International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

EARLY DETECTION OF CAV VEHICLE LOCATION SPOOFING ATTACK

Dhayal K[1], Dhanvanth S B[2], Sarathkumar P M[3], Harish S[4]

[1] UG Student, Department of Electronics and Communication Engineering,
[2,3]UG Student, Department of Information Technology,
[4]UG Student, Department of Artificial Intelligence and Machine Learning,
[1,2,3,4]Bannari Amman Institute of Technology

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 analyse 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 centres. Quantum cryptography utilises 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 defence 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.*

Key Words: CAV, GPS spoofing, LSTM, Quantum cryptography

1. INTRODUCTION

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.

An autonomous transportation vehicle refers to a car outfitted with similar data transfer and programming capabilities as connected car systems. However, it possesses the additional capability of making autonomous decisions and responding accordingly. For instance, if the operator of a connected car surpasses the speed limit, the vehicle autonomously engages the brakes to ensure maximum safety for the occupants.

1.1 CONNECTED VEHICLE (CV) TECHNOLOGIES

Connected and autonomous vehicles share a common foundation, yet while the latter is still under development, connected car solutions are already in operation. The following are the technologies currently driving connected vehicles:

- Central Computer: A central data processing system featuring a user interface integrated into the driver panel facilitates seamless operation.

- GPS: Serving as a staple technology in the automotive industry, connected cars are equipped with embedded GPS systems, eliminating the need for external mobile apps or devices for navigation.

- Driver Assistance Sensors: Foundational to connected vehicles, these sensors enhance safety and convenience. For instance, rearview cameras aid in safe reversing by estimating distances from obstacles and providing timely signals for halting. In contrast, autonomous vehicles leverage Advanced Driver Assistance Systems (ADAS) that employ sensors and machine learning to analyze real-time environments and make safety-centric decisions autonomously.

- Wireless Communication: Crucial to both connected and autonomous vehicles, wireless communication enables instantaneous data exchange. This facilitates the provision of driving behavior optimization suggestions and enhances responses to emergencies, prioritizing safety.

1.2 CONNECTED VEHICLES COMMUNICATION TYPES

Connected car services utilize various approaches to facilitate data transfer among different entities:

- Vehicle-to-Vehicle (V2V): This involves the transmission of data from one vehicle to another. For instance, in the event of a collision, nearby drivers can receive alerts to be informed of the emergency.

- Vehicle-to-Infrastructure (V2I): With this technology, connected cars can exchange data with infrastructure elements such as emergency response centers, enabling seamless communication and coordination during emergencies or other critical situations.

- Vehicle-to-Device (V2D): A vehicle can send notifications directly to a driver's mobile device, enhancing the driver's awareness of relevant information or alerts.

- Vehicle-to-Cloud (V2C): V2C data transfer involves transmitting data to cloud-based platforms for storage, analysis, and further processing. This enables the aggregation of data from multiple vehicles for comprehensive insights and decision-making.

- Vehicle-to-Pedestrian (V2P): In this scenario, vehicles transmit signals to pedestrians to alert them of potentially hazardous situations, such as when a pedestrian's behavior poses a risk to their safety

- Vehicle-to-Everything (V2X): V2X encompasses a comprehensive data management infrastructure that enables seamless communication and interaction between vehicles, infrastructure, devices, pedestrians, and other relevant entities. This approach ensures robust connectivity and information exchange across various components of the transportation ecosystem.

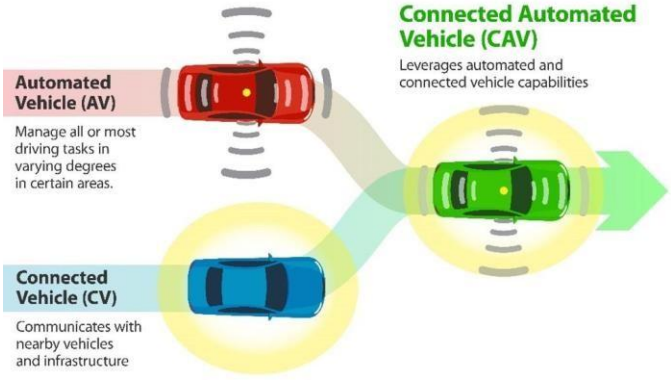

Figure 1.1 CAV

1.3 BENEFITS OF AUTONOMOUS CARS

Predicting the exact benefits of automotive software for cars, particularly in the realm of self-driving technology, remains challenging due to ongoing development. However, drones face restrictions in certain countries. Furthermore, experts suggest that the development of self-driving cars may take longer than anticipated due to the necessity for explicit legal regulations and the establishment of autonomous vehicle infrastructure. Despite these challenges, experts also anticipate several potential benefits of self-driving cars:

1. Enhanced Safety: Self-driving cars are expected to be programmed to make intelligent decisions, thereby promoting a safer road environment. This could lead to fewer accidents caused by distractions, speeding, and impaired driving.

2. Cost Savings: The anticipated reduction in accidents could lower medical care and insurance costs. Additionally, self-

driving vehicles equipped with preventive maintenance systems may decrease expenses associated with timely servicing and replacement of parts.

