Detection of Multiple Small Biased GPS Spoofing Attacks on Autonomous Vehicles

1st Ahmad Mohammadi
Electrical and Computer Engineering
North Carolina A&T State University
Greensboro, USA
amohammadi@aggies.ncat.edu

2nd Vahid Hemmati
Electrical and Computer Engineering
North Carolina A&T State University
Greensboro, USA
vhemmati@ncat.edu

3rd Reza Ahmari
Computer Science
North Carolina A&T State University
Greensboro, USA
rahmari@aggies.ncat.edu

4th Frederick Owusu-Ambrose
Electrical and Computer Engineering
North Carolina A&T State University
Greensboro, USA
fowusuambrose@aggies.ncat.edu

5th Mahmoud Nabil Mahmoud
Electrical and Computer Engineering
North Carolina A&T State University
Greensboro, USA
mnmahmoud@ncat.edu

6th Abdollah Homaifar
Electrical and Computer Engineering
North Carolina A&T State University
Greensboro, USA
homaifar@ncat.edu

2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC) | 979-8-3315-1888-2/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICAIC63015.2025.10849307

***Abstract*—This paper introduces an algorithm designed to detect GPS spoofing attacks in Autonomous Driving Systems (ADS). The algorithm combines data from in-vehicle sensors, including the speedometer and gyroscope. This data is then fed into a Deep Neural Network (DNN) to predict the vehicle's displacement between timestamps. These predictions are continuously compared with GPS-provided displacement and velocity to detect the turn-by-turn, stop, and overshoot GPS spoofing attacks. Also, the same data is processed through an analytical model that uses the vehicle's dynamic movement equations to compute its position and velocity and to juxtapose them with GPS-provided position and velocity to detect the aforementioned spoofing attacks. A threshold is predetermined by using clean datasets to calculate the maximum possible deviation between in-vehicle sensor and GPS provided position/displacement and speed. Subsequently, spoofing attack detection uses this threshold for its continuous, real time comparison. Additionally, the proposed algorithm is able to detect a sequence of multiple biased attacks that fall below the mentioned threshold but can create a large deviation between the position/displacement and speed provided by GPS and Inertial Measurement Unit (IMU). To validate the effectiveness of the work, datasets simulating four distinct spoofing scenarios such as turn-by-turn, overshoot, stop and multiple biased attacks were generated using real-world data from [1]. The analyses shows that the Data-driven model successfully identifies the turn-by-turn, stop, overshoot and multiple biased spoofing attacks with the accuracies of 100%, 99.95%, 99.91%, 97.83%, respectively.**

***Index Terms*—GPS Spoofing Attack, Autonomous Vehicle (AV), cybersecurity, Data-Driven**

I. Introduction

The increasing use of Automated Driving Systems (ADS), also known as Autonomous Vehicles (AV), has significantly improved safety, security, and convenience for civilian use. However, this has also introduced challenges, including various attacks and unauthorized access, since ADS rely on multiple sensors for situational awareness [2]–[4]. One of the most critical challenges facing ADS is the threat of spoofing attacks on their Global Navigation Satellite System (GNSS) receivers [5]–[9]. Spoofing attacks transmit fake signals to deceive the AV's GNSS receiver and lead to erroneous positioning and navigation decisions. The consequences of successful spoofing attacks can be severe, ranging from potential catastrophic accidents to minor inconveniences like route deviations. The peril posed by spoofing attacks stems from their capacity to distort an AV's environmental perception. Simple spoofing attacks, such as feeding false location and trajectory data to an AV's onboard systems, can lead to critical errors like sudden lane changes or incorrect turns [10]–[13]. However, the threat escalates with advanced spoofing techniques, including turn-by-turn, stop and overshoot attacks [14]. The GNSS receiver of a target AV is taken over by a spoofer in turn-by-turn attack, causing a shift in the AV's position to make the navigation system recalculate the trajectory to the destination based on the spoofed positioning data. The AV then follows this incorrect trajectory and ends up in an wrong destination instead of the intended one [14], [15]. If a vehicle is stopped, for example at a stoplight, and its GPS signal is compromised to indicate movement along the road, a stop attack is mounted. This can cause the vehicle to have an accident or make an incorrect turn when the light turns green [16]. In the case of an overshoot attack, the GPS signal of the target vehicle is manipulated to show that it is stopped while it is actually moving on the road [16]. This can cause the vehicle to either have an accident or make a wrong turn, especially at forks in the road. These sophisticated maneuvers further compromise the AVs' decision-making processes, amplifying risks to passengers, other road users, and overall road safety [7], [14], [17]–[20]. Consequently, these malicious activities not only endanger lives but also erode public trust in AV technology, emphasizing

This research is supported by the University Transportation System (UTC), USA through grant number 69A3552348327. Also, this work is partially supported by (the NASA-ULI under Cooperative Agreement Number 80NSSC20M0161.

the urgent need for robust countermeasures and detection mechanisms.

While significant efforts have been made to develop robust security measures for AVs, including anti-spoofing algorithms and sensor fusion techniques [6], [14], [21]–[25], the field still faces several *critical gaps and challenges*. Existing anti-spoofing technologies often struggle to detect sophisticated spoofing attacks that mimic genuine GNSS signals closely. Moreover, if the attack's nature is more stealthy, mounted in a series of multiple small scale biased steps, it is extremely challenging to differentiate between legitimate and spoofed signals accurately.

In this context, this paper contributes to the ongoing research efforts by proposing an approach for detecting both advanced spoofing attacks and series of multiple biased attacks that are much smaller than a system threshold and thus difficult to detect. In this paper, we first introduce approaches of detecting anomaly in GNSS data based on analytical and Machine Learning (ML) methods to predict the displacement based on IMU and juxtapose them with GNSS derived displacement. We then discuss multiple biased attacks with magnitudes smaller than system threshold value. By addressing key limitations in existing methods and leveraging advancements in machine learning and sensor fusion, the proposed solution seeks to enhance the resilience of AVs against malicious spoofing attacks, thereby advancing the safety and reliability of autonomous transportation systems.

The remainder of this study is organized as follows: Section II describes how this work contributes to innovation. Section III reviews the existing spoofing attack detection methods and identifies gaps in the current research. Section IV highlights the proposed methodology. Section V presents the results of spoofing attack detection. Section VI summarizes the work, and section VII gives a brief future direction of the work.

