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.

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. By amalgamating these elements into the SpooferChain framework, the project aims to provide a holistic and resilient defense against location spoofing attacks on CAVs. It will ensure the safety and the proper functioning of autonomous vehicles and also paves the way for a more secure and trustworthy environment for CAVs in the future.