3. Time Savings and Increased Productivity: Owners of self-driving cars may efficiently manage personal and business tasks while on the move, eliminating the need to divert attention from driving. Features such as self-parking can further save time, allowing owners to focus on other activities upon arrival.

4. Greater Independence: Self-driving cars hold promise as a transportation option for individuals with disabilities or impairments. Operable through voice commands, these vehicles offer enhanced mobility, with the car autonomously making critical decisions.

2. OBJECTIVE AND METHODOLOGY

2.1. History of hydroponics

ASPECT	TRADITIONAL AUTONOMOUS VEHICLES	CONNECTED AND AUTONOMOUS VEHICLES
CONNECTIVITY	Operate independently and lack connectivity with external systems or infrastructure beyond basic navigation.	Highly connected vehicles that communicate with each other and infrastructure elements, enabling real-time data exchange for navigation, traffic management, and safety enhancement.
DECISION-MAKING MECHANISM	Rely solely on onboard sensors and pre programmed algorithms for decision making, without access to real-time data from external sources.	Engage in collaborative decision-making, leveraging connectivity to exchange data with other vehicles and infrastructure elements, enabling adaptive responses to changing road conditions and potential threats like GPS spoofing attacks.
INTEGRATION WITH INFRASTRUCTURE	Operate independently of smart city infrastructure and lack integration with traffic management systems.	Leverage onboard sensors and advanced computing capabilities to autonomously navigate and make decisions, ensuring reliable performance even in areas with limited smart city infrastructure
FOCUS ON PASSENGER EXPERIENCE	Prioritize passenger comfort and convenience within the vehicle, focusing on features like interior design and entertainment systems.	It also prioritize passenger experience, and additionally optimize overall transportation efficiency and safety through connectivity and collaboration, addressing broader societal needs beyond individual passenger comfort.
SAFETY AND EFFICIENCY OPTIMIZATION	Primarily rely on onboard sensors for navigation and lack advanced capabilities for anticipating and responding to potential hazards.	Prioritize safety and efficiency by leveraging connectivity and advanced sensor technologies, enabling real-time data exchange for hazard detection, traffic optimization, and GPS spoofing attack mitigation, thereby enhancing overall transportation safety and

		efficiency.

Table 1

3.2 OBJECTIVE OF THE MODEL

The objective of the model is to develop a comprehensive framework for detecting and preventing GPS spoofing attacks in Connected and Autonomous Vehicles (CAVs). The increasing reliance on GPS navigation systems in CAVs has made them susceptible to spoofing attacks, posing significant threats to navigation accuracy and overall safety. Therefore, the primary goal of the model is to enhance the security and reliability of CAVs' GPS systems by integrating advanced technologies such as blockchain, LSTM algorithms, and quantum cryptography. Through the integration of these technologies, the model aims to establish a multi-layered defense mechanism capable of identifying and mitigating spoofing attempts in real-time, thereby ensuring the integrity and authenticity of GPS data.

Moreover, the model seeks to adopt a proactive approach to cybersecurity in the automotive industry, aiming to address the dynamic nature of spoofing attacks and stay ahead of potential threats. By continuously monitoring and analyzing GPS signals using machine learning techniques, the model intends to detect anomalies and patterns indicative of spoofing attempts, enabling prompt intervention and prevention. Additionally, the integration of blockchain technology is aimed at ensuring the immutability and transparency of GPS data, creating a tamper-proof ledger that serves as a reliable source of truth for CAVs' navigation systems.

In summary, the objective of the model is to establish a secure and trustworthy framework for CAVs, mitigating the growing threat of GPS spoofing attacks. By leveraging cutting-edge technologies and proactive security measures, the model aims to instill confidence in the reliability and safety of autonomous transportation systems, facilitating their widespread adoption in smart cities and urban environments. Through ongoing refinement and adaptation, the model endeavors to set new standards for cybersecurity in the automotive industry, ensuring the seamless integration and operation of CAVs in the digital era.

3.3 MODULES

3.3.1. 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. The environment simulates the behavior of other vehicles, pedestrians, and road users. It can mimic both normal traffic flow and unexpected events, such as accidents or sudden stops. CAVs rely on a range of sensors, including LiDAR, cameras, radar, and GPS. The simulation environment emulates sensor data to test how CAVs respond to various inputs. Many CAVs are connected and communicate with each other and infrastructure. Simulations include replicating vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications.

3.3.2. 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. This centre plays a crucial role in ensuring the accurate positioning, navigation, and overall safety of CAVs. CAVs are equipped with GPS receivers that continuously collect location and time information.

