Detecting GPS Spoofing Attacks Using Corrected Low-Cost INS Data with an LSTM Network

Mohammed AFTATAH, Khalid ZEBBARA
IMISR Laboratory, FSA Ait Melloul, Ibn Zohr University, Agadir, Morocco

***Abstract*—With the emergence of new technologies ranging from smart cities to the Internet of Things (IoT), many objects rely on satellite-based navigation systems, such as GPS, to accomplish their tasks securely. However, GPS receivers are exposed to various unintentional and intentional attacks, threatening the availability and reliability of the delivered information. GPS spoofing is considered as one of the most dangerous attacks, where attackers transmit intense signals on the same frequency to disrupt the GPS receiver, leading to erroneous position calculations. Detection methods for GPS spoofing are crucial to ensure secure navigation. This paper proposes a method for GPS spoofing detection that utilizes artificial intelligence algorithms in combination with raw data from an inertial navigation system (INS). Since INS sensors are prone to accumulating errors over time, these inaccuracies are corrected via a Long Short-Term Memory (LSTM) algorithm. The corrected accelerations and angular rates are then compared to the accelerations and angular rates estimated from the GPS data to detect GPS spoofing signals. This comparison uses the modified M-of-N method, demonstrating its effectiveness by a detection rate reaching 80% of the spoofing zones.**

***Keywords*—Secure navigation; GPS spoofing; inertial systems; LSTM; M-of-N method; anti-spoofing techniques**

I. Introduction

In the era of recent technologies such as smart cities and IoT, Global Navigation Satellite Systems (GNSS), including GPS, play a pivotal role in delivering navigation information, time, and location, which are essential for the security of systems relying on such information [1]. GPS is a constellation of satellites orbiting the Earth at approximately 20,200 kilometers of altitude. These satellites continuously transmit signals to the Earth's surface, which are received by GPS receivers to determine precise locations and time information.

However, this reliance on radio signals introduces a significant vulnerability: the susceptibility to interference and malicious attacks. One of the most concerning types of attacks is GPS spoofing. This attack broadcasts false GPS signals that deceive the receiver into calculating incorrect position or time. This exploitation poses a serious threat to the integrity and security of GPS-based systems, especially in safety-critical applications such as autonomous vehicles, aviation, and drones.

In response to this growing threat, there is an urgent need to develop robust detection methods to secure GNSS from spoofing attacks. This work proposes a novel method that integrates inertial data with an LSTM network to detect the GPS spoofing attack and ensure secure navigation for GPS-dependent systems.

The structure of the rest of this paper is as follows: The introduction of the study, the review of related work, the research gaps, and the discussion of associated challenges are detailed in Section I. Section II outlines our approach to simulate the IMU sensors, followed by the mechanization process to derive navigation data. Section III focuses on GPS vulnerabilities, particularly spoofing attacks, which are examined in detail. Section IV presents our proposed approach to recognize GPS spoofing attacks using the LSTM algorithm, INS raw data, and the M-of-N method. Section V demonstrates the performance of our approach in a simulated transport scenario. Section VI concludes the paper, while Section VII explores future directions for this research.

A. Existing Work

During the last decade, diverse works have been published in the literature dealing with the problems of detecting, identifying, and mitigating intentional and unintentional attacks on satellite-based systems such as GPS. Intentional attacks include both jamming and spoofing attacks [2] [3] [4] [5]. For example, the authors of study [6] developed a covert spoofing algorithm for UAVs using a GPS/INS-integrated navigation system. The method involves estimating the UAV's current state using external sensors and calculating a spoofing control input to guide the UAV toward a deceptive trajectory while making it appear as if it is following its original reference trajectory. The proposed algorithm was validated through simulations, demonstrating that the UAV can be covertly spoofed by making its estimated position remain near the reference trajectory, while its actual path deviates towards the deceptive target state. The results showed effective trajectory manipulation with minimal disruption to the UAV's original path. To overcome these issues, numerous research studies were developed employing various techniques of machine learning, including Artificial Neural Networks (ANN) and Support Vector Machine (SVM), to evaluate their effectiveness in identifying spoofed signals [7].

The authors of study [8] developed an approach based on machine learning called PERDET for detecting GPS spoofing attacks in unmanned aerial vehicles (UAVs). This method utilizes perception data collected from real flight experiments, including both normal and attacked scenarios, to enhance the detection capabilities against GPS spoofing. The authors performed feature analysis based on the principles of position and attitude estimation, selecting relevant sensor data types to improve the accuracy of their detection model. They concluded that PERDET outperformed in terms of effectiveness compared to various machine learning algorithms after applying them to their dataset.

In study [9], the authors developed a method for detecting GNSS signal spoofing based on supervised machine learning. The technique used includes SVM and Principal Component Analysis (PCA) for identifying manipulated GNSS signals. The SVM model achieved high performance in the experiments, with over 98% accuracy. However, the paper notes a potential challenge with model complexity, which may result in longer computation times.

Sun et al. [10] developed a method for GPS spoofing detection, specifically designed for small UAVs, based on deep learning techniques. They proposed a model combining a PCA, a Convolutional Neural Network (CNN), and an LSTM to enhance the detection accuracy. The approach was validated using a dataset acquired from UAV flights with normal and spoofed GPS signals, achieving an accuracy of 99.49%. In contrast, the primary gap identified in this paper is the challenge of adapting the model to real-world environments.

In 2020, Kwon and Shim [11] exploited Attitude and Heading Reference System (AHRS) accelerometers to develop a direct GPS spoofing detection method. This method involves a comparison between the acceleration estimated from the GPS receiver and the acceleration generated by the accelerometers to detect potential spoofing. The results indicated that both decision variables showed strong detection capabilities under different spoofing scenarios. However, the gap identified in this paper lies in the sensitivity of the decision variables to changes in moving acceleration.

In study [12], the authors developed a GPS spoofing detection method using a tightly coupled Receiver Autonomous Integrity Monitoring (RAIM) with INS integration. The method monitors discrepancies between GPS and inertial measurements, using residual-based RAIM techniques. This approach utilizes an integrated GPS/INS architecture with a tightly coupled Kalman filter to improve sensitivity to spoofing attacks. The results demonstrated that the RAIM monitor effectively detected short-duration spoofing attacks.

Shafique et al. [13] used two machine-learning techniques, SVM and K-fold analysis, for GPS spoofing detection. Various machine-learning algorithms were tested, and SVM with a polynomial kernel achieved the best results. Multiple metrics were utilized to evaluate the proposed, including accuracy, precision, recall, and F1-score, achieving an overall accuracy of 99%. However, the gap identified is that the method's performance may degrade with noisy data and might not be robust against highly sophisticated spoofing attacks.

The authors of study [14] designed a method, for detecting GPS spoofing attacks on Unmanned Aerial Systems (UAS), based on supervised machine learning. The proposed approach leverages an ANN model to classify GPS signals as genuine or spoofed using extracted features such as pseudo-range, Doppler shift, signal-to-noise ratio (SNR), and satellite vehicle number (SVN). The results showed that the ANN model with two hidden layers provided high detection accuracy, achieving up to 98.3% accuracy and a probability of detection of 99.2% with a low probability of false alarms. However, a primary gap identified in the study is that the model's performance is highly dependent on the quality of the collected GPS data.

