Date of publication JUN-30, 2025, date of current version MAY-29, 2025.
www.computingonline.net / computing@computingonline.net

Print ISSN 1727-6209
Online ISSN 2312-5381
DOI 10.47839/ijc.24.2.4008

High-Precision Detection of GPS Spoofing Attacks on UAVs Using MLP

VASYL LYTVYN[1], IVAN PELESHCHAK[1], YAROSLAV STEPANIAK[1], ROMAN PELESHCHAK[1], OLEKSII ISHCHUK[2]

[1]Lviv Polytechnic National University, Lviv, 79013 Ukraine
[2]The Specialist Hospital in Sanok Autonomous Public Healthcare Centre, Sanok, 38500 Poland

Corresponding author: Ivan Peleshchak (e-mail: ivan.r.peleshchak@lpnu.ua).

The research was carried out with the grant support of the National Research Fund of Ukraine "Methods and means of active and passive recognition of mines based on deep neural networks", project registration number 273/0024 from 1/08/2024 (2023.04/0024). Also, we would like to thank the reviewers for their precise and concise recommendations that improved the presentation of the results obtained.

ABSTRACT This work addresses the problem of detecting GPS spoofing attacks on Unmanned Aerial Vehicles (UAVs) using a multilayer perceptron (MLP). Such attacks allow adversaries to inject artificial signals of increased power that confuse the drone's navigation system and cause deviations from its planned route. The open-source TEXBAT dataset was used for experimental research, with separate highlights of the DS3 and DS7 scenarios that simulate synchronous GPS spoofing. During the data preparation stage, the signal parameters (pseudorange, power, and Doppler shift) were leveraged, and their statistical analysis was performed using correlation matrices and mean-value distributions. The proposed MLP model, featuring an optimized architecture with three hidden layers and a sigmoid activation function at the output, demonstrated a detection accuracy of 93% on the validation data. The advantages of this approach include high performance and ease of integration into navigation systems. However, the relatively small amount of real data limits scalability and comprehensiveness of the evaluation.

KEYWORDS GPS spoofing; Unmanned Aerial Vehicles (UAVs); Multilayer Perceptron (MLP); TEXBAT.

I. INTRODUCTION

The importance of security measures for telecommunication and electronic systems has grown significantly, prompting the development of various methods for signal protection. This is due to the fact that smart devices and unmanned aerial vehicles (UAVs, drones) use their communication systems [1], which are typically based on Internet of Things (IoT) networks and GPS channels. GPS-based communication systems between UAVs and satellites face two main threats: jamming and spoofing attacks [1]. During a jamming attack, the attacker aims to cause a denial of service (DOS) (Disk Operating System), so that the UAV cannot receive GPS signals. During a spoofing attack, the attacker creates a replica of the GPS signal and boosts its power so that it becomes the UAV's positioning reference. The increased power affects the correlation between signals from the GPS and the navigation system. Therefore, once the spoofed signal is transmitted to the UAV, it ignores the genuine GPS signal [2] and begins to drift from its original path.

In a spoofing attack, the targeted UAV is unable to immediately detect the deviation because, if the attack is effectively executed, there are no abrupt changes in the received GPS signal. Furthermore, there is no known correct location that could help the UAV detect the drift. For these reasons, spoofing attacks are difficult to detect. In addition, the attacker gains the ability to move the targeted UAV by changing the characteristics of the reference signal.

Global Positioning System (GPS) signals require reliable protection against attacks. One of the most common types of threats is GPS spoofing, whose goal is to deceive the receiver by transmitting fake signals. The attacker increases power until the fake signal overpowers the real one, which confuses the missile. Typically, such signals have a slightly higher power than authentic ones. They can be generated by delaying and re-emitting protected GPS signals [3]. Since GPS systems use wireless communication, receivers are vulnerable to cyberattacks, including GPS spoofing. A spoofer (attacker) generates fake GPS signals and transmits them [4]. A nearby GPS receiver tracks these spoofed signals and thus obtains incorrect timestamps [5].

The task of early warning and detection of SPOOFING attacks on unmanned aerial vehicles (UAVs) and drones is particularly relevant in the military sphere. UAVs are frequently used not only for military purposes but also for logistics. Commercial UAVs can operate autonomously for tasks such as cargo delivery, infrastructure monitoring, and agriculture [6]. A large number of civilian UAVs use control and navigation systems that rely on unencrypted and unauthenticated signals broadcast by the Global Positioning

System (GPS). Consequently, they are vulnerable to GPS spoofing attacks.

Over the past decade, a number of studies have focused on security issues related to aircraft and navigation. In recent years, UAVs have become increasingly popular and, consequently, more vulnerable in terms of security. The most common threats to UAVs rely on Internet of Things (IoT) protocols or GPS communication.

The authors of [7] categorize UAV threats into three types: navigation attacks (hijacking), routing attacks (based on IoT networks), and data attacks (where data are stolen from captured drones). Regarding navigation attacks, jamming and spoofing attacks are identified as the primary threats.

Several works have been dedicated to detecting spoofing attacks. In [8], the Monte Carlo method is employed to compare two detectors: the sum-of-squares detector and the D^3 detector. The authors of [2] take a more traditional approach: they test models such as the Bayesian classifier and the k-nearest neighbors (K-NN) classifier, achieving accuracies of 62.31% and 77.29%, respectively, when detecting synchronous spoofing attacks.