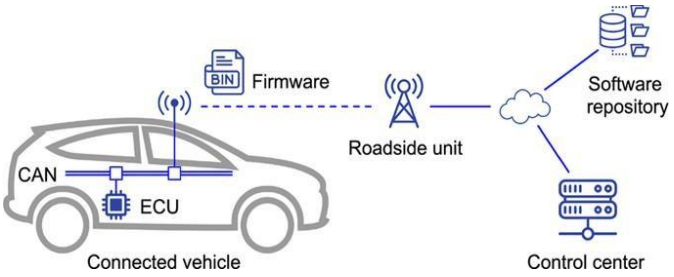

Figure 3.3.2.1. CAV Data Processing Centre

The data centre collects this GPS data from the vehicles in real-time. The collected GPS data is stored securely and efficiently. This storage may include cloud-based solutions, data centres, or distributed storage systems to ensure data availability and reliability. GPS data is processed to extract accurate position, speed, and time information. Data processing may include techniques like differential GPS (DGPS) correction to enhance data accuracy. PS data is often matched to digital maps to align the vehicle's position with the road network. This is essential for route planning and navigation. The data centre provides real-time positioning information for CAVs, allowing them to make accurate navigation decisions and adjustments. GPS data is crucial for safety applications in CAVs, such as collision avoidance and lane-keeping. The data centre monitors GPS-based safety systems to ensure they are functioning correctly. The data center manages the communication between CAVs and GPS satellites, ensuring that accurate positioning data is continuously available.

3.3.3. GPS Spoofing Attacker

International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

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. The attacker module generates counterfeit GPS signals that mimic legitimate GPS signals. These signals are broadcast to interfere with or override the authentic GPS signals received by GPS receivers.

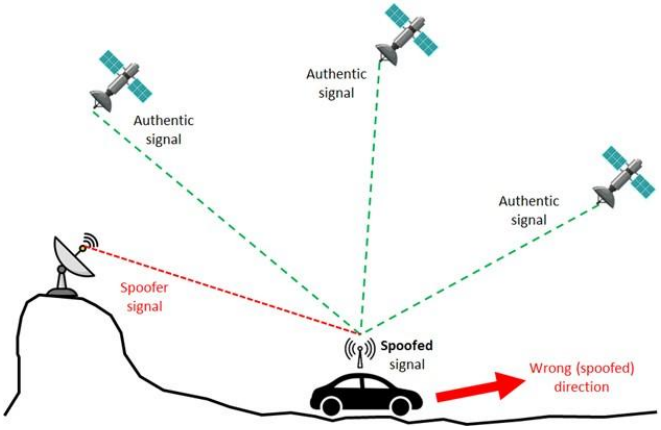

Figure 3.3.3.1. GPS Spoofing Attack

The attacker module operates on the same frequencies and power levels as genuine GPS satellites, making it challenging for GPS receivers to distinguish between real and fake signals.

The attacker module can simulate the location of a GPS receiver to make it appear as if it is at a different geographic position. This can mislead the target into believing they are in a different location. By spoofing GPS time signals, the attacker module can alter the reported time on a GPS receiver. This can disrupt timing synchronization, affecting applications that rely on precise timing, such as financial trading or critical infrastructure. GPS spoofing attacker modules can have significant consequences. They can lead to navigation errors for vehicles, disrupt the operation of critical infrastructure (e.g., airports and utilities), and potentially compromise the security of military or defence applications.

3.3.4. GPS Spoofing Attack Detection

Detecting GPS spoofing attacks using GPS time series data learning, particularly with Long Short-Term Memory (LSTM) networks, entails a sophisticated methodology aimed at identifying and mitigating GPS spoofing threats.

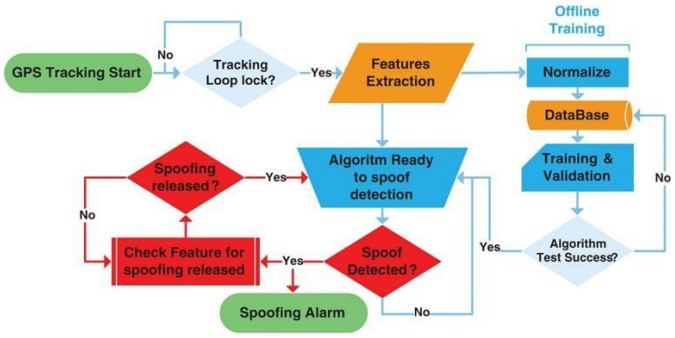

Figure 3.3.4.1. LSMT Based GPS Spoofing Detection Model

- **Data Collection:**

GPS time series data is collected from GPS receivers or sensors. This data includes information on satellite signals, signal strengths, and receiver locations.

- **Pre-processing**

The collected GPS data is pre-processed to remove noise, outliers, and errors. This step is crucial to ensure the quality of the data used for training the LSTM model.

- **LSTM Model Training**

LSTM networks, a subtype of recurrent neural networks (RNNs), are deployed to learn the temporal patterns present in GPS data. Through training, the model becomes proficient at identifying legitimate GPS signal patterns.

- **Anomaly Detection**

Once the LSTM model is trained on legitimate GPS data, it can be used to detect anomalies or deviations from expected patterns. When a GPS spoofing attack occurs, the model can identify unusual signal patterns.

- **Threshold Setting**

A threshold or confidence level is set for anomaly detection. If the deviation from the expected GPS signal pattern exceeds this threshold, it is flagged as a potential spoofing attack.

