to navigate and perform autonomous operations accurately. However, this reliance on GPS technology introduces a critical vulnerability: GPS location spoofing attacks.

Such attacks involve the deliberate manipulation of GPS signals to mislead vehicles about their true location, posing significant risks

ranging from minor navigational errors to severe safety threats, including collisions and traffic disruptions. Addressing these vulnerabilities is essential for the secure and reliable deployment of CAVs in real-world environments.

## II. LITERATURE SURVEY

### 2.1. TITLE: 3D RADIO MAP-BASED GPS SPOOFING DETECTION AND MITIGATION FOR CELLULAR-CONNECTED UAVS

Author: Yong Chao Dang; Alp Karakoc;

Year: 2023

Reference

Link:

<https://ieeexplore.ieee.org/document/10254521>

### PROBLEM:

The paper 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 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.

## **2.2. 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 paper 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 paper 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 paper 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 paper mentions the use of the "VeReMi" 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.

### III. PROPOSED SYSTEM

The proposed system, "SpoofChain," is a cutting-edge framework designed to effectively detect and prevent location spoofing attacks in Connected and Autonomous Vehicles (CAVs) by integrating blockchain technology, GPS time series data learning using Long Short-Term Memory (LSTM) networks, and the robust security of quantum cryptography. This innovative system offers a comprehensive approach to enhance the security and reliability of CAVs' GPS-based navigation systems. Here are the key components and features of the proposed system:

- **Real-Time Detection**  
"SpoofChain" provides real-time detection of location spoofing attempts. It continuously monitors incoming GPS data for anomalies, ensuring rapid responses to potential threats.
- **GPS Time Series Data Learning (LSTM)**  
The system employs machine learning techniques, particularly LSTM networks, to analyse historical GPS time series data. This enables the system to recognize patterns and anomalies indicative of spoofing attacks, enhancing detection accuracy.
- **Blockchain Integration**  
"SpoofChain" leverages blockchain technology to create a tamper-proof and transparent ledger of GPS data. This ensures the integrity of GPS data records and maintains a secure history of vehicle locations.
- **Quantum Cryptography**  
Quantum cryptography is used to secure communication channels between CAVs and infrastructure. It provides unbreakable encryption, preventing eavesdropping and ensuring the confidentiality of transmitted data.
- **Enhanced CAV Security**

The system significantly enhances the security of CAVs, reducing the risks associated with location spoofing attacks, which could lead to accidents, traffic disruptions, and security breaches

#### ADVANTAGES:

- It provides a multi-layered defence, significantly enhancing the security of CAVs.
- Swiftly detects and responds to spoofing attempts, minimizing operational disruption.
- Improved accuracy in detecting subtle anomalies, reducing false alarms.
- Blockchain ensures the integrity and transparency of GPS data records.
- Quantum cryptography safeguards data confidentiality.
- Enhances CAV safety, reducing accident and disruption risks.

### IV. MODULES

#### 1. CAV Simulation Environment

A Connected and Autonomous Vehicle (CAV) simulation environment is a virtual platform designed for testing and validating connected and autonomous vehicle technologies. CAV simulation environments often feature a realistic 2D virtual world that replicates real-world road networks, traffic conditions, and urban environments

#### 2. CAV Data Processing Centre

A Connected and Autonomous Vehicles (CAV) GPS Data Processing Centre is a specialized facility or infrastructure that focuses on the collection, management, processing, and analysis of GPS (Global Positioning System) data generated by CAVs.

#### 3. GPS Spoofing Attacker

A GPS spoofing attacker module is a component or software that is designed to manipulate or deceive Global Positioning System (GPS) receivers by transmitting false signals. Its primary purpose is to disrupt the accuracy of GPS-based location and timing information, which can have various implications, including security breaches and navigation errors

#### 4. GPS Spoofing Attack Detection

GPS spoofing attack detection using GPS time series data learning, specifically with Long Short-Term Memory (LSTM) networks, involves a sophisticated approach to identify and counteract GPS spoofing threats.