Due to the rapid growth of data volumes and limited resources for their annotation, recent studies have paid special attention to the optimal selection of training samples. In [9], strategies were introduced that combine classifier uncertainty (margin sampling) with sample diversity (k-center clustering), enabling the same level of accuracy to be achieved using 30 % less data. The authors of [10] analyzed the sample size requirements for popular classification algorithms (RF, SVM, KNN, and Naive Bayes) and identified empirical relationships between dataset characteristics (minority class proportion, nonlinearity, number of features) and the number of samples needed to reach an AUC within 0.02 of that obtained on the full dataset.

The use of the Haar wavelet transform as a feature-extraction method for classification is gaining popularity. In [11], a visual-information classification method based on Haar wavelet coefficients and their Shannon-entropy measurement was proposed, resulting in a 20 % reduction in class-boundary detection time without any loss in accuracy.

In [2], the authors explore the use of supervised learning algorithms to detect GPS spoofing attacks on UAVs. They compared three models, training each on labeled examples of UAV sensor data from both normal autonomous flights and GPS spoofing attacks, then comparing their performance. They also repeated the tests with Gaussian noise added to the dataset and with a reduced amount of spoofing data. The evaluated models included a support vector machine (SVM) classifier with principal component analysis (PCA) for dimensionality reduction, a logistic regression classifier with a long short-term memory (LSTM) autoencoder for dimensionality reduction, and a logistic regression classifier with a standard autoencoder. The combination of PCA and SVM was the most effective model in all tests.

In [8], researchers compared several supervised and unsupervised learning models for detecting GPS spoofing attacks on UAVs. Most research on detecting UAV GPS spoofing using machine learning focuses on supervised approaches, making this particular work unique. The unsupervised models compared were PCA, k-means clustering, and an autoencoder. These models analyze a dataset of unlabeled GPS signals and attempt to classify anomalies. They use various signal features, which makes this approach less suitable for civilian UAVs with basic equipment.

In [12], the researchers compared three one-class classifiers for detecting GPS spoofing and jamming in UAVs, aiming to find the best model for general UAV attack detection. This study also provided the dataset used in [2]. One-class classification (the main focus of this study) is typically considered a form of unsupervised learning. In this context, only benign data are provided to the classifier for training, and the trained model must then classify samples from the test data as either belonging to those training data or as outliers. This is well-suited for detecting GPS spoofing in civilian UAVs, as it is unlikely that civilians would have access to the data or equipment needed to conduct spoofing. The algorithms compared were Local Outlier Factor, an autoencoder, and a one-class support vector machine.

In [13], a multilayer perceptron was developed to process flight parameters and GPS signals, signaling GPS spoofing attacks on UAVs. The accuracy achieved in [13] ranges from 83.23% for the TEXBAT dataset to 99.93% for the MAVLINK dataset.

Summarizing the results of previous studies on the detection of synchronous spoofing attacks, one can see that their accuracy ranges from 93.4% to 99%. An important drawback of these studies is their use of synthetic datasets and the lack of comparison with other deep learning models. Only one general dataset (based on simulated flight parameters) has been used for verifying spoofing attack detection [14], but overall metrics for comparison with other research were not considered.

Although the above-mentioned methods are robust and theoretically grounded, they are not capable of quickly detecting deviations from the target UAV's original course during spoofing attacks, since in the case of synchronous SPOOFING, there are no abrupt changes in the received GPS signal. Moreover, there is no information about the UAV's true position to help it recognize drift (deviation). For these reasons, spoofing attacks are difficult to detect.

The goal of our work is to develop an optimized MLP architecture to detect GPS spoofing attacks on UAVs with high accuracy (>90%).

II. MATERIAL AND METHODS

A. TYPES OF GPS SPOOFING ATTACKS

For UAV flight path determination and navigation, a connection between GPS satellites and the UAV is required. UAV navigation relies on a minimum of four satellites. In addition, GPS satellites provide positional referencing for the UAV [8]. To improve accuracy and security, sensors such as inertial measurement units, magnetometers, and gyroscopes are often used [8].

An attacker can use either a synchronous spoofing attack [1] or an asynchronous one. In a synchronous spoofing attack [1] (Figure 1 – curve solid line), the attacker tracks the target UAV, which makes it possible to precisely determine its location and obtain the corresponding reference GPS signal (Figure 1 – solid straight line). The attacker generates a spoofed signal that is a copy of the reference signal but with a higher power than the authentic one. The spoofed signal, sent back to the target UAV, becomes the new "reference" signal because of its higher power. As a result, the attacker gains the ability to move the UAV by altering the characteristics of the reference signal.

In an asynchronous attack (Figure 1 – dashed line), the attacker does not control the target's GPS reference signal. Generating a spoofed signal without knowledge of the reference signal leads to differences in the signal characteristics and simply broadcasts a different location to the UAV. Thus, in an asynchronous attack, abrupt positional changes are transmitted to the UAV, making these attacks easier to detect than synchronous attacks [1].

Figure 1 shows the power-versus-phase relationships for three types of signals: the synchronous spoofing signal (curve solid line); the asynchronous spoofing signal (dashed line); the authentic GPS signal (solid straight line).