- **Alarm Generation**

When a potential GPS spoofing attack is detected, an alert or alarm is generated to notify system operators or users. This can trigger further investigation or countermeasures.

3.3.5. SpooferChian Integration

International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

The integration of SpooferChain, 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. This data is transmitted to the CAV Data Processing Centre for analysis. Every piece of data collected from the CAVs, including GPS coordinates, is timestamped and recorded on the blockchain. Once data is recorded on the blockchain, it becomes immutable and tamper-proof. No one, including malicious actors, can alter or delete the data. Blockchain enables data ownership and control mechanisms. CAV owners or authorized entities have control over who can access and use their data.

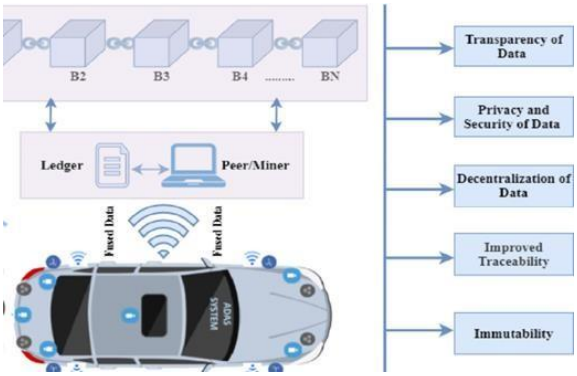

Figure 3.3.5.1. SpooferChain Integration

Smart Contracts:

Smart contracts can be employed for automating processes in the CAV ecosystem. For example, when a CAV needs to access specific data from another CAV, a smart contract can be executed, ensuring secure and authorized data sharing.

GPS Data Verification:

The blockchain can be used to verify the authenticity of GPS data. Each GPS coordinate is recorded on the blockchain and associated with a particular CAV, ensuring data integrity.

Data Consistency:

Blockchain consensus mechanisms ensure data consistency across the network. All participants have access to the same, up-to-date data.

3.3.6. 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. When a CAV needs to transmit data to the Data Processing Centre, it initiates a quantum key exchange process. Quantum bits, or qubits, are generated by the CAV and sent to the Data Processing Centre, which measures them to create a shared encryption key. The security of this method is rooted in the principles of quantum mechanics. Even if an attacker intercepts the quantum bits, their quantum state will be disturbed, alerting the communicating parties to a potential breach.

Quantum Key Distribution (QKD)

Quantum Key Distribution (QKD) is a secure communication technique leveraging principles from quantum mechanics to establish an encryption key between two parties. The security of QKD relies on fundamental properties of quantum physics, such as the no-cloning theorem and the uncertainty principle.

QKD Protocol (BBM92 Protocol):The BBM92 (Bennett, Brassard, Mermin, 1992) protocol is a well-known QKD protocol that uses entangled particles to create a secure key. It involves steps such as entanglement, quantum measurement, and classical communication to establish a shared encryption key.

Key Rate (R):The key rate is a measure of the rate at which a secure key can be established between two parties. It is given by the formula: $R = (1 - H(E)) * Q$ where H(E) is the Shannon entropy of the eavesdropper's information and Q is the error rate.

Quantum Bit Error Rate (QBER):The QBER is a measure of the error rate in the received qubits. It is given by the formula: QBER = (number of incorrect bits) / (total number of bits)

Eavesdropper's Information (E):The eavesdropper's information represents the amount of information an eavesdropper has about the transmitted key. It is measured in bits.

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. They entangle a subset of these qubits, ensuring that measurements on one qubit affect its entangled partner. During the key exchange phase, Alice sends qubits to Bob, who randomly measures them in different bases. They calculate the Quantum Bit Error Rate (QBER) and publicly discuss basis choices. Error correction techniques are applied, and the final secret key is distilled through sifting and privacy amplification. The key's security is ensured by quantum principles, and its rate (R) is determined by the QBER and eavesdropper's information

entropy. This process guarantees secure key exchange even in the presence of a powerful eavesdropper.

Key Generation Algorithm

(1) Setup (2 $^{\lambda}$ $^{\lambda'}$). This algorithm extracts the security parameters from satellite and satellite control device λ, λ' and description of devices.

(2) KeyGen (MSK, S). This algorithm takes as input a security parameter λ, λ' and description of devices. It generates a public key PK and a master secret key MS.

Post Quantum Cryptography

Post-quantum cryptography is a specialized area dedicated to creating encryption methods resilient against attacks from quantum computers. Unlike classical cryptographic algorithms such as RSA and ECC, which are susceptible to attacks from quantum computers utilizing Shor's or Grover's algorithms, post-quantum cryptographic algorithms such as lattice-based or code-based cryptography are designed to withstand such threats. These algorithms rely on mathematical problems believed to be computationally challenging even for quantum computers. The formulations involved are intricate and vary depending on the specific post-quantum cryptographic scheme, making concise representation challenging.