#### 5. SpoofChain Integration

The integration of SpoofChain, a blockchain-based system, with Connected and Autonomous Vehicles (CAV) and a CAV Data Processing Centre



provides a robust and secure framework for enhancing the security and reliability of CAV systems. CAVs generate a vast amount of data, including GPS information, sensor data, and vehicle performance metrics.

#### 6. Secure Communication

Quantum cryptography offers a highly secure means of communication between Connected and Autonomous Vehicles (CAVs) and CAV Data Processing Centres. This approach relies on Quantum Key Distribution (QKD) to establish secure encryption keys.

- **Quantum Key Distribution (QKD)**

Quantum Key Distribution (QKD) is a secure communication method that uses the principles of quantum mechanics to establish a secure encryption key between two parties.

- **Quantum Key Exchange**

The Quantum Key Exchange process, or Quantum Key Distribution (QKD), is a secure communication method based on quantum mechanics. In this process, two parties, typically Alice and Bob, exchange qubits, which can be in one of four quantum states.

- **Post Quantum Cryptography**

Post-quantum cryptography is a field focused on developing encryption schemes that remain secure against quantum computer attacks. The security of classical cryptographic algorithms, such as RSA and ECC, can be compromised by quantum computers using Shor's or Grover's algorithms.

### V. EXPERIMENT AND RESULTS

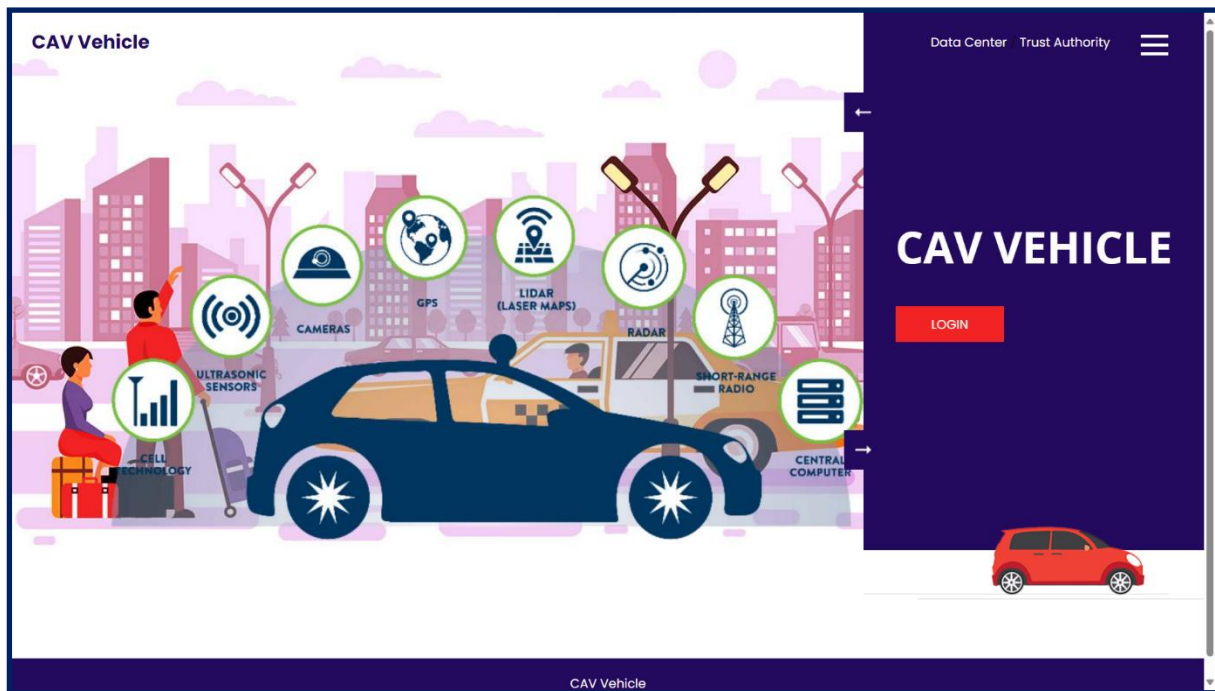


FIGURE NO.1 HOME PAGE



CAV Vehicle Data Center Trust Authority

### Data Processing Center

[LOGIN](#)