B. Research Gaps and Challenges

Despite the increasing use of low-cost INS in navigation applications, these sensors suffer from high error rates and limited accuracy, making them unreliable in scenarios involving GPS spoofing or jamming. Current methods to address these issues heavily depend on high-grade INS, which are expensive and not feasible for large-scale adoption. This highlights a significant gap in the availability of robust, low-cost solutions that can maintain high accuracy. Additionally, many approaches lack adaptability to real-time changes in error characteristics, particularly during GPS spoofing or jamming events, making them less effective in dynamic environments.

To address these challenges, our research focuses on developing a methodology for enhancing the quality of low-cost INS data by employing LSTM networks, using tactical-grade INS as a reference. The developed simulation platform in MATLAB enables researchers to build and validate their solutions based on our sensor modeling approach. This platform can simulate various scenarios without the need for complex infrastructure or expensive real-world setups involving GPS receivers and sensors mounted on vehicles. This flexibility makes it easier to test multiple configurations and spoofing scenarios efficiently. Successfully addressing these challenges will provide a practical and accessible platform for reliable navigation in GPS-compromised environments.

II. Inertial Navigation Simulation and Mechanization

A. INS Simulation

In this study, a real INS was not used; instead, a simulated one was employed, with errors affecting its sensors taken into consideration. This section presents the simulation of the six sensors of the Inertial Measurement Unit (IMU). Typically, a real INS is mounted on a mobile platform during a trajectory, measuring accelerations and angular rates [15]. However, in this case, we assume the availability of the real trajectory coordinates and proceed to simulate the behavior of the sensors accordingly. This allows us to replicate how the IMU would function in a real-world scenario, accounting for sensor errors without using an actual INS.

To model INS sensors, two main frames are used to represent the sensor outputs, the navigation frame and the body frame [16]. The body frame represents local coordinates relative to the vehicle [17], while the navigation frame aligns with the Earth's coordinate system [18]. Table I explains the differences between these frames, including their axes, alternative names, and reference centers.

TABLE I. Differences Between the ENU Frame and the Body Frame

Characteristic	Body frame	Navigation frame
Axes	X(Longitudinal), Y (Lateral), and Z (Vertical)	East (E), North (N), and Up (U)
Alternative name	Local frame, vehicle frame, or b-frame	ENU frame or n-frame
Reference Center	Center of the vehicle or mobile object	Earth's surface

The equations that model the outputs of the three orthogonal accelerometers and the three orthogonal gyroscopes in the navigation frame can be expressed using the following equations (1) (2) (3) [19].

$$\begin{bmatrix}\varphi\\ \theta\\ \psi\end{bmatrix} = \begin{bmatrix} \dfrac{\partial\left(\arctan\dfrac{\partial N/\partial t}{\partial E/\partial t}\right)}{\partial t} \\ \dfrac{\partial\left(\arctan\dfrac{\partial U/\partial t}{\partial E/\partial t}\right)}{\partial t} \\ \dfrac{\partial\left(\arctan\dfrac{\partial U/\partial t}{\partial N/\partial t}\right)}{\partial t} \end{bmatrix}^{n} \tag{1}$$

$$\begin{bmatrix}p\\ q\\ r\end{bmatrix}^{b} = \left(\begin{bmatrix} 1 & \dfrac{\sin\varphi\sin\theta}{\cos\theta} & \dfrac{\cos\varphi\sin\theta}{\cos\theta} \\ 0 & \cos\varphi & -\sin\varphi \\ 0 & \dfrac{\sin\varphi}{\cos\theta} & \dfrac{\cos\varphi}{\cos\theta} \end{bmatrix} * \begin{bmatrix}\dot{\varphi}\\ \dot{\theta}\\ \dot{\psi}\end{bmatrix}\right)^{-1} \tag{2}$$

$$\begin{bmatrix}f_E\\ f_N\\ f_U\end{bmatrix}^{b} = \frac{\partial}{\partial t}\left(C_n^b \begin{bmatrix}\dfrac{\partial E}{\partial t}\\ \dfrac{\partial N}{\partial t}\\ \dfrac{\partial U}{\partial t}\end{bmatrix}^{n}\right) - C_n^b\begin{bmatrix}0\\0\\g\end{bmatrix} + \begin{bmatrix}0 & -r & q\\ r & 0 & -p\\ -q & p & 0\end{bmatrix} * C_n^b \begin{bmatrix}\dfrac{\partial E}{\partial t}\\ \dfrac{\partial N}{\partial t}\\ \dfrac{\partial U}{\partial t}\end{bmatrix}^{n} \tag{3}$$

The components of Eq. (1), (2), and (3) are detailed in Table II.

TABLE II. DESCRIPTION OF EQUATION COMPONENTS FOR IMU MODELING

Equation component	Description/Meaning
[φ, θ, ψ]	Euler angles
[E, N, U]	3D position in the ENU frame
t	Time
[p, q, r]	Angular velocity
$\left[\dot{\varphi}, \dot{\theta}, \dot{\psi}\right]$	Time derivative of the Euler angles
$\left[f_E, f_N, f_U\right]$	3D linear acceleration
C_n^b	Transformation matrix from n-frame to b-frame

B. INS Mechanization

Once the sensors are simulated, their outputs can be generated using any predefined trajectory. The simulated sensor outputs include specific forces and angular rates. These outputs are processed through the mechanization equations to compute position, velocity, and orientation of the mobile. The mechanization equations integrate the sensor data over time, allowing for the continuous update of the navigation solution. These equations are given by Eq. (4) [20] [21] [22].

$$\begin{pmatrix}\dot{r}^n\\ \dot{v}^n\\ \dot{C}_b^n\end{pmatrix} = \begin{pmatrix} D^{-1}v^n \\ C_b^n f^b - (2\Omega_{ie}^n + \Omega_{en}^n)v^n + g^n \\ C_b^n(\Omega_{ib}^b - \Omega_{in}^b)\end{pmatrix} \tag{4}$$

Where,

r^n presents the position components in terms of latitude, longitude, and height;

v^n is the velocity;

C_n^b is a 3x3 conversion matrix from the ENU frame to the body frame;

f^b are the raw accelerations in the body frame;

g^n is the gravity.

The specific forces are integrated twice to derive the position in the body frame. Following this, the angular rates play a crucial role in calculating the transformation matrix, which is used to convert the values from the b-frame to the ENU frame. This transformation is key to ensuring that the navigation information, such as position and velocity, is expressed correctly relative to the Earth or the navigation frame. The process of INS mechanization is detailed in Fig. 1, illustrating the steps involved in converting raw IMU data into usable navigation data.

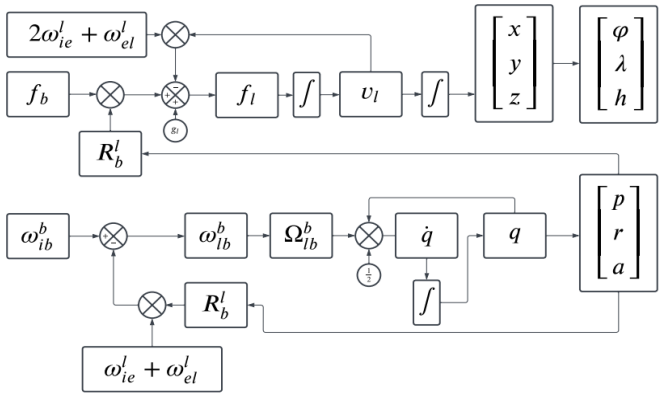


Fig. 1. Illustration of the INS mechanization process [23] [24].