II. Contributions of this study

This study makes notable contributions to the domain of GPS spoofing attack detection by leveraging in-vehicle sensor data. First, it introduces a novel Data-Driven framework that fuses data from multiple sensors, including speedometer and gyroscope, to predict displacement at future timestamps via a Deep Neural Network (DNN) architecture. This innovative approach effectively identifies potential spoofing attacks by contrasting predicted displacements with those derived from GPS data, thereby addressing issues related to safety and security of ADS. Second, the major novelty of this study is high accuracy in detecting multiple biased stealthy attacks that remain below predefined system thresholds that is not addressed by any of the current studies. The framework reliably distinguishes between authentic and spoofed samples by harnessing the characteristics of the Gaussian distribution that 99.73% of samples lie within three standard deviations (STD) from the mean value. Furthermore, the framework undergoes rigorous validation against four distinct types of attacks, underscoring its practical efficacy. Lastly, a comparative analysis between the proposed Data-Driven framework and a traditional analytical approach demonstrates the superiority of the Data-Driven method in terms of accuracy and efficiency in detection of various spoofing scenarios. Collectively, these contributions significantly advance the field of GPS spoofing detection, offering improved reliability and applicability in real-time contexts.

III. Literature Review

Spoofing attack detection techniques for GNSS receivers fall into five types: (i) encryption-based techniques, (ii) codeless cross-correlation methods, (iii) analysis of signal statistics , (iv) approaches based on antenna [26], and (v) machine learning (ML)-based strategies. Encryption-based anti-spoofing algorithms are used in the military to safeguard GNSS receivers. However, due to their high computational expenses, these algorithms are not economical for use in AVs. Additionally, the implementation of such security measures may require specialized hardware that can further escalate the overall cost of vehicle systems. Codeless cross-correlation techniques detect spoofing by analyzing the correlation between encrypted GPS L1 P(Y) codes from a number of receivers [27], [28]. While effective, the method's success hinges on the availability of expensive instrumentation, thus increasing the complexity of signal processing as the number of receivers grows and making it economically expensive for the AVs. Signal statistics analysis for spoofing detection leverages characteristics such as strength received signal [29], spatial coherence [30], pseudorange measurements, arival time, and signal parameter estimation. This method relies on identifying deviations from expected signal characteristics to flag potential spoofing incidents. However, it may struggle to differentiate between sophisticated spoofing attacks and natural signal fluctuations, potentially leading to either false positives or missed detections. Moreover, this technique requires a baseline of 'normal' signal behavior, which can vary significantly in complex environments where AVs operate. Spoofing detection using multiple GNSS antennas relies on bit carrier-phase measurements [31], but this method demands high computational resources and complex antenna setups for precise detection. [26], [32]. Alternatively, GNSS spoofing is detectable by a comparison between IMU-measured acceleration with GNSS-derived acceleration [33], though this technique is less effective for AVs because of their restricted dynamic range. Positioning from IMU (accelerometer and gyroscope) and GNSS is compared in [14], [34], [35] to detect spoofing attack.

Machine learning (ML) and deep learning (DL) techniques have emerged as effective tools for detecting GNSS spoofing. For instance, [36] employs a Support Vector Machine (SVM) to estimate the state and detect spoofing in unmanned aerial vehicles, while [37] uses classifiers like K-Nearest Neighbor (KNN) and Naïve Bayes to identify spoofing based on features such as early-late phase, delta, and signal levels. Additionally, [14] utilizes DL-based neural networks to predict step-by-step location shifts using in-vehicle sensors, detecting spoofing by comparing these predictions with GNSS-provided locations.

Although all the above mentioned and some other existing techniques [6], [14], [14], [21], [24] can detect both simple and advanced spoofing attacks, no research has been conducted to more stealthy spoofing attacks that are mounted in an iterative or step-by-step manner on the system. Therefore, the field still faces a critical challenge in the face of multiple biased spoofing attacks. In other words, if the attack mounted in a series of multiple small scale biased steps, it is extremely challenging to differentiate between legitimate and spoofed signals accurately.

IV. Proposed Methodology

This section provides both analytical and Data Driven GPS spoofing detecting algorithms.

A. Analytical GPS Spoofing Detection Algorithm

To continuously compare IMU and GPS data in attack detection, two distinct sources of speed and position are required. Consequently, vital data parameters such as latitude, longitude, yaw rate, and speed are used. The perceived displacement from GPS, indicating the distance traversed between timestamps, is then computed utilizing the Haversine displacement as in 1 [38]:

$$disp_h = 2r\sin^{-1}\left(\sqrt{\sin^2\left(\frac{\Delta\phi}{2}\right) + \cos(\phi_1)\cos(\phi_2)\sin^2\left(\frac{\Delta\psi}{2}\right)}\right) \tag{1}$$

where:

$disp_h$ is the distance between two points on the Earth's surface (m)

r is the Earth's radius (6378 km)

$\Delta\phi = \phi_2 - \phi_1$ is the difference in latitudes (rad)

$\Delta\psi = \psi_2 - \psi_1$ is the difference in longitudes (rad)

Additionally, GPS provided speed is calculated by dividing the perceived displacement by time as in equation 2.

$$S_{GPS}(t) = \frac{disp_h(t)}{\Delta t} \tag{2}$$

where $S_{GPS}(t)$ is the GPS derived speed at time t, $disp_h(t)$ is the Haversine displacement at time t, Δt is the time.

Figure1(a) illustrates the analytical framework for GPS spoofing attack detection, which is partly based on the spoof detection architecture outlined in [14], [39], [40]. Clean data from two sources, in-vehicle sensors and the GPS receiver, is utilized to calculate the vehicle's speed and position at each step. The maximum difference between GPS and IMU speed and position are considered as the error thresholds. Once the speed and position thresholds are defined, a continuous comparison is made between these thresholds and each new data point to detect values greater than threshold as anomalous and classify them into different attacks types using GPS and IMU-provided speed and position. Upon detecting an anomaly, speed values from GPS and the speedometer are used to classify the anomaly into overshoot and stop attacks, respectively, while position information is used for classifying anomalies into turn-by-turn attacks. Thus, precise vehicle speed and position should be calculated based on the data from GPS and IMU. The following steps outline the process of determining position and the two thresholds:

First, input data from sensors is acquired, and yaw angle is calculated by integrating the angular velocity (yaw rate) as in equation 3:

$$\psi(t) = \int_{t_0}^{t} \omega(t)\, dt \tag{3}$$

where $\psi(t)$ and $\omega(t)$ are the yaw angle (rad) and the yaw rate (rad/s) at time t, respectively. t_0 and t are the previous and current time steps.

Second, velocities in both direction (x,y) are calculated by using speed and $\psi(t)$ as in equation 4:

$$\begin{aligned} V_x(t) &= S_{IMU} \cdot \cos(\psi) \\ V_y(t) &= S_{IMU} \cdot \sin(\psi) \end{aligned} \tag{4}$$

where $V_x(t)$, $V_y(t)$ and S_{IMU} are the x-y components of velocity and vehicle speed at time t, respectively.