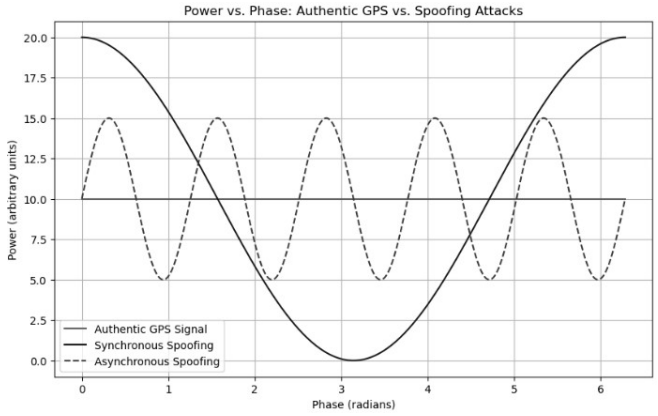


Figure 1. Signal graphs of synchronous, asynchronous spoofing attacks and authentic GPS signal in power-phase coordinates.

As can be seen from Figure 1, the power of the authentic GPS signal remains constant for all phase values, which is a characteristic feature of a genuine satellite GPS signal. This is explained by the fact that satellites provide a uniform signal to ground receivers. The absence of power fluctuations allows the system to determine coordinates with high accuracy.

The power of the synchronous spoofing signal changes smoothly depending on the phase value, indicating synchronized spoofed signals. The UAV's software-defined radio (SDR) accepts these fake signals as legitimate, causing the UAV to follow an incorrect route defined by the synchronous spoofing signal.

The power of the asynchronous spoofing signal fluctuates unevenly with respect to the phase value due to the mismatch of phases and amplitudes in the spoofed signals. The irregularity in power is explained by random changes in the phases and amplitudes of the signals, which can result in chaotic UAV behavior—abrupt course changes, loss of control, or even crashes.

This approach to signal analysis helps identify spoofing attacks based on the nature of power changes relative to phase values. These characteristics are used in security systems to detect spoofing attacks by examining signal power and phase behavior.

For effective protection of UAVs and FPV drones from GPS spoofing attacks, it is advisable to combine several approaches. For example, one can integrate multi-channel signal analysis, use INS, employ encrypted data, and apply machine learning.

To monitor multi-channel signals, it is worthwhile to use software-defined radios (SDRs), which can detect and analyze anomalies in the signals. These receivers can simultaneously analyze signals from several satellites and compare parameters such as power, phase, and frequency.

Multi-factor signal authentication systems use algorithms that encrypt the satellite's data, and the receiver verifies the authenticity of the signal using predefined keys.

Based on an analysis of the signal's time characteristics (Time-Based Analysis) — specifically the time of arrival (ToA) — the distance to the signal source can be determined. Authentic signals have an expected time of arrival corresponding to the distance between the satellite and the receiver. Spoofed signals may exhibit an incorrect time of arrival. For example, an algorithm based on Time Difference of Arrival (TDoA) can calculate the precise location of the signal source and detect fake transmitters.

In cases where spoofing is suspected, the drone switches to an inertial navigation system (INS), which operates on gyroscopes and accelerometers, or it can use alternative satellite systems such as Galileo, BeiDou, or GLONASS.

Deep neural networks (MLP, CNN, LSTM, GRU) [15–17], as well as their combinations, can automatically detect differences in real time between authentic GPS signals and spoofed signals.

B. GPS SPOOFING ATTACK DETECTION ON UAVS

The GPS spoofing attack detection algorithm for UAVs includes the following steps:

1. Intercepting GPS signals (Intercept). This is done using an SDR (Software-defined radio). An SDR is a radio system that uses software to perform functions such as modulation, demodulation, signal processing, and frequency changes. Instead of dedicated hardware, software-configurable equipment is used, which can be adapted to work with different frequencies and communication protocols such as GSM, LTE, Wi-Fi, and Bluetooth. The SDR receives real-time GPS signals transmitted by satellites to the UAV, analyzing their frequency, modulation, and structure. These signals contain data about the satellite's coordinates, the signal transmission time, and error correction algorithms.

2. Generating spoofed GPS signals (Spoofing). The spoofer (attacker) creates a fake GPS signal that "imitates" the signal from a satellite. This signal transmits false coordinate or timing data and alters the UAV's location coordinates. By using SDR, the attacker can modify navigation parameters (coordinates, altitude) and mimic authentic satellite signals. The signal power is increased so that the UAV "trusts" it more than the real satellite signals. Specifically, based on GPS-SDR-SIM software, the attacker creates a signal with spoofed coordinates. This signal is transmitted via SDR at a power level sufficient to override the genuine satellite signals [18–20].

3. Transmitting a higher-power signal. The SDR broadcasts the spoofed GPS signal with greater power than that of the legitimate satellite signals. This boosted power affects the correlation between the GPS signals and the navigation system. Consequently, once the spoofed signal is sent to the UAV, it ignores the real GPS signal [2] and begins to drift (deviate) from its original path. An SDR device, such as HackRF One or USRP, allows the attacker to adjust amplitude and transmission frequency in order to "fool" the UAV's GPS receiver. For example, a fake signal at a frequency of 1575.42 MHz could be transmitted at -50 dBm, whereas legitimate satellite signals arrive at about -120 dBm. The GPS receiver automatically selects the stronger signal.