III. GPS SPOOFING

Radiofrequency technologies are widely used to offer mobility and cost-effectiveness for numerous applications. GPS, one of the most in-demand navigation systems, relies on electromagnetic waves for positioning and navigation. However, this reliance on electromagnetic signals makes GPS

highly vulnerable to various attacks. These vulnerabilities can be categorized into intentional and unintentional threats. Unintentional threats may arise from environmental interference or signal obstruction. The primary unintentional attacks targeting GPS systems are illustrated in Fig. 2, highlighting the risks associated with GPS's reliance on radio frequencies.

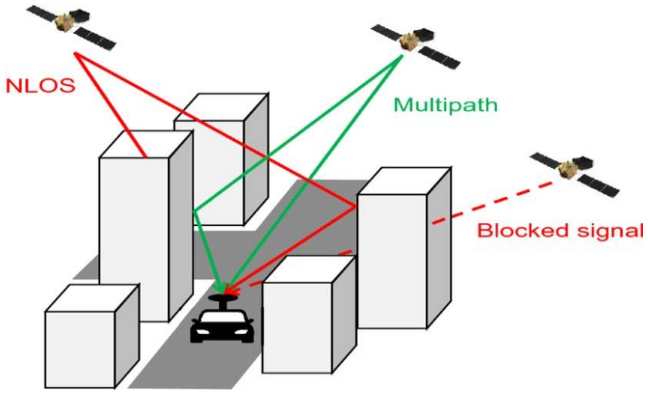


Fig. 2. Primary unintentional attacks targeting GPS [25].

Intentional attacks, often realized by hackers, include jamming and spoofing. Spoofing involves a powerful illegitimate signal transmitted at the same frequency as the legitimate GPS signal, with the intent to disrupt the receiver's ability to calculate the accurate location. The attacker can trick the GPS receiver into accepting false location data, leading to errors in navigation and positioning or reporting incorrect coordinates. The principle behind this spoofing attack is depicted in Fig. 3.

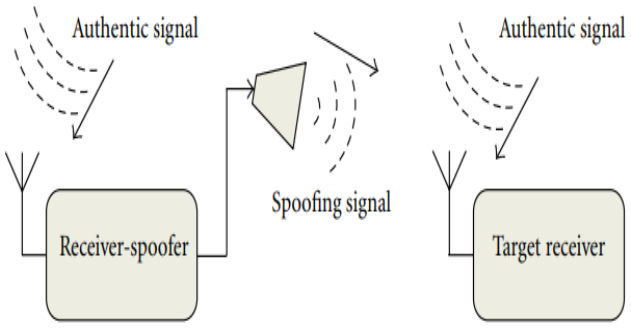


Fig. 3. The principle of the GPS spoofing attack [26].

In a legitimate GPS operation, the pseudo-range is the calculated distance between the receiver and the satellite, based on the time it takes for the satellite signal to reach the receiver. The legitimate pseudo-range to satellite *i* can be represented as Eq. (5).

$$\rho_i = c.(t_r - t_s^i) \tag{5}$$

Where ρ_i is the true pseudo-range to satellite i, c is the light's speed, t_r is the time of signal reception, and t_s^i is the time of signal transmission from the satellite i.

When a spoofing signal is introduced, the receiver detects a false signal that leads to an altered pseudo-range $\rho_i^{'}$ given by Eq. (6).

$$\rho_i^{'} = c.(t_r - t_s^{'i}) \tag{6}$$

Where $t_s^{'i}$ is the fake time of transmission introduced by the spoofer. This new pseudo-range $\rho_i^{'}$ deviates from the true pseudo-range ρ_i, causing the receiver to calculate an incorrect position. The difference between the true and spoofed pseudo-ranges, $\Delta\rho_i$, can be expressed as Eq. (7).

$$\Delta\rho_i = \rho_i^{'} - \rho_i = c.(t_s^i - t_s^{'i}) \tag{7}$$

IV. LSTM AND M-OF-N METHOD

A. LSTM Model

LSTM is a deep learning network belonging to the Recurrent Neural Networks (RNNs) family. It is particularly preferred when dealing with sequential data, such as INS measurements, effectively capturing long-term dependencies in time-series data, unlike traditional neural networks or deep neural networks. Fig. 4 illustrates the main structure of a basic LSTM unit. As shown in the following figure, this unit consists of three gates: the input gate, the forget gate, and the output gate.

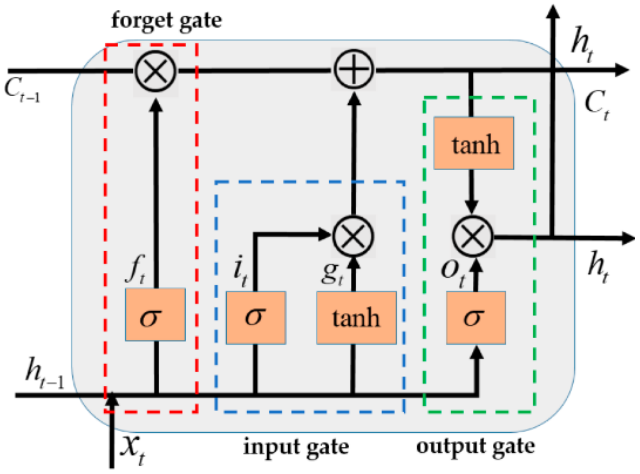


Fig. 4. Structure of a basic LSTM unit with input, forget, and output gates [27].

The input gate controls the information entering the cell state, the forget gate determines which information should be discarded from the memory, and the output gate decides which information is sent to the output. Eq. (8) (9) (10) (11) (12) give the LSTM-specific formulas [27] [28].

$$f_t = \sigma.(x_t W_{xf} + h_{t-1} W_{hf} + b_f) \tag{8}$$

$$i_t = \sigma.(x_t W_{xi} + h_{t-1} W_{hi} + b_i) \tag{9}$$

$$o_t = \sigma.(x_t W_{xo} + h_{t-1} W_{ho} + b_o) \tag{10}$$

$$c_t = f_t.c_{t-1} + i_t.g_t \quad (11)$$

$$h_t = o_t.\tanh c_t \quad (12)$$

B. M-of-N Method

In this study, we employ a modified M-of-N method to enhance the detection of GPS spoofing through the fusion of INS and GPS data. This approach compares sensor measurements from both systems and evaluates whether at least *M-of-N* measurements remain within an acceptable threshold. Deviations beyond this threshold are flagged as potential GPS spoofing events. Unlike traditional methods, the modified M-of-N approach incorporates tolerance for minor deviations arising from sensor noise and environmental factors, which are common in real-world scenarios. This method is based on calculating key statistical metrics such as the residual error E_k, the standard deviation σ_k, and a predefined confidence threshold C. These metrics help in determining whether the discrepancies between GPS and INS measurements are significant enough to be classified as spoofing or normal deviations due to noise. The equations used in this approach are as follows (13) (14).

$$E_k = \left| GPS_k - INS_k \right| \quad (13)$$

$$\left(\sigma_k\right)^2 = \frac{1}{n}\sum_{i=1}^{n}\left(E_i - \mu\right)^2 \quad (14)$$

Where E_k is the absolute difference between the GPS estimated measurement at the time step k and the corresponding INS measurement, σ_k is the standard deviation of the residual errors over a window of size N, and μ is the mean of the residual errors in that window. Furthermore, the threshold is expressed as Eq. (15).

$$Th = C \cdot \sigma_k \quad (15)$$

This threshold helps to distinguish between normal measurement deviations and significant anomalies caused by GPS spoofing. If the residual error E_k exceeds this threshold, a potential spoofing event is flagged.