Third, displacements in both direction are then calculated as in equation 5:

$$\begin{aligned} dispx_{IMU}(t) &= V_x(t) \cdot \Delta t \\ dispy_{IMU}(t) &= V_y(t) \cdot \Delta t \end{aligned} \tag{5}$$

where $dispx_{IMU}(t)$, $V_x(t)$ and $dispy_{IMU}(t)$, $V_y(t)$ are the displacement and velocity in the x-y directions, respectively. Δt is the time step between consecutive time stamps.

Fourth, positions in both direction are then calculated and in equation 6:

$$\begin{aligned} X_{IMU}(t) &= dispx_{IMU}(t) + X_{IMU}(t - \Delta t) \\ Y_{IMU}(t) &= dispy_{IMU}(t) + Y_{IMU}(t - \Delta t) \end{aligned} \tag{6}$$

where $X_{IMU}(t)$, $Y_{IMU}(t)$ are the x-y components of position at time t, respectively and $X_{IMU}(t - \Delta t)$ and $Y_{IMU}(t - \Delta t)$ are positions at the previous time step.

Fifth, GPS-derived position is converted from latitude and longitude to UTM coordinates relative to the starting point, also GPS-derived speed is calculated by equation 1.

Sixth, position and speed errors are then calculated using equation 7:

$$\begin{aligned} &X_{\text{error}}(t) = X_{IMU}(t) - X_{GPS}(t), \\ &Y_{\text{error}}(t) = Y_{IMU}(t) - Y_{GPS}(t), \\ &EUC_{\text{error}}(t) = \sqrt{(X_{\text{error}}(t))^2 + (Y_{\text{error}}(t))^2}, \\ &S_{\text{error}}(t) = S_{IMU}(t) - S_{GPS}(t). \end{aligned} \tag{7}$$

where $X_{\text{error}}(t)$, $Y_{\text{error}}(t)$, $EUC_{\text{error}}(t)$ are the x, y and Euclidean error at time t, and $S_{\text{error}}(t)$ is the speed error at time t.

Seventh, error thresholds for speed and position are established to account for maximum deviation between in-vehicle sensors and GPS (see equation (8)):

$$\begin{aligned} \delta_x &= \max\left(|X_{\text{error}}(t)|\right) \\ \delta_y &= \max\left(|Y_{\text{error}}(t)|\right) \\ \delta_{EUC} &= \max\left(|E_{\text{error}}(t)|\right) \\ \delta_s &= \max\left(|S_{\text{error}}(t)|\right) \end{aligned} \tag{8}$$

where: δ_x, δ_y, δ_{EUC} are the x, y and Euclidean error thresholds, and δ_s is the speed error threshold.

To ensure the system can detect any anomaly created by manipulation of GPS-provided position/displacement or speed, the thresholds (δ_{EUC},δ_s) are considered as the maximum deviation/error values between GPS and IMU on clean datasets. An

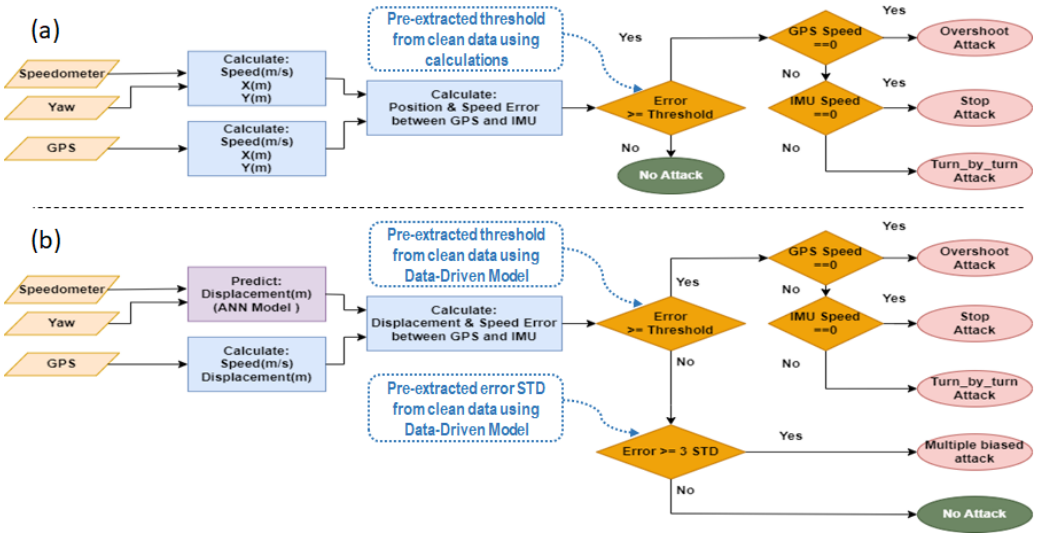

Fig. 1. (a) Analytical GPS Spoofing Detection Algorithm: uses position and speed threshold for anomaly detection. Stop/overshoot and turn-by-turn attacks are detected by speed and position monitoring (b) Data-Driven GPS Spoofing Detection Algorithm: uses displacement and speed threshold for anomaly detection and 3 STD of clean data error for multiple biased attack detection. The violet box is the DNN model that predicts next step displacement.

anomaly is detected if any of the errors, position/displacement or speed, exceeds the established thresholds. Following the detection of an anomaly, the stop attack flag is activated if the IMU-provided speed is zero or below speed threshold while GPS-derived speed is above threshold, whereas the overshoot attack flag is activated if the GPS-derived speed is zero or below speed threshold where the IMU-provided speed is above threshold. Alternatively, if both speedometer and GPS derived speeds are more than speed threshold, the turn-by-turn attack flag will be set to true, indicating the presence of turn-by-turn attack.

B. Data-Driven GPS Spoofing Detection Algorithm

The Data-Driven GPS spoofing detection algorithm builds upon the spoofing detection architecture described in [14] (see figure 1). In this framework utilizing the same data used by analytical framework, an ML-Based model is trained to predict the displacement between consecutive timestamps rather than calculating position to account for deviation between in-vehicle sensors and GPS. This predicted displacement is compared to the perceived displacement from GPS data samples to calculate displacement error as in equation 8. The procedures for developing the Data-Driven model to predict the displacement of vehicle based on the data from vehicle sensors are as follows:

First, the input data utilized by the DNN is the same as input data used by the analytical model. This data comprises speedometer readings, yaw angle measurements, the time interval between consecutive samples, and GPS data.

Second, Equation 1 is employed to compute the GPS-perceived displacements (in meters) once every 10 samples.