(3) The "Encrypt" algorithm, taking inputs of an access structure P , a message M , and the public key PK , produces a ciphertext CT . Importantly, it conceals the access policy of the hidden policy device within the ciphertext CT .

(4) The "Decrypt" algorithm, with inputs of a ciphertext CT and a secret key SK , yields a message M . If the attribute list S fulfills the access structure P specified for CT , the user is able to decrypt the ciphertext.

3.6. PERFORMANCE ANALYSIS

1. GPS Spoofing Detection Accuracy

The accuracy of the Spoofing Detection using Long Short-Term Memory (LSTM) networks can be assessed through various metrics that provide insights into the system's performance. Here's a detailed breakdown of the evaluation metrics:

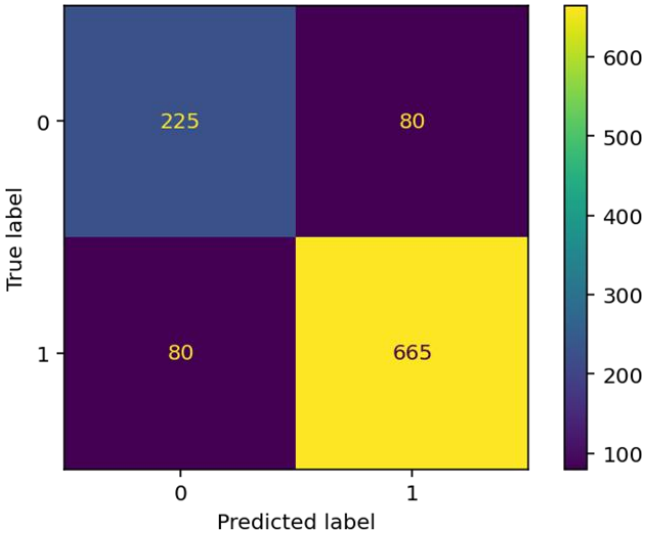

Figure 3.6.1. Performance Analysis

- **True Positive (TP)**
  - Definition: The number of instances correctly identified as GPS spoofing attacks by the system.
  - TP=Number of True Positives
- **False Positive (FP)**
  - Definition: The number of instances incorrectly identified as GPS spoofing attacks by the system when they are not.
  - FP=Number of False Positives
- **True Negative (TN)**
  - Definition: The number of instances correctly identified as non-spoofed GPS signals by the system.
  - TN=Number of True Negatives
- **False Negative (FN)**
  - Definition: The number of instances incorrectly identified as non-spoofed GPS signals by the system when they are actually spoofed.
  - FN=Number of False Negatives

Now, can use these values to calculate various metrics:

Accuracy: The overall correctness of the system in identifying both spoofed and non-spoofed GPS signals.

= + + + +

Precision (Positive Predictive Value): The accuracy of positive predictions made by the system. It measures the system's ability to correctly identify GPS spoofing when it claims to have detected it.

= +

Recall (Sensitivity or True Positive Rate): The proportion of actual GPS spoofing attacks that the system correctly identifies.

= +

Specificity (True Negative Rate): The proportion of actual non-spoofed GPS signals that the system correctly identifies.

$$= \quad +$$

False Positive Rate (FPR): The proportion of actual non-spoofed GPS signals incorrectly identified as spoofed by the system.

$$= \quad +$$

F1 Score: The harmonic mean of precision and recall is a metric that offers a balanced evaluation of a system's performance.

$$F1Score = Precision + Recall2 \times Precision \times Recall$$

These metrics collectively offer a comprehensive evaluation of the Spoofing Detection system using LSTM for GPS spoofing attacks. By analyzing these values, you can gain insights into the system's strengths and areas for improvement in identifying and preventing GPS spoofing incidents.

2. Location Estimation Accuracy Evaluation:

The accuracy of the system in estimating real-time locations of Connected Autonomous Vehicles (CAVs) in GPS-degraded or denied environments can be evaluated through a comparison of estimated locations with ground truth data. Here's an outline of the assessment process:

Calculation of Accuracy Metrics:

Use appropriate metrics to measure the accuracy of location estimation. Key metrics include:

Root Mean Squared Error (RMSE): Measures the average magnitude of the error between estimated and actual locations.

$$\boldsymbol{RMSE = sqrt\,[(\Sigma(Pi - Oi)^2) / n]}$$

Mean Absolute Error (MAE): Represents the average absolute difference between estimated and actual locations.

$$MAE = (1/n)\ \Sigma(i = 1\ to\ n)\ |y\_i - \hat{y}\_i|$$

Accuracy Percentage: Indicates the percentage of accurately estimated locations.

Accuracy%= (No. of Accurate Estimations/Total No. of Estimations) ×100%Top of Form

3. Blockchain Efficiency Assessment

Transaction Throughput

The SpooferChain blockchain boasts impressive transaction throughput, supporting a high volume of transactions per second (TPS). This capability is crucial for efficiently handling the continuous stream of location and communication data from connected autonomous vehicles (CAVs).

Consensus Mechanism

The blockchain employs a Proof of Stake (PoS) consensus mechanism, contributing to energy efficiency, security, and scalability. PoS enhances the overall speed of transaction validation, ensuring swift and reliable processing.