In this study, we fix $C = 3$ to balance between sensitivity and false alarm rate. In a Gaussian distribution, a threshold of 3σ encompasses 99.73% of all normal data, meaning that only 0.27% of residual errors are expected to exceed this threshold due to noise. This makes the system sensitive to significant deviations while minimizing false alarms. Using a lower value, such as $C = 2$, would increase the sensitivity but also result in a higher false alarm rate, as 4.55% of the data would exceed the threshold, potentially flagging benign deviations as spoofing. Conversely, a higher value, such as $C = 4$, would further reduce the false alarm rate but could make the system less sensitive, missing smaller but meaningful anomalies. Therefore, $C = 3$ is chosen as an optimal value to provide reliable detection while minimizing false positives. The calculated values of E_k and Th are then used to detect the presence of anomalies in the GPS data. The flowchart of the detection process using the modified M-of-N technique is detailed in Fig. 5.

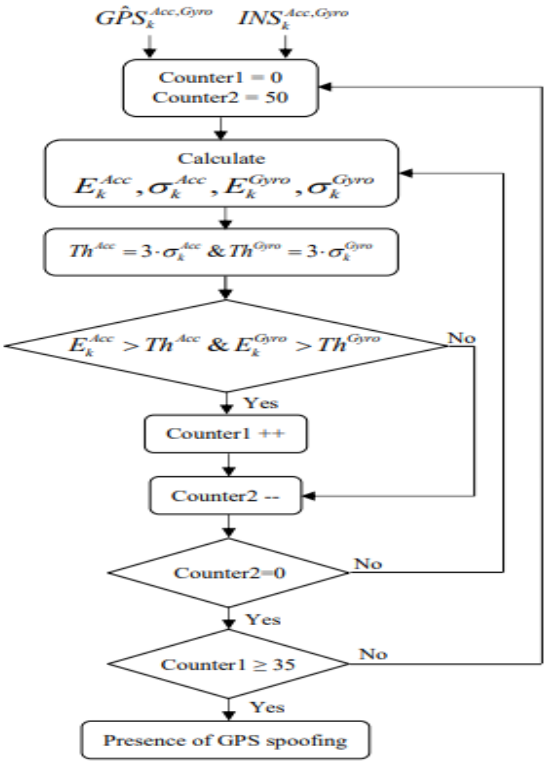


Fig. 5. Flowchart diagram of GPS spoofing detection using modified M-of-N technique.

To reduce false alarms in GPS spoofing detection, a reasonable value for N is 50, meaning spoofing is checked over every window of 50 points. This ensures that approximately 60 regions are covered in the trajectory. The value of M determines the sensitivity of the spoofing detection algorithm. To avoid high sensitivity to false positives due to noise, M is set at 35, around 70-80% of N. This ensures that the method requires a majority of the measurements in each window to exceed the threshold to flag an anomaly, providing a balance between sensitivity and robustness against noise.

V. Proposed Approach

Our proposed method relies on three key factors: corrected raw INS data, a supervised LSTM algorithm, and the modified M-of-N method. First, we model two categories of INS, tactical and low-cost, using the model described in Section I with adjustment of the appropriate characteristics for each category. The data from the tactical-grade INS are used with the LSTM algorithm to correct the raw data from the low-cost INS. Next, the simulated GPS data are employed to estimate accelerations and angular rates. The difference between the corrected low-cost INS data and the GPS-estimated values is then computed. Finally, the M-of-N method is applied to detect GPS spoofing by setting a threshold to identify discrepancies between the two data sources.

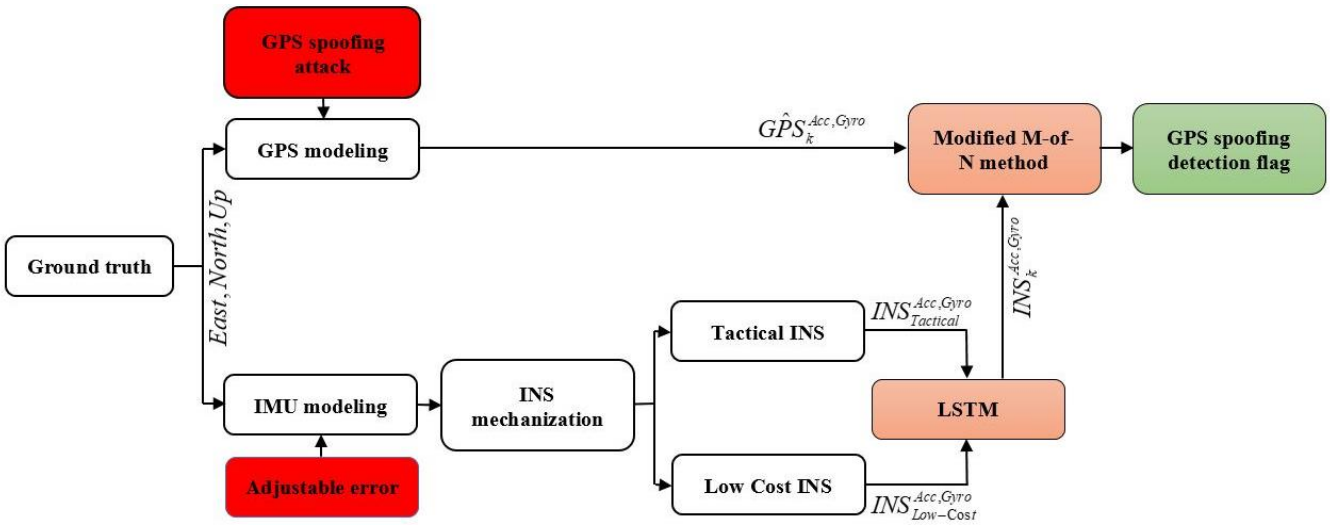


Fig. 6. The proposed approach.

The proposed method is highlighted in Fig. 6, showing the process steps from the initial INS sensor modeling to the final stage of GPS spoofing detection using the modified M-of-N method. The process begins with modeling the tactical and low-cost INS systems, followed by applying the LSTM algorithm for data correction. The simulated GPS data is then integrated to estimate motion parameters, which are compared to the corrected INS data. Discrepancies between these two sources are assessed using the modified M-of-N method, allowing for precise identification of GPS spoofing events.

Algorithm 1 provides a step-by-step description of the developed approach to detect GPS spoofing attacks using corrected inertial data.