Third, Equation 3 performs the integration of the angular velocity around the z-axis, denoted as $\omega(t)$, to determine the yaw angle $\psi(t)$. Since displacement is not linearly related to $\psi(t)$, the $\cos(\psi)$ and $\sin(\psi)$ functions are used as substitute inputs for the neural network. These replacements enable the prediction of displacements in both x and y directions, respectively.

Fourth, the precise time intervals between consecutive samples are calculated and incorporated as an additional input feature to the neural network.

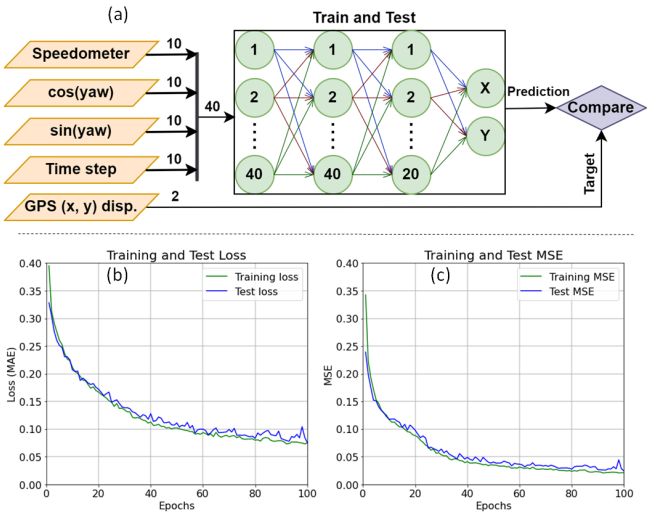

Fig. 2. (a) Ten samples of speed, $\cos(\psi)$, $\sin(\psi)$, and time step are fed into the proposed DNN and GPS-perceived displacement, sampled once every 10 samples, is used as the target value. (b) and (c) The test and training Mean loss profile and metrics illustrating the smooth decrease in the learning curve over 100 epochs.

Fifth, figure 2(a) illustrates the process of feeding 40 input features into the neural network. These features consist of 10 consecutive samples of speed, $\cos(\psi)$, $\sin(\psi)$and time intervals in addition to GPS-perceived displacements taken

every 10 samples. The GPS-perceived displacements in both x and y directions serve as target features to be compared with the predicted outputs of the DNN. The development and tuning of the DNN model are discussed in the next session.

1) Detection of Attacks with magnitudes larger than System Threshold: In the framework shown in figure 1(b) anomaly is detected if either displacement error or speed error is greater than or equal to speed or displacement thresholds. Upon the detection of an anomaly, the stop attack flag will be activated if the IMU-provided speed is less than the speed threshold, while the GPS-derived speed remains greater than speed threshold. Similarly, the overshoot attack flag will be activated if the GPS-derived speed is less than the speed threshold, while the IMU-provided speed is greater than the speed threshold. Otherwise, if both speeds are greater than the speed threshold, the turn-by-turn attack flag will be activated to indicate the presence of an attack.

2) Detection of Multiple Biased Attacks with Magnitude Smaller than System Threshold: In general, if the magnitude of a single attack on the system is smaller than or comparable to the established error thresholds, it does not pose a significant concern or location shift on the system though an attack that has already happened and challenged the security of the system. However, the scenario becomes much more problematic when such an attack is persistently applied over consecutive iterations. In this case, even though the magnitude of the attack remains below the error threshold in each individual step, the cumulative effect of these repeated small location shifts can result in a significant position error that eventually exceeds the predefined thresholds. This insidious accumulation can occur without the detection algorithm raising any alarms, as the algorithm typically compares each new data point against the error thresholds independently, failing to account for the cumulative impact of continuous smaller than threshold attacks. As a result, the vehicle can be gradually shifted from its actual position on it's rout similar to what happens by single attacks with magnitude larger than threshold in one step. This kind of attack poses a substantial threat to the safety and security of the vehicle's navigation system. Detection algorithms need to be designed to recognize the effect of these minor location shifts, as the failure can lead to significant position errors.

The distribution of errors between GPS and in-vehicle sensors exhibits a normal or Gaussian pattern. According to the properties of the Gaussian distribution, approximately 99.73% of the samples are expected to fall within three standard deviations (STD) from the mean value [41]. To facilitate anomaly detection, the mean and standard deviation of the error between the GPS (ground truth) and in-vehicle sensors' provided displacements are computed. These computed values, intrinsic to the sensors, remain constant and serve as reliable metrics for identifying deviations from expected behavior. In contrast to previous approaches like [14], which rely on thresholds based on maximum absolute errors between ground truth and predictions, this algorithm utilizes the three STDs rule derived from the normal distribution. Thus, if the error samples deviate from the computed mean value by more than three STDs, there is a high probability (99.73%) that they indicate spoofing. Consequently, employing the three STDs rule enables the algorithm to effectively detect spoofing attacks that fall below predefined error thresholds, thereby enhancing the robustness and reliability of anomaly detection in safeguarding against such attacks.

To further substantiate the normal distribution of errors between GPS and in-vehicle sensors, the Central Limit Theorem (CLT) is applied. The Central Limit Theorem (CLT) is a key principle in statistics. It states that a large number of independent random variables, all with the same distribution, their summed distribution will approximate a normal distribution, no matter what the original distribution was. This convergence to normality becomes more accurate as the sample size increases, provided the individual random variables have finite means and variances [42].

Given that the dataset comprises of sufficiently large number of samples, the conditions of the CLT are met, thereby justifying the application of normal distribution rules to the error data. This implies that the error measurements between the GPS and in-vehicle sensors can be modeled using a Gaussian distribution. This modeling is crucial for the anomaly detection algorithm, which relies on statistical thresholds derived from the mean and standard deviation of the error data. By adhering to the principles of the CLT, the reliability of the detection methodology is ensured. The results of evaluating this methodology, including its effectiveness in detecting GPS spoofing attacks are discussed in section V.

V. Data Preparation and Evaluation

This research leverages the Honda Research Institute Driving Dataset (HDD) [1] to create and assess a reliable algorithm for the detection of GNSS spoofing attacks. This dataset encompasses data from IMU, camera, LiDAR, GNSS, and the controller area network (CAN) of an standard vehicle in the market. The data is collected from diverse settings such as suburban and urban roads and highways of San Francisco, Bay Area. Since AVs have similar sensors, the HDD serves as an ideal foundation for simulating GNSS spoofing attack scenario datasets specific to AVs. The HDD captures various sensor data, including GNSS signals, relative accelerator pedal position (%), steering angle (deg), steering wheel speed (deg/s), speed (km/s), pressure on brake pedal (kpa), and yaw rate (deg/s), at a rate of 100Hz.