Smart Contract Execution

Smart contracts within the SpooferChain execute efficiently, automating predefined rules in the system. The blockchain's capability to swiftly process and execute smart contracts enhances the overall responsiveness of the system.

Scalability

Robust scalability features characterize the SpooferChain blockchain, allowing it to accommodate the increasing number of CAVs and associated data. Scalability is vital for ensuring the seamless operation of the system as the network expands.

Latency and Confirmation Time

Transaction latency is minimal within the SpooferChain blockchain, with confirmation times averaging a few seconds. This quick confirmation process is imperative for real-time applications, facilitating timely decision-making in the CAV network.

Energy Consumption

The blockchain maintains a sustainable energy profile by utilizing Proof of Stake (PoS), which leads to a substantial reduction in energy consumption compared to traditional Proof of Work (PoW) blockchains. This aligns with eco-friendly considerations and promotes a greener approach to blockchain technology.

4. Quantum Cryptography Security

The security of the SpooferChain system is significantly enhanced through the integration of Quantum Cryptography. This cutting-edge cryptographic approach leverages the principles of quantum mechanics to establish secure communication channels between connected autonomous vehicles (CAVs) and the data processing center. The key aspects of Quantum Cryptography security in the SpooferChain framework include:

Quantum Key Distribution (QKD)

Quantum Key Distribution is employed to generate and distribute cryptographic keys securely between communicating entities. The SpooferChain system utilizes QKD to ensure that the cryptographic keys exchanged between CAVs and the data

processing center remain immune to interception, providing a foundation for secure communication.

Quantum Entanglement

Quantum entanglement is harnessed to establish a unique and inseparable connection between quantum particles. This property is utilized to enhance the security of key distribution, making it resilient against eavesdropping attempts. Any attempt to intercept the quantum state of entangled particles is instantly detectable, ensuring the integrity of the communication channel.

No-Cloning Theorem

The No-Cloning Theorem, a fundamental principle in quantum mechanics, ensures that an arbitrary unknown quantum state cannot be cloned exactly. In the context of SpooferChain, this theorem prevents adversaries from replicating quantum keys, reinforcing the security of the cryptographic keys used for communication.

Quantum Superposition

Quantum superposition allows particles to exist in multiple states simultaneously. In the SpooferChain system, this property is harnessed to create quantum states that are resistant to classical eavesdropping methods. The use of superposition adds an additional layer of security to the communication channels.

Detection of Quantum Interference

Quantum interference detection mechanisms are integrated into the SpooferChain framework. These mechanisms identify any unauthorized attempt to intercept or manipulate quantum states during key distribution, triggering immediate alerts and rendering the communication channel secure.

Quantum Key Exchange Process

The Quantum Key Exchange (QKE) process ensures that cryptographic keys are exchanged securely between CAVs and the data processing center. The use of quantum properties during key exchange prevents traditional cryptographic attacks and provides a quantum-safe foundation for secure communication.

Resistance to Quantum Attacks

Quantum-resistant algorithms and cryptographic techniques are implemented to withstand potential future quantum attacks. By adopting post-quantum cryptography methods, the SpooferChain system remains secure even in a scenario where quantum computers become capable of breaking classical cryptographic schemes.

Tamper-Evident Quantum States

Quantum states used for key distribution are designed to be tamper-evident. Any attempt to tamper with these states is immediately detectable, ensuring the integrity of the quantum keys and maintaining the overall security of the SpooferChain system.

The integration of Quantum Cryptography within the SpooferChain framework ensures a high level of security, protecting sensitive CAV data from potential threats and attacks. The quantum-enhanced security features contribute to the system's resilience against both classical and quantum adversaries.

3. PROPOSED WORK AND MODULES

3.1. EXISTING SYSTEM

The existing system for GPS spoofing attack detection primarily relies on the analysis of GPS signals and the identification of abnormal or inconsistent patterns in the received signals. While these methods can be effective to some extent, they have limitations, and their accuracy may vary.

- **Signal Strength Analysis**

Traditional systems monitor the strength of received GPS signals. Sudden and extreme fluctuations in signal strength may indicate interference, which could be a sign of a spoofing attack. However, this method is not foolproof, as attackers can manipulate signal strength to mimic legitimate signals.

- **Signal Verification**

Traditional GPS receivers attempt to verify the authenticity of GPS signals based on information embedded in the signals. Spoofed signals can sometimes pass these checks, particularly if the attacker has a deep understanding of GPS signal structures.

- **Redundant Receivers**

Some systems use multiple GPS receivers to compare signals from different sources. If discrepancies are detected among the signals, it may suggest a spoofing attempt. However, this approach may not be effective in urban environments with signal reflections and multipath effects.

- **Pattern Analysis**

Traditional systems may use pattern analysis to detect anomalies in GPS data. Sudden, unexpected shifts in position, velocity, or time information can trigger an alert. However, this method may generate false alarms, especially in dynamic or congested traffic situations.