Algorithm 1: GPS spoofing detection using corrected INS and modified M-of-N method

Initialization :
- Set Counetr1=0;
- Set Counetr2=50;
- Parameters : M=50, N=35, C=3;

Computation:
While (new data is available) do
  For (each point k of the trajectory) do
  Compute residual errors E_k^{Acc} and E_k^{Gyro}
  Calculate detection thresholds Th^{Acc} and Th^{Gyro}
    If ($E_k^{Acc} > Th^{Acc}$ & $E_k^{Gyro} > Th^{Gyro}$) then
      Increment counter1
    Else
      If (counter2) then
        Decrease counter2
      Else
        Move to the next trajectory point k+1
    If (Counter1≥35) then
      Confirm the presence of GPS spoofing
    Else
      Reinitialize Counter1=0 and reset Counter2=50
  End
  End

VI. Simulation and Results

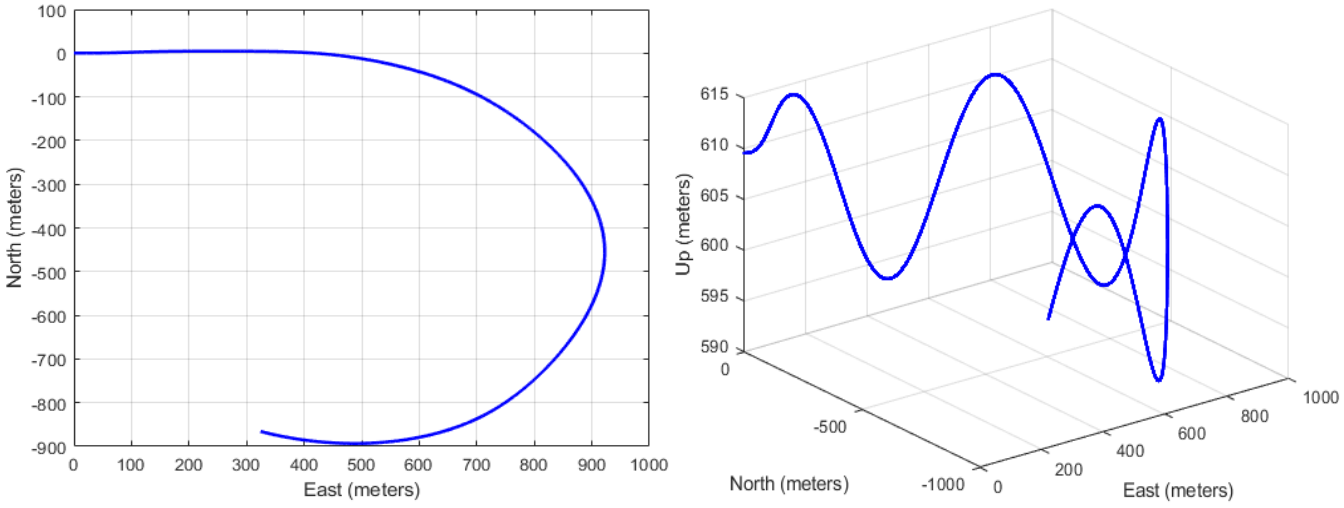
A. Simulation Platform

The experience was conducted using the MATLAB environment. The simulation begins by generating a reference trajectory with a total duration of 50 minutes. This ground truth trajectory incorporates both straight paths and complex curves, along with changes in the vertical (Up) direction, to emulate a realistic urban transportation scenario, as depicted in Fig. 7. These variations aim to reflect the dynamic conditions often encountered in such environments, providing a more accurate representation for evaluating the system's performance in challenging navigation contexts. Additionally, ten spoofing attacks were carried out on the GPS signal at separate intervals along the trajectory.

B. LSTM Correction of Low-Cost INS Data

The key characteristics of the two grades of INS include the levels of bias, scale factor, and noise, which directly affect both the accelerometers and gyroscopes. In this paper, the values were selected based on the specifications of existing and commercially available INS. The main characteristics of each grade of INS are summarized in Table III, highlighting the differences in performance and precision between the low-cost and tactical models.

Using the characteristics of each INS grade and based on the INS modeling equations presented in Section I, we modeled the six sensors composing both the low-cost and tactical INS grades. The result of this modeling process was the simulated outputs of the sensors in terms of specific forces and angular rates. Fig. 8 and Fig. 9 illustrate the comparison between the reference values, the estimated measurements from the low-cost INS sensors, and the estimated measurements from the tactical INS sensors. This comparison highlights the performance differences between the two grades, with the tactical INS showing improved accuracy and lower error margins compared to the low-cost INS.

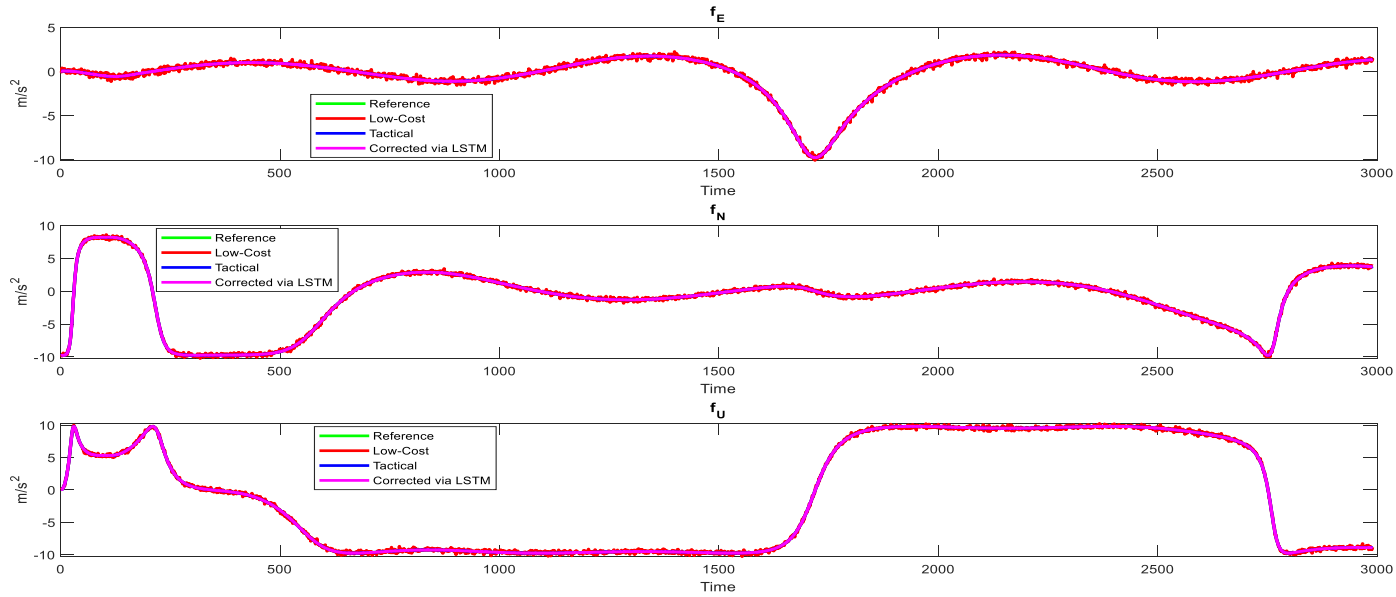


(a) (b)