A. Data-Driven model development

The proposed DNN architecture includes an input layer, followed by two hidden layers, and an output layer with neuron counts of 40, 40, 20, and 2, respectively. The input layer and the two subsequent hidden layers employ the tanh activation function, while the output layer utilizes a linear activation function. The network is trained using the Adam optimizer over 100 epochs with a batch size of 32, resulting in a smooth decrease in both the loss function Mean Absolute Error (MAE) and the metric Mean Square Error (MSE), as illustrated in

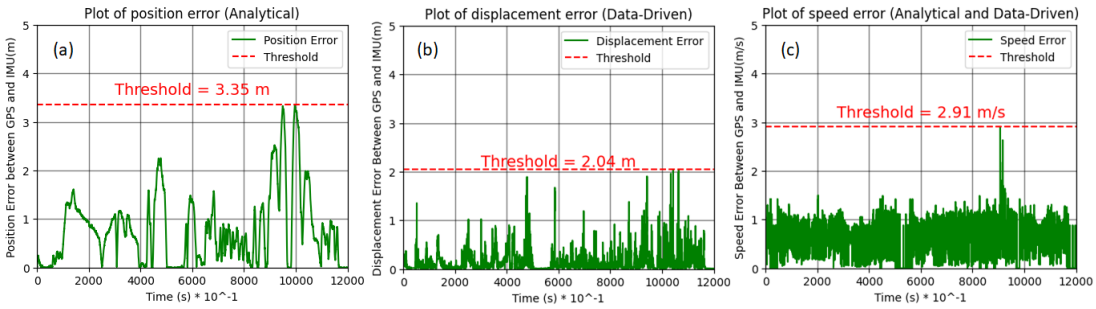

Fig. 3. (a): position error under no attack and the threshold value of 3.35m. (b): displacement error under no attack and the threshold value of 2.04m which is 39% less than that of analytical approach. (c): speed error with a threshold value of 2.91m/s

figure 2(b) and (c). This smooth decrease indicates there are no signs of overfitting during training. Furthermore, the two curves in figure 2(b) and (c) demonstrate that underfitting is not present, as the test and training curves closely follow each other. Training was halted at 100 epochs since no further decrease in the loss function was observed, and only minor fluctuations were noted. A summary of the hyperparameters used in the developed model is provided in Table I.

TABLE I
HYPERPARAMETERS OF THE DEVELOPED DNN MODEL FOR DISPLACEMENT PREDICTION.

Hyperparameters	Value
Number of neurons (1st and 2nd layers)	40
Number of neurons (3rd layer)	20
Number of neurons (4th layer)	2
Number of epochs	100
Batch size	32
Activation function (layers 1-3)	tanh
Activation function (output layer)	linear
Optimizer	Adam

The dataset used for the development of the proposed DNN model consists of a total of 144,000 samples. These samples were divided into training and testing sets following a 70-30 split ratio. Specifically, 100,800 samples were designated for training the model, allowing it to learn and adapt to the underlying patterns within the data effectively. The remaining 43,200 samples were used for testing the model's performance, providing a robust measure of its generalization capabilities on unseen data. This distribution was chosen to ensure a substantial amount of data for training while still retaining a large enough subset for testing, thereby minimizing the risk of overfitting and ensuring the model's ability to perform well in practical scenarios. The dataset split strategy supports a comprehensive evaluation during the training process, as reflected in the close tracking of the training and testing loss curves, indicating an effective learning process without signs of underfitting or overfitting. This setup is critical for achieving a well-balanced model that accurately predicts on new, unseen data, as demonstrated in the results.

To assess the efficiency of the proposed Data-Driven attack detection algorithm, it is validated under different compromised datasets, chosen selectively to represent diverse paths in urban and suburban driving conditions with different ranges of speed, that simulate the real scenarios of turn-by-turn, overshoot, stop and multiple biased attacks.

B. Detection of Attacks with magnitudes larger than System Threshold

First, in order for the position, displacement and speed thresholds to be determined, clean datasets are used as inputs for both analytical and Data-Driven algorithms to plot the position, displacement and absolute value of speed errors between GPS and IMU. In figure 3 the horizontal axes are time and the vertical axes are position, displacements and speed errors respectively, and the maximum error values are chosen as thresholds to assure sensor uncertainty is addressed so that in the presence of intrinsic sensor errors of the system, anomalies are still detectable and there are less False Negative rates (instances where attacks is detected but not mounted on the system in reality). Position threshold is extracted from analytical algorithm while the displacement threshold is extracted from Data-Driven algorithm and speed threshold is used for both algorithms. According to figure 3, the displacement threshold, derived from the data-driven approach, is lower than position threshold, obtained through analytical method. This difference arises because DNNs are adept at handling the inherent uncertainties and variabilities present in sensor data. Unlike traditional analytical methods, which often rely on simplified assumptions and models, DNNs process the raw, unfiltered input data and learn directly from the complexity and noise embedded within. This capability allows them to discern subtle patterns that are not immediately apparent under standard analytical evaluations. Moreover, DNNs effectively mitigate the impact of non-linear behaviors and biases in the sensor outputs, which often skew analytical predictions. By training on comprehensive datasets that include a wide range of operational conditions and error scenarios, DNNs calibrate more refined and accurate thresholds. These thresholds are not just safer, by reducing the risk of undetected attacks, but are also more practical, decreasing the likelihood of false alarms triggered by normal sensor noise or minor deviations. Thus, the adoption of a data-driven threshold ensures a more robust and reliable defense mechanism in the face of complex, real-world data challenges.

Second, to create turn-by-turn attacks, five attack scenarios with random magnitudes less than 100 meters are mounted on different parts of a clean dataset while the vehicle is moving, resulting in both compromised and uncompromised data. The results of turn-by-turn GPS spoofing attack detection for both approaches are shown in figure 4, where the horizontal axes are time and the vertical axes are the position and displacement errors respectively. According to figure 4 wherever the position and displacement errors between IMU and GPS are less than position or displacement threshold the situation is normal, no spoofing is mounted on the system, but on the instances the errors exceed the thresholds GPS spoofing attack is detected.

Third, to create stop attack a part of a clean dataset, during which the vehicle is stopped, is chosen and GPS data are compromised in five different parts such that the vehicle is moving along the road while it is actually stopped. The accuracy, recall and F1-score of stop attack detection are shown on second row of table II for both data-driven and analytical approaches. For more information about stop attack and its detection see [14].