4. Deviation from the route (Manipulation). After accepting the spoofed signal, the UAV changes its route; in other words, it "believes" it is at a different location and starts to execute commands corresponding to that new position. All GPS parameters (coordinates, altitude, speed) can be changed in real time, enabling precise control over the UAV's route. For instance, a UAV intended to fly to location A now perceives coordinates for location B and may land at that specified point.

An attack scenario with a real-world example of "drone hijacking" involves an attacker transmitting a signal with coordinates corresponding to their own location, causing the UAV to land nearby. More advanced attacks are used to precisely redirect the aircraft to a chosen location [21]. Figure 2 illustrates how an attacker uses GPS spoofing to force an autonomous drone to deviate from its intended destination.

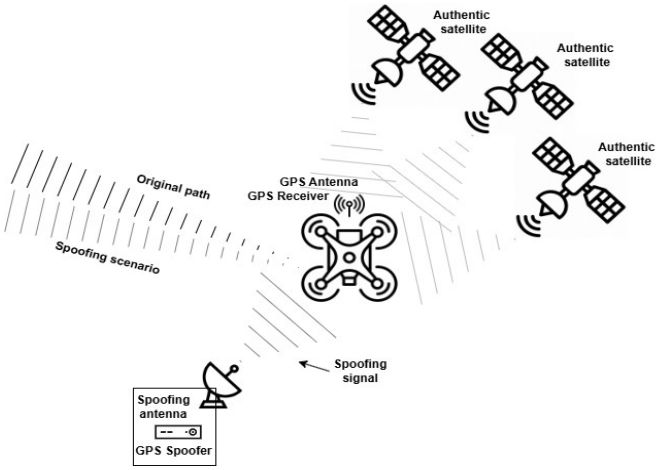


Figure 2. Scheme of how the spoofing signal is applied.

GPS spoofing detection is typically carried out using hardware-based methods that analyze various characteristics of the GPS signal:

1. Analysis of GPS signal amplitudes from satellites and attackers (spoofers). Satellite GPS signals typically have low power because they are transmitted from a great distance. Spoofing signals often have abnormally high amplitude since the spoofer's transmitter is much closer to the receiver. This kind of analysis is performed using RSSI (Received Signal Strength Indicator), based on the following steps: -Measure the signal power for each received satellite signal.

- If several signals exhibit significantly higher power compared to standard values, this may indicate spoofing.

- Hardware implementation is achieved with a GNSS (Global Navigation Satellite System) receiver equipped with integrated signal analyzers [22–24].

2. Analysis of Doppler shift. Due to the relative motion of satellites and the receiver, satellite signals exhibit a predictable Doppler frequency shift. A spoofer usually does not account for these shifts or does so inaccurately. This analysis relies on high-precision GPS receivers, such as those equipped with quartz oscillators, to determine frequency shifts. The hardware module calculates the Doppler shift for each GPS signal. Any anomalies, such as all signals having the same Doppler shift, are indicative of spoofing.

3. Analysis of signal time of arrival (TOA). Authentic GPS signals have different arrival times at the receiver because of varying distances to each satellite. Spoofing signals are typically synchronized to appear credible, but their arrival times may be identical or inconsistent. This analysis is performed by high-precision GNSS receivers equipped with atomic clock–based synchronizers. Specifically:

- The difference in arrival times of signals at the receiver's antenna is analyzed.

- Synchronized arrivals—uncharacteristic of real satellite signals—are identified.

4. Analysis of multipath propagation. Signals from satellites may reflect off objects, creating multipath effects. Authentic GPS signals have a typical multipath profile; spoofing signals can produce an unnatural multipath profile. Multipath analysis is performed by multi-channel GNSS receivers with built-in signal analyzers.

5. Analysis of signal synchronization. GNSS receivers with embedded algorithms analyze signal synchronization. GPS satellites synchronize their signals using atomic clocks. Spoofers often lack this level of synchronization precision. The accuracy of synchronization among several satellites' signals is examined. Any discrepancies in synchronization may indicate spoofing.

6. Use of phased array antenna arrays. For example, CRPA (Controlled Reception Pattern Antennas). Anomalies in the direction of signal arrival can indicate spoofing. Real satellite signals come from different directions based on satellite positions. An antenna array with multiple elements measures the incoming direction of each signal. If all signals arrive from one direction, this suggests spoofing.

7. Use of additional sensors — GNSS receivers integrated with INS. Integrating GPS data with other sensors (inertial, magnetometers, barometers) makes it possible to verify GPS data reliability. GPS data are compared with readings from the Inertial Navigation System (INS) [25]. Discrepancies can be detected, for instance, a change in coordinates that does not align with the UAV's INS-derived speed.

These methods are often combined to ensure reliable detection of GPS spoofing. For instance, modern GNSS receivers for critical applications (aviation, UAVs [26], military systems) can simultaneously use signal power analysis, TOA, and Doppler shift assessment.

C. DESCRIPTION OF THE DATASET AND MODEL

TEXBAT Dataset. TEXBAT [27] is a publicly available dataset commonly used to test the robustness of GPS receivers. It contains digital recordings of authentic static and dynamic GPS L1 C/A spoofing tests. The characteristics of TEXBAT allow the dataset to generalize the problem of spoofing-attack detection, addressing not only UAVs but also any GPS-equipped vehicles.