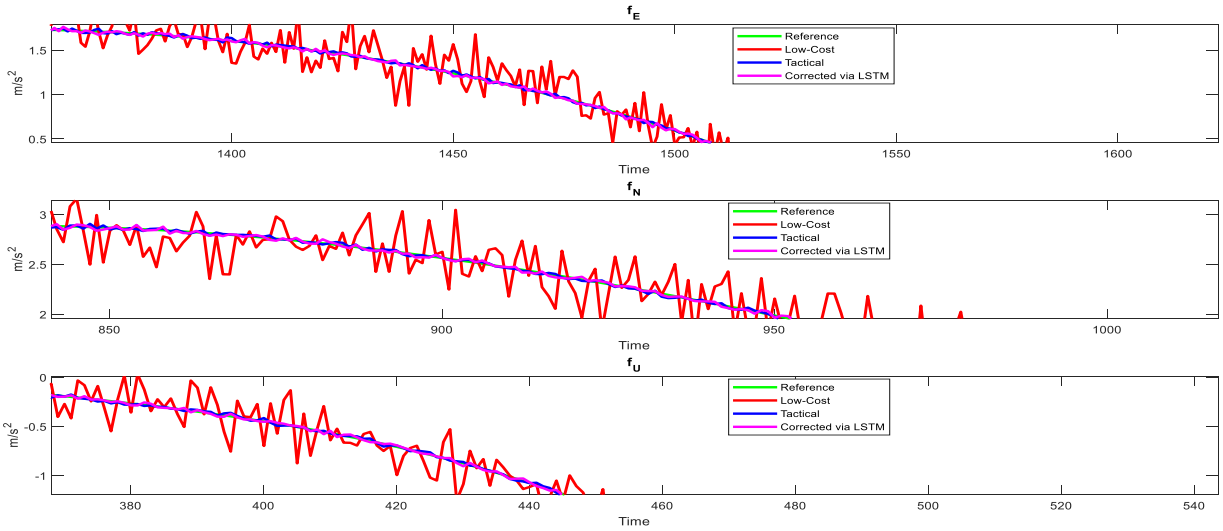
Fig. 7. Reference trajectory for urban transportation simulation: 2D overview (a) and 3D overview (b).

TABLE III. KEY CHARACTERISTICS OF LOW-COST AND TACTICAL INS MODELS [29] [30]

Key characteristics	**INS grade**	
	Low Cost	***Tactical***
Gyroscopes		
Noise	0.1°/s/√Hz	0.01°/s/√Hz
Bias	<±1.5 deg/s	<±0.0055 deg/s
Scale factor	<2%	<0.15%
Accelerometers		
Noise	500 µg/√Hz	50 µg/√Hz
Bias	1 mg	0.1 mg
Scale factor	<1%	<0.4%
Range	±6 g	±10 g

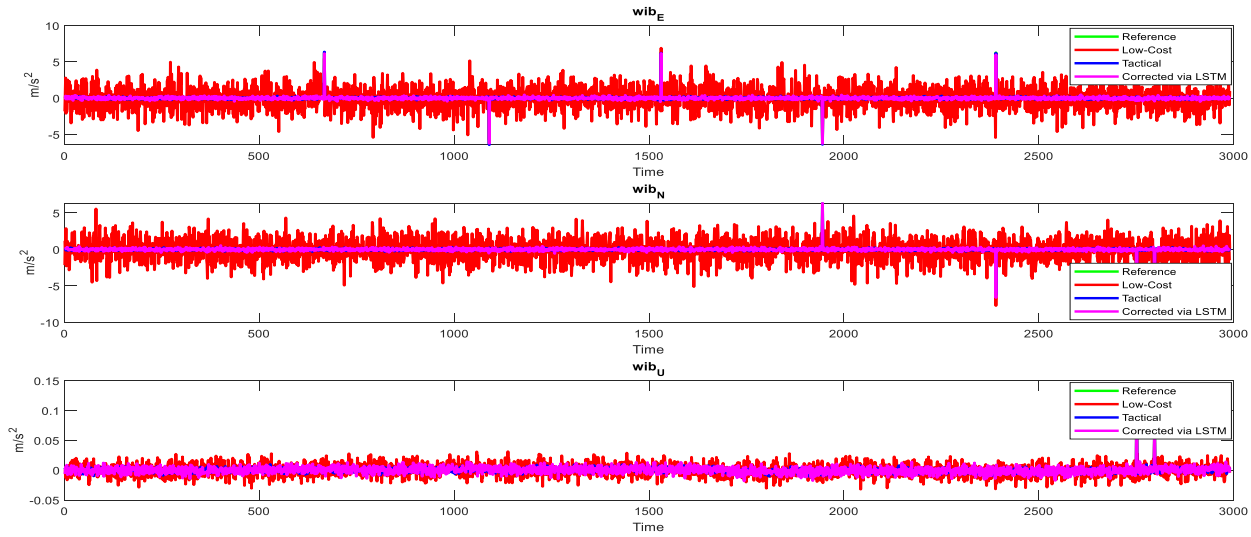


(a)

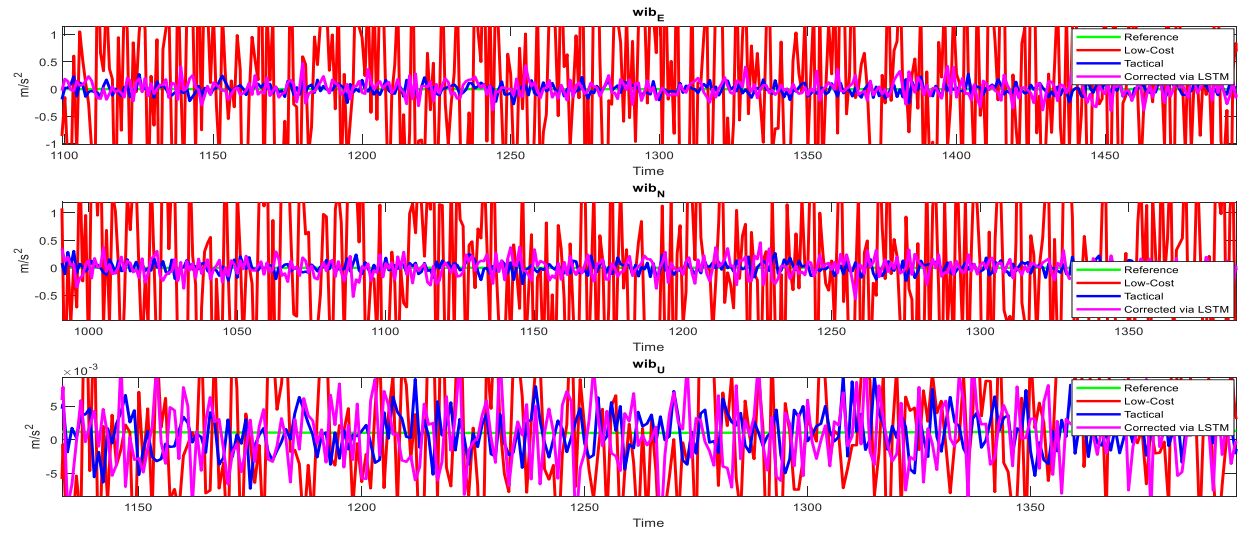


(b)

Fig. 8. Comparison of accelerometer outputs from reference, Low-Cost INS, tactical INS, and corrected data: (a) Full view and (b) Zoomed-in view.



(a)



(b)

Fig. 9. Comparison of gyroscope outputs from reference, Low-Cost INS, tactical INS, and corrected data: (a) Full view and (b) Zoomed-In view.

The Root Mean Square Error (RMSE) is the metric used to highlight the deviation from the reference for the low-cost INS, the tactical INS, and the corrected data. Table IV presents the calculated metric in the three directions (E, N, and U) for each grade. The equation of this metric is given in Eq. (16) [31].

$$RMSE^2 = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2 \quad (16)$$

Where y_i = Actual value, $\hat{y}_i$ = Estimated value, and n = Number of observations.