Fourth, to create overshoot attack GPS data are manipulated in five different parts, attack scenarios, to show that the car is stopped while is it moving along the road. The accuracy, recall and F1-score of overshoot attack detection are shown on third row of table II for both data-driven and analytical approaches. For more information about stop attack and its detection see [14].

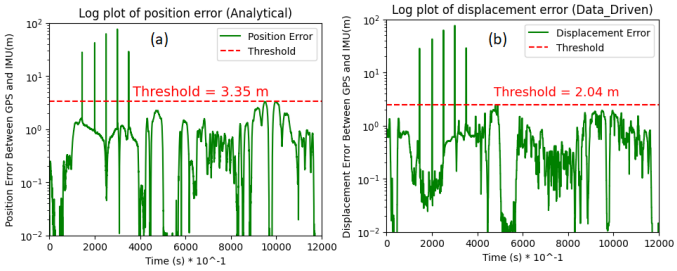

Fig. 4. Detection of five turn-by-turn attack scenarios for both analytical (left) and data-driven (right) approaches when errors exceed thresholds

C. Detection of Multiple Biased Attacks with Magnitudes Smaller than System Threshold

To further evaluate the Data-Driven algorithm against multiple biased attacks that are smaller than system threshold, GPS data are manipulated by one meter location shift on x and y coordinates during 1000 iterations and in 101 steps so that approximately 141 meters location shift is posed on the system. The accuracy, recall and F1-score of multiple biased attacks detection for Data-Driven algorithm are shown on forth row of table II. Additionally, figure 5 compares the conditions of no attack (a), single attack with magnitude larger than system threshold (b) and a series of 100 small biased attacks smaller than system threshold (c) where the horizontal axes are predicted displacement based on IMU and the vertical axes are GPS displacements, respectively. The black dashed line (y=x) is drown as a guide to show the deviation between GPS and IMU provided displacements in the dataset. The red dot on figure 5(b) represents a single large magnitude attack by 141 meters location shift while the red dots on figure 5(c) represent a series of 101 attacks smaller than error threshold shown on figure 3.

TABLE II
SUMMARY OF RESULTS FOR ALL FOUR TYPES OF SPOOFING ATTACK DETECTION FOR BOTH ANALYTICAL (A ON THE LEFT SIDES OF COLUMNS) AND DATA-DRIVEN (DD ON THE RIGHT SIDES OF COLUMNS) FRAMEWORKS.

Attack Type	Accuracy A|DD	Recall A|DD	F1-Score A|DD
Turn-by-turn	99.74 | 100	100 | 100	99.87 | 100
Stop	99.99 | 99.95	99.5 | 95.23	99.7 | 97.56
Overshoot	100 | 99.91	100 | 99.54	100 | 99.77
Multiple Biased	**97.83**	**100**	**98.9**

Table II summarizes the results of both approaches for the detection of turn-by-turn, stop and overshoot attacks and the results of only Data-Driven method for the detection of multiple biased attacks. Table II illustrates that multiple biased attacks are detected with the accuracy of 97.83% which is slightly less than the expected 99.73% due to the false positive samples that are not dangerous for the security of the system. Provided that the uncertainty range, non-linearity, and bias of the sensors are known during the data collection phase, the analytical approach is expected to perform perfectly. However, it performs poorly compared to the data-driven approach because the data-driven method addresses the data uncertainty, non-linearity, and bias to achieve optimal predictions at it's output.

Also, The superior performance of the proposed data-driven approach is evident in table III, showcasing its effectiveness in detecting GNSS spoofing attacks with an unparalleled F1-score of 1.00 for "turn-by-turn" attacks, outperforming previous studies [21], [43], and [44] with scores of 0.904, 0.913, and 0.987, respectively. Unique to our methodology is the successful detection of "Multiple Biased" attacks, with F1-scores of 0.989. These achievements mark a significant advancement in the field, enhancing security for critical navigation systems where others have not ventured.

TABLE III
COMPARISON TABLE OF SIMILAR WORKS BASED OF F1-SCORE METRIC THE FIELDS WITH * ARE AVERAGED OR CALCULATED FROM THE CORRESPONDING WORKS' RESULTS. ALSO, – MEANS THE ATTACK DETECTION IS NOT SEEN IN THE RESULTS OF CORRESPONDING WORK.

Attack Type	[21]	[43]	[44]	**This work**
Turn-by-turn	0.904 *	0.913 *	0.987 *	**1**
Stop	–	–	–	**0.975**
Overshoot	–	–	–	**0.997**
Multiple Biased	–	–	–	**0.989**

VI. CONCLUSION

In this paper, an innovative Data-Driven framework for detecting GPS spoofing attacks using data from in-vehicle

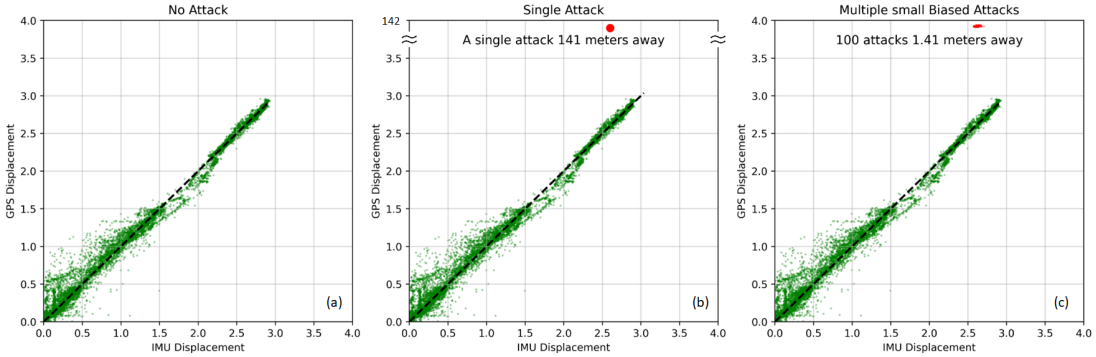

Fig. 5. GPS displacement versus IMU displacement. (a) No attack: IMU displacement closely matches GPS displacement, with the black dashed line (y=x) as the ideal guide. (b) Single large-magnitude attack: the red dot indicates the error between GPS and IMU displacement by 141m. (c) Multiple small biased attacks: each red dot shows an error of 1.41m between GPS and IMU displacements.