Among all the spoofing attacks covered by the TEXBAT dataset, scenarios DS3 and DS7 exhibit characteristics of a synchronous spoofing attack. Scenario DS3 is based on static attacks with matched power. Scenario DS7 explores the same spoofing attack as DS3, but with carrier phase alignment. Since DS7 is based on DS3 and introduces new alignment that increases the complexity of intrusion detection, our focus is on scenario DS7.

The TEXBAT dataset contains binary data. Using GRID code [28], we convert the binary file into navigation data, which we then use to train our model in this work.

To detect synchronous GPS spoofing attacks with high accuracy (>90%) based on real TEXBAT data, this paper

proposes an MLP architecture with the following morphology (Figure 3).

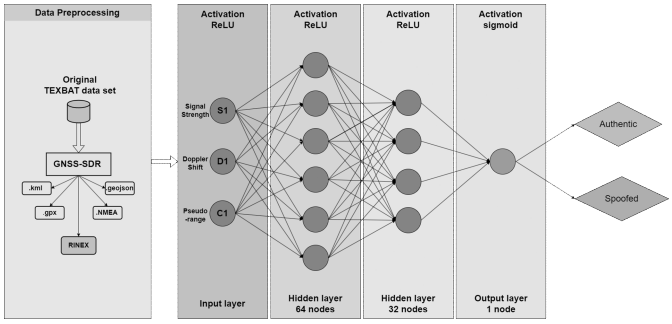


Figure 3. Diagram of a multilayer perceptron model.

After preliminary processing of the TEXBAT data with GNSS-SDR (Global Navigation Satellite System software-defined receiver), we extracted features from the files generated by GNSS-SDR.

After the dataset is processed in GNSS-SDR, the following types of files are obtained, each containing different GNSS data aspects:

1. **rinex** (Receiver INdependent EXchange format)

- A standard format for exchanging GNSS data.
- Contains raw measurements from the GNSS receiver, including pseudorange data, carrier phase, Doppler shift, and signal-to-noise ratio.
- Used for post-processing position, signal analysis, or correction computations.

2. **kml** (Keyhole Markup Language)

- A format for geospatial visualization.
- Contains information on the GNSS receiver's trajectory, including coordinates (latitude, longitude, altitude) and timestamps.
- Used for viewing the route in software such as Google Earth.

3. **gpx** (GPS Exchange Format)

- A format for exchanging GPS data.
- Contains waypoints, tracks, or paths collected by the GNSS receiver.
- Used for route analysis and for uploading data to other GPS devices or navigation apps.

4. **geojson**

- A JSON-based format for storing geospatial data.
- Contains trajectory coordinates along with possible additional information (timestamps, speed, direction of movement).
- Used in geographic information systems (GIS) for data processing and visualization.

5. **nmea** (National Marine Electronics Association)

- A standard format for transmitting GNSS data.
- Contains messages with information on position, speed, time, and other parameters.
- Used for real-time applications and integration with other systems, such as autopilots or mapping programs.

The MLP receives three primary input parameters:

1. Signal Power (S1): This parameter (in dB/Hz) indicates the signal level and its reliability. Attacks are often accompanied by an increase in this value.

2. Doppler Shift (D1): This frequency shift indicates the relative velocity of the satellite with respect to the receiver. Unnatural changes in this parameter signal a potential attack.

3. Pseudorange (C1): This is the distance estimated by the receiver based on the signal transmission time. Deviations indicate possible manipulation.

To ensure the correct operation of the MLP model, a data preprocessing stage is carried out:

1. Data Transformation: Each feature (S1, D1, C1) is normalized to align the input values. Methods such as min-max normalization (0–1 range) or standardization (mean = 0, standard deviation = 1) may be employed.

2. Aggregation by Timestamps: Signal values are averaged for each point in time, reducing data dimensionality and improving processing efficiency.

3. Handling Missing Values: Any missing (NaN) values are handled by either interpolation or by removing incomplete records to avoid errors during model training.

Model Architecture: The MLP model comprises an input layer with 12 neurons. The structure includes three hidden layers with 12, 64, and 32 neurons, respectively, each using the ReLU activation function for efficient training [29-32]. The output layer consists of a single neuron with a sigmoid activation function, which is used for binary classification of the signal as authentic or spoofed. The model is trained using the Adam optimizer with a learning rate of 0.001 and a binary cross-entropy loss function, ensuring stable and accurate classification.

The dataset used in this work consists of two subsets: 3,016 "clean" signal samples and 2,737 spoofed samples, for a total of 5,753 instances. For model training and evaluation of its generalization performance, a 70%/15%/15% split was applied to the training, validation, and test sets, respectively. This corresponds to 4,027 samples in the training set, 863 in the validation set, and 863 in the test set.

III. RESULTS

The MLP model was trained and tested on the TEXBAT dataset, focusing on the DS3 and DS7 spoofing scenarios and the clean scenario. The model achieved a detection accuracy of 93%.

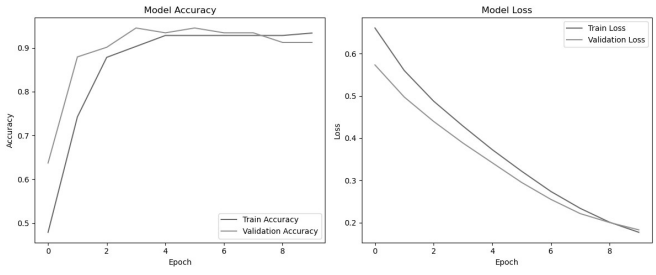


Figure 4. Accuracy and loss graphs over epochs.