TABLE IV. RMSE FOR LOW-COST INS, TACTICAL INS, AND CORRECTED DATA IN EAST, NORTH, AND UP DIRECTIONS

Direction	RMSE					
	Low-Cost INS		*Tactical INS*		*Corrected data*	
	Accelo	*Gyro*	*Accelo*	*Gyro*	*Accelo*	*Gyro*
E (East)	1.97	1.48	0.11	0.10	0.18	0.15
N (North)	2.03	1.52	0.97	0.12	1.04	0.19
U (Up)	2.94	2.13	1.12	0.83	1.68	1.12
Total RMSE	2.36	1.74	0.86	0.49	1.15	0.66

The results show a significant reduction in RMSE values when comparing the low-cost INS to the corrected data via LSTM. The low-cost INS determines higher errors in all directions, with a total RMSE of 2.36 m/s² for accelerometers and 1.74 rad/s for gyroscopes. Due to its higher precision, the tactical INS achieves a notable decrease in RMSE, particularly in the East and North directions, resulting in a total RMSE of 0.86 m/s² for accelerometers and 0.49 rad/s for gyroscopes. The corrected data, representing the application of the LSTM algorithm for error mitigation, shows improved performance over the low-cost INS, with a total RMSE of 1.15 m/s² for accelerometers and 0.66 rad/s for gyroscopes, indicating successful error reduction.

C. GPS Spoofing Detection via M-of-N Method

To test our detection method, we have introduced ten zones of GPS spoofing along the trajectory, each lasting 60 points. Using the corrected accelerations and angular rates with estimated values from GPS, we applied the modified M-of-N method to detect GPS spoofing. As depicted in Fig. 10, the method detected eight of the 10 zones. This indicates good performance in detecting GPS spoofing, achieving a detection percentage of 80%. However, two zones were not detected due to the spoofing signal's similarity to the true GPS data or to the duration of spoofing in these zones, set to 60 points, was insufficient for the method to accumulate the required number of consecutive detections, leading to missed detections. These limitations suggest the need for refining the detection thresholds or increasing sensitivity in specific regions to improve overall performance.

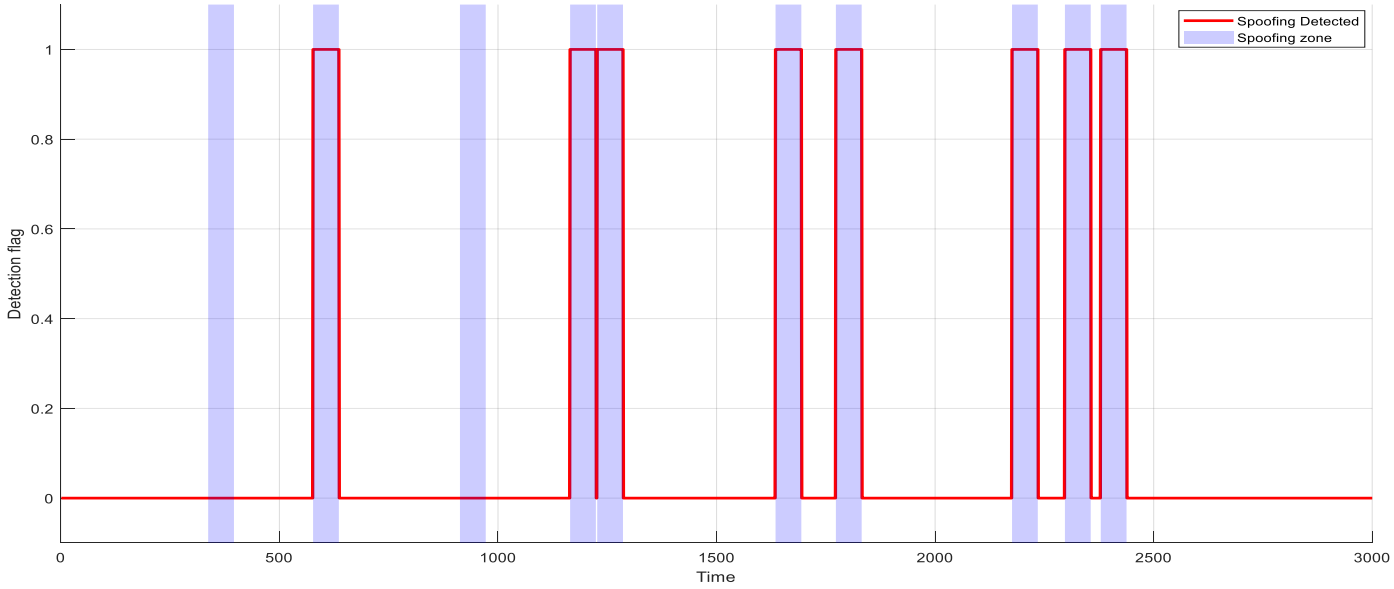


Fig. 10. Detection of GPS spoofing zones along the trajectory.

VII. CONCLUSION

This paper presents a GPS spoofing detection technique that integrates artificial intelligence algorithms with data from INS. By exploiting an LSTM algorithm to correct inherent INS errors, the proposed approach significantly improves the accuracy of the INS measurements, as evidenced by the reduction in the RMSE values. The corrected accelerations and angular rates are used in combination with the modified M-of-N method to detect spoofing by comparing INS outputs with GPS-estimated values. Experimental results demonstrate that the approach successfully detected 80% of the introduced spoofing zones. However, some zones were not detected, likely due to similarities between the spoofed and true GPS signals or the limited duration of the spoofing events, which did not provide enough consecutive detections for confirmation. These findings highlight the potential of the proposed technique but also indicate areas for further refinement, such as optimizing detection thresholds and improving sensitivity in specific segments of the trajectory to achieve reliable spoofing detection in diverse scenarios.

VIII. Future Work

Although the modified M-of-N method demonstrated promising results in detecting GPS spoofing attacks, it revealed certain limitations. One of the main challenges is its sensitivity to transient anomalies, which can lead to false positives in the detection process. To address these limitations, our future work will explore the robustness of both the K-consecutive alarm method and the modified Tong method. We will then compare the performances of these three approaches to identify the most effective solution for GPS spoofing detection.

References

[1] Phudinan Singkhamfu, Parinya Suwansrikham, "An Experiment for Outdoor GPS Localization Enhancement using Kalman Filter with Multiantenna Consumer-Grade Sensors," International Journal of Advanced Computer Science and Applications, Vol. 12, No. 4, 2021.

[2] Cuntz, M., Konovaltsev, A., Dreher, A., Meurer, M, "Jamming and Spoofing in GPS/GNSS Based Applications and Services – Threats and Countermeasures, " In: Aschenbruck, N., Martini, P., Meier, M., Tölle, J. (eds) Future Security. Future Security 2012. Communications in Computer and Information Science, vol 318. Springer, Berlin, Heidelberg, 2012, https://doi.org/10.1007/978-3-642-33161-9_29

[3] Warner, Jon S., and Roger G. Johnston, "GPS spoofing countermeasures," Homeland Security Journal 25.2 (2003): 19-27.