sensors has been presented. First, error thresholds for displacement and speed of vehicle are extracted using clean datasets and used as references for anomaly detection. Second, data from various sensors such as the speedometer and sin and cosine of yaw angle from gyroscope are utilized in the proposed Data-Driven approach to predict displacement using a DNN architecture with lower error rates. The error between predicted displacements from in-vehicle sensors' data and perceived displacement from GPS data is then compared with the predefined error thresholds to identify any anomalies in GPS data in real time. Moreover, the analysis involves the comparison of vehicle speed data obtained from GPS with speedometer readings to further enhance the detection and classification capabilities of spoofing attacks. The incorporation of this comparison mechanism accompanying lower thresholds than analytical approach, significantly contributes to the effectiveness of the Data-Driven approach. Third, a high degree of accuracy is achieved by the proposed Data-Driven model in identifying multiple biased stealthy attacks operating below the predefined thresholds. Given large sample size of the dataset, the distribution of sensor errors follows a normal pattern and 99.73% of samples are expected to fall within three STDs from the mean value. The mean and STD of the errors are computed using clean datasets and are expected to remain unchanged after attacks are mounted since they are intrinsic to sensors and do not change by attack. This enables the determination of whether the samples are spoofed, by checking if they deviate from the predefined mean value by more than three STDs. Also, the comprehensive validation of the framework against four distinct attack types further confirms its effectiveness in real-world scenarios. Additionally, a detailed comparison between the proposed Data-Driven framework and an analytical approach is provided. This comparative analysis showcases the superiority of the Data-Driven method in terms of accuracy and efficiency to different spoofing attack scenarios since it has lower threshold compared to the analytical algorithm. In conclusion, the Data-Driven framework presented in this paper stands as a reliable solution for detecting GPS spoofing attacks, offering enhanced accuracy and dependability in real-time applications.

VII. Future Work

Attention will be directed towards developing spoofing detection mechanisms for mitigating multiple biased spoofing attacks on GNSS signals below predefined thresholds. This will involve adopting Long Short-Term Memory (LSTM) networks known for retaining both long and short-term dependencies in data. The LSTM-based spoofing detection framework will be designed to surpass conventional methods by leveraging inherent memory capabilities. Training on diverse spoofing scenarios and authentic GNSS signal data aims to enhance its ability to discern subtle discrepancies indicative of spoofing attempts. Additionally, integrating real-time data streams into the LSTM-based spoofing detection system will ensure responsiveness to dynamic spoofing threats in operational GNSS environments. This will involve deploying efficient data preprocessing pipelines and adaptive model updating mechanisms for resilience against evolving spoofing tactics.

References

[1] V. Ramanishka, Y.-T. Chen, T. Misu, and K. Saenko, "Toward driving scene understanding: A dataset for learning driver behavior and causal reasoning," in *Conference on Computer Vision and Pattern Recognition (CVPR)*, 2018.

[2] Y. Deng, T. Zhang, G. Lou, X. Zheng, J. Jin, and Q.-L. Han, "Deep learning-based autonomous driving systems: A survey of attacks and defenses," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 12, pp. 7897–7912, 2021.

[3] M. J. Zideh, M. R. Khalghani, and S. K. Solanki, "An unsupervised adversarial autoencoder for cyber attack detection in power distribution grids," *Electric Power Systems Research*, vol. 232, p. 110407, 2024.

[4] M. J. Zideh, P. Chatterjee, and A. K. Srivastava, "Physics-informed machine learning for data anomaly detection, classification, localization, and mitigation: A review, challenges, and path forward," *IEEE Access*, vol. 12, pp. 4597–4617, 2024.

[5] M. L. Psiaki and T. E. Humphreys, "Gnss spoofing and detection," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270, 2016.

[6] R. A. Agyapong, M. Nabil, A.-R. Nuhu, M. I. Rasul, and A. Homaifar, "Efficient detection of gps spoofing attacks on unmanned aerial vehicles using deep learning," in *2021 IEEE Symposium Series on Computational Intelligence (SSCI)*, 2021, pp. 01–08.

[7] C. Kwon, W. Liu, and I. Hwang, "Analysis and design of stealthy cyber attacks on unmanned aerial systems," *Journal of Aerospace Information Systems*, vol. 11, no. 8, pp. 525–539, 2014.

[8] M. Mynuddin, S. U. Khan, and M. N. Mahmoud, "Trojan triggers for poisoning unmanned aerial vehicles navigation: A deep learning approach," in *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*. IEEE, 2023, pp. 432–439.

[9] C. Kwon and I. Hwang, "Cyber attack mitigation for cyber–physical systems: hybrid system approach to controller design," *IET Control Theory & Applications*, vol. 10, no. 7, pp. 731–741, 2016.

[10] X. Yan, M. Sarkar, B. Lartey, B. Gebru, A. Homaifar, A. Karimoddini, and E. Tunstel, "An online learning framework for sensor fault diagnosis analysis in autonomous cars," *IEEE Transactions on Intelligent Transportation Systems*, 2023.

[11] K. Surendhar, B. K. Pandey, G. Geetha, and H. Gohel, "Detection of payload injection in firewall using machine learning," in *2023 IEEE 12th International Conference on Communication Systems and Network Technologies (CSNT)*, 2023, pp. 186–190.

[12] K. Shaikh, I. Hussain, and B. S. Chowdhry, "Deep learning-based fault detection in railway wheelsets using time series analysis," *Mehran University Research Journal Of Engineering & Technology*, vol. 42, no. 3, p. 154–159, 2023.

[13] V. S. Rao, R. Balakrishna, Y. A. B. El-Ebiary, P. Thapar, K. A. Saravanan, and S. R. Godla, "Ai driven anomaly detection in network traffic using hybrid cnn-gan," *Journal of Advances in Information Technology*, vol. 15, no. 7, 2024.

[14] S. Dasgupta, M. Rahman, M. Islam, and M. Chowdhury, "A sensor fusion-based gnss spoofing attack detection framework for autonomous vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 12, pp. 23 559–23 572, 2022.

[15] K. C. Zeng, Y. Shu, S. Liu, Y. Dou, and Y. Yang, "A practical gps location spoofing attack in road navigation scenario," in *Proceedings of the 18th international workshop on mobile computing systems and applications*, 2017, pp. 85–90.

[16] J. R. Van Der Merwe, X. Zubizarreta, I. Lukčin, A. Rügamer, and W. Felber, "Classification of spoofing attack types," in *2018 European Navigation Conference (ENC)*. IEEE, 2018, pp. 91–99.

[17] P. M. Kebria, A. Khosravi, S. Nahavandi, A. Homaifar, and M. Saif, "Experimental comparison study on joint and cartesian space control schemes for a teleoperation system under time-varying delay," in *2019 IEEE International Conference on Industrial Technology (ICIT)*. IEEE, 2019, pp. 108–113.

[18] Y. Ayalew, W. Bedada, A. Homaifar, and K. Freeman, "Data-driven urban air mobility flight energy consumption prediction and risk assessment," in *Intelligent Systems Conference*. Springer, 2023, pp. 354–370.