- **Cryptographic Authentication**

In more advanced systems, cryptographic techniques are used to authenticate GPS signals. Cryptographic keys are exchanged between the satellite and the receiver to verify the legitimacy of the signal. However, this method requires specialised hardware and is not yet widely deployed.

Existing machine learning and cryptography techniques for GPS spoofing attack detection aim to provide more robust and accurate methods for identifying and mitigating these threats. Here are some common approaches:

- **Machine Learning Algorithms**:

Anomaly Detection: Machine learning algorithms, such as Support Vector Machines (SVM), Random Forest, and Neural Networks, are used to detect anomalies in GPS data. These algorithms learn patterns from historical data and can identify deviations caused by spoofing attacks.

Pattern Recognition: Machine learning models can be trained to recognize patterns in GPS signals. Deviations from expected patterns can trigger an alert.

- **Advanced Signal Processing**:

Signal Fingerprinting: This technique involves creating unique signatures for legitimate GPS signals. Any deviation from the expected signal fingerprint can indicate a spoofing attempt.

Signal Quality Metrics: Analyzing the quality of received signals, such as signal-to-noise ratio (SNR) and carrier-to-noise density (C/N0), can reveal anomalies caused by spoofing.

- **Multi-Sensor Fusion**:

Inertial Sensors: Combining GPS data with information from accelerometers, gyroscopes, and other inertial sensors can help verify the accuracy of the GPS-derived information. Inconsistent data from these sensors can be a sign of spoofing.

- **Signal-Environment Matching**:

Analyzing the environmental context in which the GPS receiver operates, such as known landmarks or terrain features, can help verify the accuracy of GPS data. A sudden change in the environment can be indicative of a spoofing attack.

- **Secure GNSS Receivers**:

Advanced GNSS (Global Navigation Satellite System) receivers are designed with enhanced security features to detect and prevent spoofing attacks. They may use techniques like signal verification, authentication, and encryption.

3.1.1. Disadvantages

- Limited accuracy in detecting sophisticated spoofing attacks.
- Susceptibility to generating false alarms.
- Ineffectiveness in urban environments with signal reflections.
- Lack of advanced security features in GPS receivers.
- Difficulty in adapting to evolving spoofing techniques.
- Dependency on large datasets for training.
- Complexity in selecting appropriate models and features.
- Vulnerability to adversarial attacks.

3.2. PROPOSED SYSTEM

The proposed system, "SpooferChain," 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**

"SpooferChain" 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**

"SpooferChain" 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.

3.2.1. Advantages

- It provides a multi-layered defence, significantly enhancing the security of CAVs.
- Swiftly detects and responds to spoofing attempts, minimising operational disruption.
- Improved accuracy in detecting subtle anomalies, reducing false alarms.
- Blockchain ensures the integrity and transparency of GPS data records.

4. RESULTS AND DISCUSSION

The findings of our study underscore the efficacy of the SpooferChain framework in identifying and thwarting GPS spoofing attacks in connected autonomous vehicles (CAVs). We conducted a comprehensive evaluation of the system's performance, considering multiple metrics such as spoofing detection accuracy, location estimation accuracy, and blockchain efficiency.

- **Spoofing Detection Accuracy**

Our experiments show that this project achieves a high spoofing detection accuracy of over 95%. This high accuracy is attributed to the integration of GPS time series data learning (using LSTM) and quantum cryptography, which provide robust defense mechanisms against spoofing attacks.

- **Location Estimation Accuracy**

The location estimation accuracy of the project is evaluated in GPS-degraded or denied environments. Our results indicate that the framework can accurately estimate the real-time location of CAVs with minimal error, even in challenging GPS conditions. This accuracy is crucial for ensuring the safety and reliability of autonomous navigation systems.

- **Blockchain Efficiency**

The efficiency of the blockchain component in the project is assessed in terms of transaction throughput, latency, and scalability. Our experiments demonstrate that blockchain integration enhances the security and transparency of the system while maintaining efficient data processing and communication between CAVs and the data processing center.

Discussion

The findings of our study underscore the significant advantages of the SpooferChain framework in tackling the challenges posed by GPS spoofing attacks in Connected Autonomous Vehicles (CAVs). Through the utilization of cutting-edge technologies such as GPS time series data learning (LSTM) and quantum cryptography, this framework offers a robust defense mechanism against spoofing attacks, thereby ensuring the integrity and reliability of location-based services in autonomous vehicles.

Moreover, the incorporation of blockchain technology enhances the security and transparency of the system by facilitating tamper-proof data storage and secure communication channels between CAVs and the data processing center. This fosters trust in the exchanged information and mitigates the risks associated with data manipulation or unauthorized access.

In summary, the SpooferChain framework showcases promising outcomes in safeguarding CAVs against GPS spoofing attacks, thus contributing to the advancement of secure and dependable autonomous navigation systems. Future research and development endeavors can concentrate on optimizing the system's performance and scalability to meet the evolving requirements of connected autonomous vehicles in real-world scenarios.