[4] Khan SZ, Mohsin M, Iqbal W, "On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions, " PeerJ Computer Science 7:e507, https://doi.org/10.7717/peerj-cs.507

[5] Aftatah, M., Zebbara, K. (2024), "A Comprehensive Survey on Secure Navigation for Intelligent Systems: Artificial Intelligence Approaches to GPS Jamming and Spoofing Detection," In: Mejdoub, Y., Elamri, A. (eds) Proceeding of the International Conference on Connected Objects and Artificial Intelligence (COCIA2024). COCIA 2024. Lecture Notes in Networks and Systems, vol 1123. Springer, Cham. https://doi.org/10.1007/978-3-031-70411-6_17

[6] Guo, Y., Wu, M., Tang, K., Tie, J., & Li, X, "Covert Spoofing Algorithm of UAV Based on GPS/INS-Integrated Navigation, " IEEE Transactions on Vehicular Technology, 68(7), 2019, 6557-6564, https://doi.org/10.1109/TVT.2019.2914477

[7] Talaei Khoei, T.; Ismail, S.; Shamaileh, K.A.; Devabhaktuni, V.K.; Kaabouch, N, "Impact of Dataset and Model Parameters on Machine Learning Performance for the Detection of GPS Spoofing Attacks on Unmanned Aerial Vehicles, " Appl. Sci, 2023, 13, 383.

[8] Wei, X.; Wang, Y.; Sun, C, "PERDET: Machine-Learning-Based UAV GPS Spoofing Detection Using Perception Data," Remote Sens. 2022, 14, 4925. https://doi.org/10.3390/rs14194925

[9] Semanjski, S., Semanjski, I., De Wilde, W., & Muls, A, "Use of Supervised Machine Learning for GNSS Signal Spoofing Detection with Validation on Real-World Meaconing and Spoofing Data—Part I, " Sensors, 20(4), 1171, 2020, https://doi.org/10.3390/s20041171

[10] Sun, Y., Yu, M., Wang, L., Li, T., & Dong, M, "A Deep-Learning-Based GPS Signal Spoofing Detection Method for Small UAVs, " Drones, 7, 370, 2023.

[11] Kwon, K.-C., & Shim, D.-S, "Performance Analysis of Direct GPS Spoofing Detection Method with AHRS/Accelerometer, " Sensors, 20(4), 954, 2020.

[12] Khanafseh, S., Roshan, N., Langel, S., Chan, F.-C., Joerger, M., & Pervan, B, "GPS Spoofing Detection using RAIM with INS Coupling, " Sensors, 20(4), 1171, 2020.

[13] Shafique, A., Mehmood, A., & Elhadef, M, "Detecting Signal Spoofing Attack in UAVs Using Machine Learning Models, " IEEE Access, 3089847, 2021, https://doi.org/10.1109/ACCESS.2021.3089847

[14] Manesh, M. R., Kenney, J., Hu, W. C., Devabhaktuni, V. K., & Kaabouch, N, "Detection of GPS Spoofing Attacks on Unmanned Aerial Systems, " IEEE Transactions on Vehicular Technology, 68(7), 6557-6564, 2020.

[15] Franček, Petar, Kristian Jambrošić, Marko Horvat, and Vedran Planinec, "The Performance of Inertial Measurement Unit Sensors on Various Hardware Platforms for Binaural Head-Tracking Applications," Sensors 23, no. 2: 872, 2023, https://doi.org/10.3390/s23020872

[16] Liu, Jianfeng & Pu, Jiexin & Sun, Lifan & He, Zishu., "An Approach to Robust INS/UWB Integrated Positioning for Autonomous Indoor Mobile Robots, " Sensors. 19. 950, 2019, https://doi.org/10.3390/s19040950

[17] Oliveros, Juan Carlos, and Hashem Ashrafiuon, "Multi-Vehicle Navigation Using Cooperative Localization," Electronics 12, no. 24: 4945, 2023, https://doi.org/10.3390/electronics12244945

[18] Negru, Sorin Andrei, Patrick Geragersian, Ivan Petrunin, and Weisi Guo, "Resilient Multi-Sensor UAV Navigation with a Hybrid Federated Fusion Architecture," Sensors 24, no. 3: 981, 2024, https://doi.org/10.3390/s24030981

[19] AFTATAH M, ZEBBARA K, "Modeling Low-cost Inertial Navigation Systems and Their Errors, " International Journal of Computer Networks & Communications (IJCNC), Vol.16, No.6, November 2024.

[20] Krystian Borodacz, Cezary Szczepański, "Impact of Motion-Dependent Errors on the Accuracy of an Unaided Strapdown Inertial Navigation System, " Sensors, Volume 23, Issue 7, 2023, Article 3528.

[21] Boguspayev, N., Akhmedov, D., Raskaliyev, A., Kim, A., Sukhenko, A, "A Comprehensive Review of GNSS/INS Integration Techniques for Land and Air Vehicle Applications, " Appl Sci, 2023;13:4819.

[22] Mahdi, AE, Azouz, A, Abdalla, AE, Abosekeen, A, "A Machine Learning Approach for an Improved Inertial Navigation System Solution, " Sensors, 2022;22:1687.

[23] Yabo Wang, Ruihan Jiao, Tingxiao Wei, Zhaoxing Guo, Yueyang Ben, "A Method for Predicting Inertial Navigation System Positioning Errors Using a Back Propagation Neural Network Based on a Particle Swarm Optimization Algorithm, " Sensors, Volume 24, Issue 12, 2024, Article 3722.

[24] Saleh S, Bader Q, Karaim M, Elhabiby M, Noureldin A, "Integrated 5G mmWave Positioning in Deep Urban Environments: Advantages and Challenges, " In Proceedings of the 2023 IEEE Global Communications Conference (GLOBECOM). IEEE, 2023. p. 195-200.

[25] AFTATAH M, ZEBBARA K, "Robust ConvNet-Kalman Filter Integration for Mitigating GPS Jamming and Spoofing Attacks Basing on Inertial Navigation System Data," Data and Metadata [Internet]. 2024 Jan. 1 [cited 2024 Sep. 28];3:.405. https://doi.org/10.56294/dm2024.405

[26] Jafarnia-Jahromi A, Broumandan A, Nielsen J, Lachapelle G, "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques, "International Journal of Navigation and Observation, 2012, https://doi.org/10.1155/2012/127072

[27] Liu, Fuchao, Hailin Zhao, and Wenjue Chen, "A Hybrid Algorithm of LSTM and Factor Graph for Improving Combined GNSS/INS Positioning Accuracy during GNSS Interruptions," Sensors 24, no. 17: 5605, 2024, https://doi.org/10.3390/s24175605

[28] Cao, Yu, Hongyang Bai, Kerui Jin, and Guanyu Zou, "An GNSS/INS Integrated Navigation Algorithm Based on PSO-LSTM in Satellite Rejection," Electronics 12, no. 13: 2905, 2023, https://doi.org/10.3390/electronics12132905

[29] Zhang, Chunxi, Xianmu Li, Shuang Gao, Tie Lin, and Lu Wang, "Performance Analysis of Global Navigation Satellite System Signal Acquisition Aided by Different Grade Inertial Navigation System under Highly Dynamic Conditions," Sensors 17, no. 5: 980, 2017, https://doi.org/10.3390/s17050980

[30] Aboutaleb, Ahmed, Amr S. El-Wakeel, Haidy Elghamrawy, and Aboelmagd Noureldin, "LiDAR/RISS/GNSS Dynamic Integration for Land Vehicle Robust Positioning in Challenging GNSS Environments," Remote Sensing 12, no. 14: 2323, 2020, https://doi.org/10.3390s/rs12142323

[31] AFTATAH M, ZEBBARA K, "Evaluating the impact of convolutional neural network layer depth on the enhancement of inertial navigation system solutions, " International Journal of Computer Networks & Communications (IJCNC), Vol.16, No.5, September 2024, DOI: 10.5121/ijcnc.2024.16504