To estimate the model's computational cost, we used the THOP library to compute FLOPS per inference. Our model was profiled with THOP using a random input tensor. The resulting value is approximately 24,000 FLOPS per prediction. This assessment confirms the extremely low computational overhead of the MLP network, making it suitable for real-time detection even on embedded platforms.

Correlation matrices were constructed for three types of data: clean, attacked (DS7), and attacked (DS3). These matrices show how the parameters relate to each other. Comparing the three correlation matrices revealed significant

changes in the statistical relationships among key GNSS signal parameters (pseudorange, signal_strength, doppler_shift) in the presence of spoofing attacks.

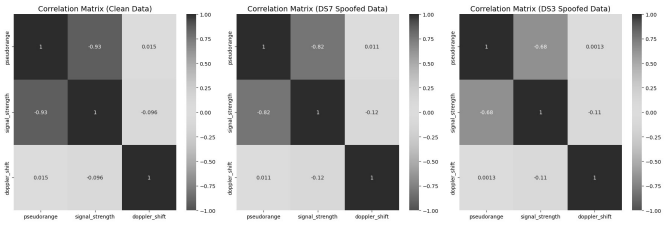


Figure 5. Data correlation matrices.

Clean Data: In non-spoofed data, there is a strong negative correlation (-0.93) between pseudorange and signal strength, which is typical for authentic reception conditions, where an increase in the distance to the satellite is accompanied by a decrease in signal strength. Other indicators (e.g., Doppler shift) do not exhibit significant correlations, reflecting the physical independence of those parameters.

DS7 (phase-aligned spoofing): The correlation between pseudorange and signal_strength decreases to -0.82. This indicates a disruption in the natural relationship between these signal parameters due to the spoofer's interference. In this scenario, the phase and frequency of the spoofed signal were carefully aligned with the authentic signal, so the changes appear rather smooth. However, even this is enough to affect the internal correlation structure.

DS3 (matched-power spoofing without full phase control): The lowest correlation between pseudorange and signal_strength (-0.68) is observed in DS3. This result points to the greatest break in statistical relationships. It may stem from the fact that in DS3 the spoofer did not have a significant power advantage, and phase alignment was less precise. This led to constant interaction between authentic and spoofed signals, creating chaotic interference and distorting the expected correlations.

Even carefully masked spoofing attacks (as in DS7) leave noticeable traces in the statistical characteristics of the signals. A reduction or distortion in the correlation relationships between parameters can be a reliable indicator of an attack. Monitoring changes in the relationship between pseudorange and signal_strength can be particularly effective, as this pair shows the greatest deviations in the presence of spoofed signals.

Additionally, an analysis of the mean distributions of the signal parameters (Pseudorange Mean Distribution, Signal Strength Mean Distribution, Doppler Shift Mean Distribution) was performed for clean vs. spoofed scenarios. The density in the graphs shows the proportion of data values falling into each interval (or histogram bin). The higher the bar, the more data values occur in that interval.

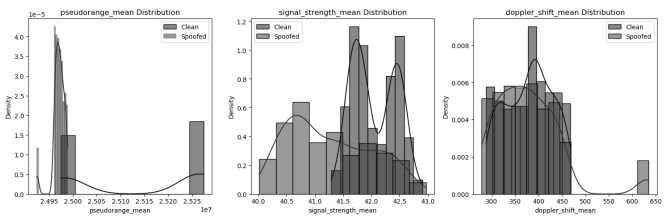


Figure 6. Analysis of the distribution of mean values of signal parameters.

Pseudorange Mean Distribution (left): The chart demonstrates a clear difference between the mean pseudoranges in clean and spoofed data. The clean data exhibits two pronounced peaks at the extreme values, indicating greater spread. The spoofed data has a single, distinct peak in the lower range, suggesting a stable, controlled generation of pseudorange by the spoofer.

Signal Strength Mean Distribution (center): This distribution shows that clean signals have two distinct peaks (around 41.5 and 42.5 dB·Hz), reflecting the natural variation of signal strength in a real environment. The spoofed signals display a smoother, more dispersed distribution with reduced peak values. This may indicate non-constant or unstable signal generation by the spoofer, or partial signal jamming/overlap.

Doppler Shift Mean Distribution (right): This chart reveals the smallest difference between the classes: both groups have similar distributions, with clean data showing a slightly higher concentration around 400 Hz, but overall the values overlap considerably. This confirms that Doppler shift is well-imitated in spoofed scenarios—a typical result of using the frequency lock mode in TEXBAT.

The average values of the signal parameters can serve as additional indicators of spoofing (solid lines). Pseudorange emerges as the most informative, with a pronounced difference in density and peak positions. Signal Strength shows changes in variability that can also be used for detection. Doppler Shift is less informative for detection, since spoofers effectively mimic it.

These distributions can be useful for classification based on statistical features in machine learning tasks.

A combined data correlation matrix was created.