CAV Vehicle

**FIGURE NO.2 DATA PROCESSING CENTER**

CAV Vehicle Home User Logout

### CAV Vehicle Details

[ADD](#)

S.No	CAV Vehicle ID	Unique Address	Delete
1	R4533	E523.2553.84DF2	<a href="#">Delete</a>

CAV Vehicle

**FIGURE NO.3 CAV VEHICLE DETAILS**



**CAV Vehicle** Home User Logout

### Add User Details

Name Mobile No.

Email Unique Address

Username Password

**ADD**

S.No	Name	Mobile No.	E-mail	Unique Address	Username	CAV Vehicle	Delete
1	Harish	8975394627	harish@gmail.com	4855-E5A6-58C2	harish	<a href="#">Assign</a>	<a href="#">Delete</a>

CAV Vehicle

FIGURE NO.4 USER DETAILS

**CAV Vehicle** Home User Logout

### Assign CAV Vehicle

ⓄR4533

**ASSIGN**

S.No	CAV Vehicle ID	Unique Address	Delete
1	R4533	E523.2553.84DF2	<a href="#">Delete</a>

CAV Vehicle

FIGURE NO.5 ASSIGN CAV VEHICLE

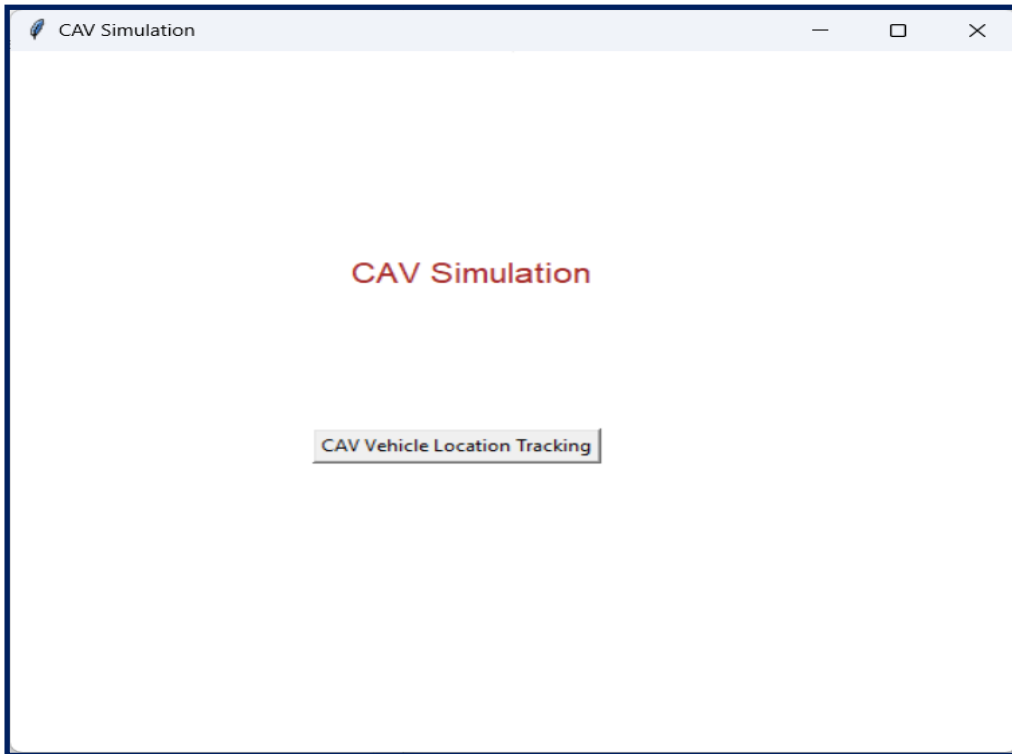


FIGURE NO.6 CAV SIMULATION

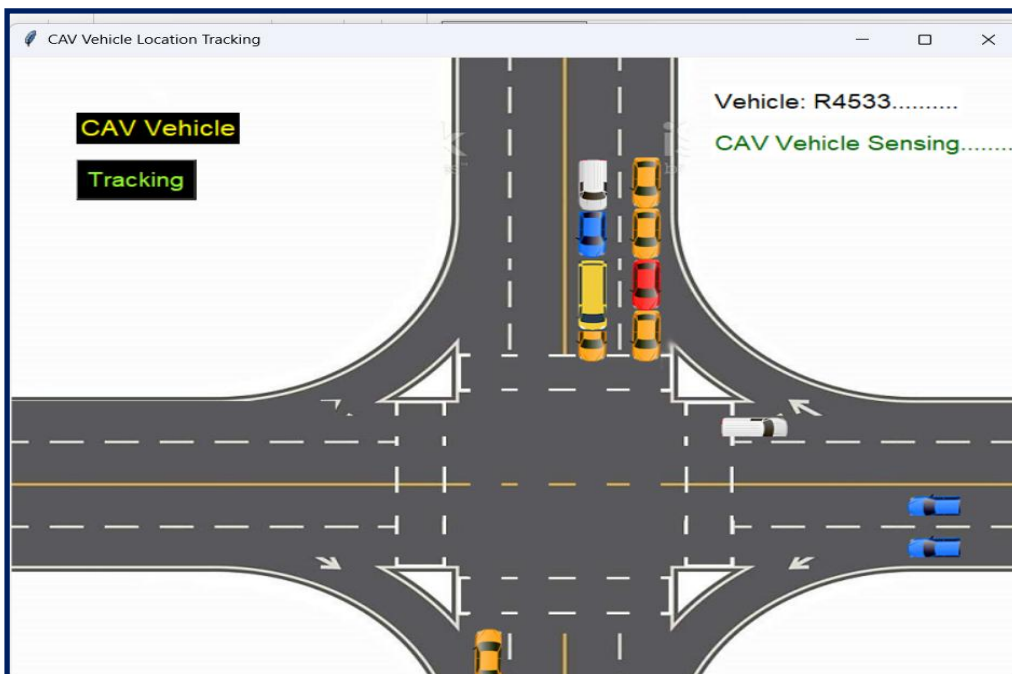


FIGURE NO.7 CAV SIMULATION TRACKING



Location	Date / Time
804d549b44 e7ea94afe5 ab61397340 82fcee0f52	2024-01-30 14:03:31
bcf09ad49a 57c641cc55 f5320ba9da f9f12c32de	2024-01-30 14:03:14
33365e3a93 d2129a9076 6252fb08a4 758b5e8966	2024-01-30 14:02:57
72bf484e3d 2c558af560 97469fcddb fc22d4c6b0	
334cbc7a44 1b7b55cf0a c9a37f3cla 469859c564	
ec34948d4a e42a97a869 06c6a6e987 b0f9ae32a6	

FIGURE NO.8 RECEIVED DATA

Decrypted Success..

Location: 12.2275, 78.2310

CAV Vehicle

FIGURE NO.9 RECEIVED DATA VERIFICATION



## VI. CONCLUSION

In conclusion, the project represents a significant advancement in the field of cybersecurity for connected autonomous vehicles (CAVs). By integrating GPS time series data learning (LSTM), quantum cryptography, and blockchain technology, the framework provides a robust defense mechanism against GPS spoofing attacks, ensuring the integrity and reliability of location-based services in autonomous vehicles.

trustable residence area for cellular based-UAVs,” in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2020, pp. 1–6.

## REFERENCE

- [1]. S. Filippou, A. Achilleos, S. Z. Zukhrif, 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