[19] A. Mohammadi and M. Chahardori, "A low-power, bootstrapped sample and hold circuit with extended input ranged for analog-to-digital converters in cmos 0.18 μm," in *2018 15th International Conference on Synthesis, Modeling, Analysis and Simulation Methods and Applications to Circuit Design (SMACD)*. IEEE, 2018, pp. 269–272.

[20] B. Sel, A. Tawaha, Y. Ding, R. Jia, B. Ji, J. Lavaei, and M. Jin, "Learning-to-learn to guide random search: Derivative-free meta black-box optimization on manifold," in *Learning for Dynamics and Control Conference*. PMLR, 2023, pp. 38–50.

[21] M. Kamal, A. Barua, C. Vitale, C. Laoudias, and G. Ellinas, "Gps location spoofing attack detection for enhancing the security of autonomous vehicles," in *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*. IEEE, 2021, pp. 1–7.

[22] Z. U. Chowdhury and et. al., "Performance comparison of yolo models for safety helmet detection: Insights from yolov5 to yolov10 with transfer learning," in *International Conference of Adisutjipto on Aerospace Electrical Engineering and Informatics (ICAAEEI)*. Institute of Electrical and Electronics Engineers (IEEE), oct 2024.

[23] M. Mynuddin, S. U. Khan, R. Ahmari, L. Landivar, M. N. Mahmoud, and A. Homaifar, "Trojan attack and defense for deep learning-based navigation systems of unmanned aerial vehicles," *IEEE Access*, vol. 12, pp. 89 887–89 907, 2024.

[24] N. Niknejad and H. Modares, "Physics-informed data-driven safe and optimal control design," *IEEE Control Systems Letters*, vol. 8, pp. 285–290, 2024.

[25] V. Hemmati, M. Behnia, A. Mohammadi, A.-R. Nuhu, and A. Homaifar, "Mission-based quadcopter flight simulation," in *Digital Avionics Systems Conference DASC (presented)*. IEEE, 2024.

[26] J. Zidan, E. I. Adegoke, E. Kampert, S. A. Birrell, C. R. Ford, and M. D. Higgins, "Gnss vulnerabilities and existing solutions: A review of the literature," *IEEE Access*, vol. 9, pp. 153 960–153 976, 2020.

[27] B. W. O'Hanlon, M. L. Psiaki, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "Real-time gps spoofing detection via correlation of encrypted signals," *Navigation*, vol. 60, no. 4, pp. 267–278, 2013.

[28] B. W. O'Hanlon, M. L. Psiaki, T. E. Humphreys, and J. A. Bhatti, "Real-time spoofing detection in a narrow-band civil gps receiver," in *Proceedings of the 23rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2010)*, 2010, pp. 2211–2220.

[29] J. Yang, Y. Chen, W. Trappe, and J. Cheng, "Detection and localization of multiple spoofing attackers in wireless networks," *IEEE Transactions on Parallel and Distributed systems*, vol. 24, no. 1, pp. 44–58, 2012.

[30] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandon, and G. Lachapelle, "A low-complexity gps anti-spoofing method using a multi-antenna array," in *Proceedings of the 25th international technical meeting of the satellite division of the institute of navigation (ION GNSS 2012)*, 2012, pp. 1233–1243.

[31] M. L. Psiaki, B. W. OHanlon, S. P. Powell, J. A. Bhatti, K. D. Wesson, and T. E. Schofield, "Gnss spoofing detection using two-antenna differential carrier phase," in *Proceedings of the 27th international technical meeting of the satellite division of the Institute of Navigation (ION GNSS+ 2014)*, 2014, pp. 2776–2800.

[32] S. Liu, X. Cheng, H. Yang, Y. Shu, X. Weng, P. Guo, K. C. Zeng, G. Wang, and Y. Yang, "Stars can tell: a robust method to defend against {GPS} spoofing attacks using off-the-shelf chipset," in *30th USENIX Security Symposium (USENIX Security 21)*, 2021, pp. 3935–3952.

[33] A. Neish, S. Lo, Y.-H. Chen, and P. Enge, "Uncoupled accelerometer based gnss spoof detection for automobiles using statistic and wavelet based tests," in *Proceedings of the 31st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2018)*, 2018, pp. 2938–2962.

[34] C. Tanil, P. M. Jimenez, M. Raveloharison, B. Kujur, S. Khanafseh, and B. Pervan, "Experimental validation of ins monitor against gnss spoofing," in *Proceedings of the 31st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2018)*, 2018, pp. 2923–2937.

[35] S. Manickam and K. O'Keefe, "Using tactical and mems grade ins to protect against gnss spoofing in automotive applications," in *Proceedings of the 29th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2016)*, 2016, pp. 2991–3001.

[36] P. Borhani-Darian, H. Li, P. Wu, and P. Closas, "Deep neural network approach to detect gnss spoofing attacks," in *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)*, 2020, pp. 3241–3252.

[37] M. Sun, Y. Qin, J. Bao, and X. Yu, "Gps spoofing detection based on decision fusion with a k-out-of-n rule." *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 670–674, 2017.

[38] C. C. Robusto, "The cosine-haversine formula," *The American Mathematical Monthly*, vol. 64, no. 1, pp. 38–40, 1957.

[39] K.-C. Kwon and D.-S. Shim, "Performance analysis of direct gps spoofing detection method with ahrs/accelerometer," *Sensors*, vol. 20, no. 4, p. 954, 2020.

[40] A. Mohammadi, V. Hemmati, R. Ahmari, F. O. Ambrose, M. N. Mahmoud, and A. Homaifar, "Gps spoofing attack detection on autonomous vehicles using modified dbscan with dynamic threshold," in *5th IFSA Winter Conference on Automation, Robotics & Communications for Industry 4.0/5.0 (ARCI) (submitted)*, 2025.

[41] F. Miller, A. Vandome, and M. John, *68-95-99. 7 Rule*. VDM Publishing, 2010. [Online]. Available: https://books.google.com/books?id=Ihw1kgAACAAJ

[42] R. M. Dudley, *Uniform central limit theorems*. Cambridge university press, 2014, vol. 142.

[43] Z. Yang, J. Ying, J. Shen, Y. Feng, Q. A. Chen, Z. M. Mao, and H. X. Liu, "Anomaly detection against gps spoofing attacks on connected and autonomous vehicles using learning from demonstration," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 9, pp. 9462–9475, 2023.

[44] S. Dasgupta, T. Ghosh, and M. Rahman, "A reinforcement learning approach for global navigation satellite system spoofing attack detection in autonomous vehicles," *Transportation research record*, vol. 2676, no. 12, pp. 318–330, 2022.