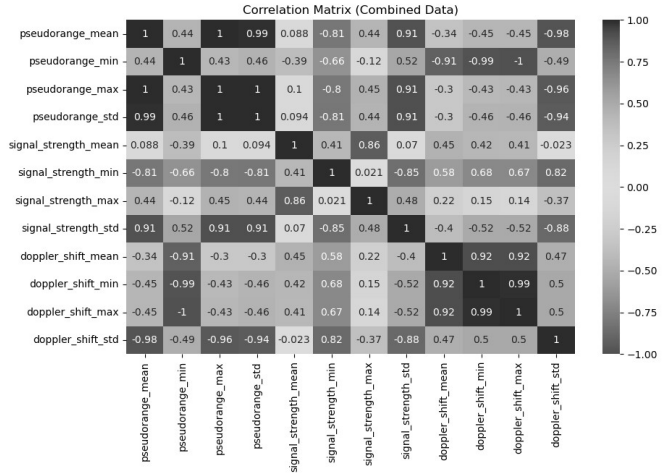


Figure 7. Combined data correlation matrices.

This heat map reflects pairwise correlations among the 12 statistical features of the three main GNSS parameters: pseudorange, signal_strength, and doppler_shift. For each parameter, the mean, minimum, maximum, and standard deviation (std) were considered. The data combines both clean and spoofed observations.

1. **Pseudorange**. All pseudorange-related features (especially mean, max, std) show extremely high positive intercorrelations (0.91–1.00). This indicates a very strong internal dependency, which is expected: as the mean value increases, the range and maximum also increase. In contrast,

pseudorange_min exhibits weaker correlations with the other pseudorange features. This may be linked to spoofers being limited in creating lower pseudorange values.

2. **Signal Strength**. signal_strength_min strongly negatively correlates with pseudorange values (to about −0.81, −0.66) and their standard deviation. This makes sense physically: greater distance corresponds to weaker signal strength. signal_strength_max and mean show moderate positive correlations with pseudorange_std but weaker or almost no correlation with pseudorange_mean. A high correlation between signal_strength_max and signal_strength_std (0.86) suggests that amplitude changes (peaks in signal strength) are sensitive to extremes in the signal, potentially serving as a spoofing marker.

3. **Doppler Shift**. doppler_shift_mean, min, and max are strongly interrelated (correlation > 0.92), indicative of smooth signal shifts without abrupt changes. They negatively correlate with pseudorange measures (up to −1.0 with pseudorange_min and pseudorange_max), which may be an indirect indication of a spoofer's attempt to simulate a stable relationship. doppler_shift_std shows a strong negative correlation with pseudorange_std (−0.94) and a positive correlation with doppler_shift_max/min (~0.5), suggesting a significant sensitivity of Doppler shift to signal dynamics.

4. **Role of the `std` Features**. The standard deviation blocks for all three parameters turn out to be especially informative for detecting anomalies, especially pseudorange_std, which correlates with many other metrics.

5. **Strong Negative Correlations**. The most pronounced negative correlations are between pseudorange and signal_strength/doppler_shift, which aligns well with GNSS physics.

6. **High Within-Block Correlation**. Each parameter's features (mean, min, max, std) show high internal correlation, implying that some metrics may be redundant and could potentially be reduced in the model.

Advantages of the Proposed Approach

1. Processing Speed. The model is capable of operating in real time. Thanks to a limited number of parameters and an optimized architecture, the processing time per signal is minimal. This is especially important for drones, which require immediate decisions to mitigate threats.

2. High Accuracy. The obtained metrics indicate that the model effectively recognizes synchronized spoofing signals even in the presence of noise in the data. This makes it suitable for real-world applications.

3. Flexibility. Our model can be adapted for other GNSS systems, such as Galileo or GLONASS. Additionally, it can be employed not only for drones but also for other navigation devices.

4. Ease of Integration. The multilayer perceptron architecture is straightforward to implement in existing onboard systems.

Limitations

1. Dataset Size. Although TEXBAT is a real and high-quality source of data, it covers a limited number of scenarios. To further improve the model, a larger volume of data is needed, including more real-world attacks and signal variations.

Potential Improvements

1. Expanding the Feature Set. We plan to add new parameters, such as signal time delay and multipath effects, which can also be indicative of spoofing.

2. Use of Ensemble Methods. Incorporating other machine learning models, such as Random Forest or Gradient Boosting, may improve the system's accuracy and robustness.

3. Development of Optimized Hybrid Neural Network Systems. Investigations could include methods based on Unsupervised Wavelet Adversarial-Refinement GAN and CNN+SOP (Self-Organizing Polynomial Network) architectures to further enhance spoofing detection performance.

IV. CONCLUSIONS

This paper addresses the task of GPS spoofing detection, focusing on synchronous attack scenarios (DS3 and DS7) using the open-source TEXBAT dataset. The main emphasis is on applying a multilayer perceptron (MLP) and performing a detailed statistical analysis of the signals. The results of the computational experiment can be summarized as follows:

1. Correlation Matrices. Matrices were constructed for three datasets: "clean" signals and spoofed signals under the DS3 and DS7 scenarios. These matrices allow us to monitor how key GPS signal parameters—namely pseudorange, signal_strength, and doppler_shift—are interrelated. To deepen the analysis, these parameters are considered not only as instantaneous values but also through statistical measures (mean, min, max, std).