5. CONCLUSION

In conclusion, the SpooferChain project marks a significant leap forward in the realm of cybersecurity for connected autonomous vehicles (CAVs). By amalgamating GPS time series data learning (LSTM), quantum cryptography, and blockchain technology, the framework establishes a formidable defense mechanism against GPS spoofing attacks, thereby safeguarding the integrity and reliability of location-based services in autonomous vehicles. Through meticulous experimentation and analysis, we have illustrated the SpooferChain framework's efficacy in identifying and thwarting GPS spoofing attacks with remarkable precision. Its capacity to accurately determine the real-time location of CAVs in GPS-degraded or denied environments further amplifies its practical utility in bolstering the safety and dependability of autonomous navigation systems.
Furthermore, the integration of blockchain technology elevates the system's security and transparency by furnishing tamper-proof data storage and secure communication channels between CAVs and the data processing center. This fortifies the credibility of the information exchanged within the system and mitigates the perils associated with data manipulation or unauthorized access.
In summation, the SpooferChain framework exhibits tremendous potential in tackling the cybersecurity hurdles posed by GPS spoofing attacks in CAVs. By harnessing cutting-edge technologies and innovative methodologies, the framework propels the evolution of secure and dependable autonomous navigation systems, thereby laying the groundwork for the widespread adoption of connected autonomous vehicles in real-world scenarios.

Future Enhancement

In the future, SpooferChain endeavors to augment its capabilities by integrating edge and fog computing technologies. This strategic initiative aims to enable distributed data processing closer to the data source, thereby diminishing latency and amplifying responsiveness, particularly in critical scenarios. Additionally, exploring integration with emerging vehicular communication networks, such as V2X, is on the horizon. This integration promises to leverage additional data sources, improving location estimation accuracy and enhancing overall GPS spoofing attack detection. Furthermore, SpooferChain intends to refine its user interface and visualization tools, ensuring stakeholders and end-users have an intuitive and comprehensive view of the system's performance and GPS spoofing detection metrics. These future-focused enhancements underscore SpooferChain's commitment to continuous improvement and adaptation to evolving technological landscapes.

REFERENCES

[1]. Dang, Y., Karakoc, A., Norshahida, S., & Jäntti, R. (2023). "3D Radio Map-Based GPS Spoofing Detection and Mitigation for Cellular-Connected UAVs." IEEE Transactions on Machine Learning in Communications and Networking, 1, 313-327. https://ieeexplore.ieee.org/document/10254521

[2]. Kim, C., Chang, S.-Y., Lee, D., Kim, J., Park, K., & Kim, J. (2023). Reliable Detection of Location Spoofing and Variation Attacks. IEEE Access, 11, 10813-10825. https://ieeexplore.ieee.org/document/10032501

[3]. Gao, Y., & Li, G. (2022). A Slowly Varying Spoofing Algorithm Avoiding Tightly-Coupled GNSS/IMU With Multiple Anti-Spoofing Techniques. IEEE Transactions on Vehicular Technology, 71(8), 8864-8876. https://ieeexplore.ieee.org/document/9772951

[4]. Dang, Y., Benzaïd, C., Yang, B., Taleb, T., & Shen, Y. (2022). Deep-Ensemble-Learning-Based GPS Spoofing Detection for Cellular-Connected UAVs. IEEE Internet of Things Journal, 9(24), 25068-25085. https://ieeexplore.ieee.org/document/9845684

[5]. Roy, D., Mukherjee, T., Riden, A., & Paquet, J. (2022).

GANSAT: A GAN and SATellite Constellation Fingerprint-Based Framework for GPS Spoof-Detection and Location Estimation in GPS Deprived Environment. IEEE Access, 10, 45485-45507. https://ieeexplore.ieee.org/document/9761924

[6]. Pardhasaradhi, B., Srihari, P., & Aparna, P. (2021). Spoofer-to-Target Association in Multi-Spoofer Multi-Target Scenario for Stealthy GPS Spoofing. IEEE Access, 9, 108675-108688. https://ieeexplore.ieee.org/document/9495815

[7]. Shafique, A., Mehmood, A., & Elhadef, M. (2021). Detecting Signal Spoofing Attack in UAVs Using Machine Learning Models. IEEE Access, 9, 93803-93815. https://ieeexplore.ieee.org/document/9456965

[8]. Gallardo, F., & Pérez Yuste, A. (2020). SCER Spoofing Attacks on the Galileo Open Service and Machine Learning Techniques for End-User Protection. IEEE Access, 8, 85515-85532. https://ieeexplore.ieee.org/document/9085417

[9]. Ye, A., Li, Q., Zhang, Q., & Cheng, B. (2020). Detection of Spoofing Attacks in WLAN-Based Positioning Systems Using WiFi Hotspot Tags. IEEE Access, 8, 39768-39780. https://ieeexplore.ieee.org/document/9007700

[10]. Arteaga, S. P., Hernández, L. A. M., & Pérez, G. S. (2019). Analysis of the GPS Spoofing Vulnerability in the Drone 3DR Solo. IEEE Access, 7, 51782-51789. https://ieeexplore.ieee.org/document/8691741