- In "clean" data, the correlation patterns reflect the physical nature of the signals. Pseudorange and power typically exhibit a strong negative correlation (e.g., -0.93). The farther the satellite, the weaker the signal. Pseudorange and Doppler shift are often less correlated because Doppler shift arises from satellite and/or receiver movement, which does not always directly depend on instantaneous distance. Power and Doppler shift correlate primarily when the drone's speed or trajectory changes relative to the satellite; however, this correlation is seldom as strong as that of the pseudorange–signal_strength pair.

- Under spoofing (specifically in DS3 and DS7), the attacker attempts to artificially "idealize" or simulate these parameters. However, completely preserving the natural relationships is difficult. In DS3, pronounced fluctuations or "chaotic" behavior significantly weaken the negative correlation between pseudorange and power (from -0.93 to -0.68). In DS7, the correlation shifts are less abrupt since the attack is more carefully synchronized; nonetheless, the statistics still deviate from the "typical" values, revealing the signals to be spoofed.

- The practical value of such an analysis lies in the fact that correlation matrices can be computed in real time for data "windows." If the system detects significant deviations from the correlations typical of a legitimate signal, it raises a "red flag" indicating a potential attack. Since drones use GPS continuously, constant monitoring of correlation relationships helps quickly detect spoofing and trigger countermeasures (e.g., switching to alternative navigation systems or immediately alerting the operator).

2. Mean Value Distributions.

Significant shifts were observed in the mean values of pseudorange and signal strength. In the "clean" signal, two distinct "peaks" are typical, whereas in spoofed scenarios, the data more frequently cluster into a single or shifted region. This confirms the presence of distortions deliberately introduced by an attacker.

3. Model Accuracy. The proposed MLP architecture,

which includes three hidden layers, achieved a detection accuracy of 93%. This demonstrates the promise of using machine learning for the rapid recognition of spoofing.

In summary, this work gathers and systematizes real GPS data, develops an MLP model, and provides a detailed analysis of the resulting correlation matrices and distributions. The results confirm that even carefully orchestrated spoofing attacks alter the signal's characteristics, and machine learning can reliably distinguish genuine data from counterfeit. This finding opens the possibility of applying the developed approach in real-world conditions to enhance UAV security.

V. ACKNOWLEDGEMENTS

The research was carried out with the grant support of the National Research Fund of Ukraine "Methods and means of active and passive recognition of mines based on deep neural networks", project registration number 273/0024 from 1/08/2024 (2023.04/0024). Also, we would like to thank the reviewers for their precise and concise recommendations that improved the presentation of the results obtained.

References

[1] M. Mozaffari, W. Saad, M. Bennis, M. Debbah, "Unmanned aerial vehicle with underlaid device-to-device communications: Performance and tradeoffs," *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 3949-3963, 2016. https://doi.org/10.1109/TWC.2016.2531652.

[2] E. Shafiee, M. R. Mosavi, M. Moazedi, "Detection of spoofing attack using machine learning based on multi-layer neural network in single-frequency GPS receivers," *Journal of Navigation*, vol. 71, no. 1, pp. 169-188, 2018. https://doi.org/10.1017/S0373463317000558.

[3] A. R. Baziar, M. Moazedi, M. R. Mosavi, "Analysis of single frequency GPS receiver under delay and combining spoofing algorithm," *Wireless Personal Communications*, vol. 83, no. 3, pp. 1955-1970, 2015. https://doi.org/10.1007/s11277-015-2497-9.

[4] M. S. Almas, L. Vanfretti, R. S. Singh, G. M. Jonsdottir, "Vulnerability of synchrophasor-based WAMPAC applications' to time synchronization spoofing," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4601-4612, 2018. https://doi.org/10.1109/TSG.2017.2665461.

[5] S. Siamak, M. Dehghani, M. Mohammadi, "Counteracting GPS spoofing attack on PMUs by dynamic state estimation," *Proceedings of the 2019 Smart Grid Conference (SGC)*, 2019, pp. 1-5. https://doi.org/10.1109/SGC49328.2019.9056583.

[6] S. Khan, M. Mohsin, W. Iqbal, "On GPS spoofing of aerial platforms: A review of threats, challenges, methodologies, and future research directions," *PeerJ Computer Science*, vol. 7, e507, 2021. https://doi.org/10.7717/peerj-cs.507.

[7] A. M. Arthur, "Detecting signal spoofing and jamming attacks in UAV networks using a lightweight IDS," *Proceedings of the 2019 International Conference on Computer, Information and Telecommunication Systems (CITS)*, pp. 1-5, 2019. https://doi.org/10.1109/CITS.2019.8862148.

[8] R. Morales-Ferre, P. Richter, E. Falletti, A. de la Fuente, E. S. Lohan, "A survey on coping with intentional interference in satellite navigation for manned and unmanned aircraft," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 249-291, 2020. https://doi.org/10.1109/COMST.2019.2949178.

[9] R. Magar and A. Barati Farimani, "Learning from mistakes: Sampling strategies to efficiently train machine learning models for material property prediction," *Computational Materials Science*, vol. 224, p. 112167, 2023. https://doi.org/10.1016/j.commatsci.2023.112167.

[10] S. Silvey and J. Liu, "Sample size requirements for popular classification algorithms in tabular clinical data: Empirical study," *Journal of Medical Internet Research*, vol. 26, p. e60231, 2024. https://doi.org/10.2196/60231.

[11] W. Huan et al., "Haar wavelet-based classification method for visual information processing systems," *Applied Sciences*, vol. 13, no. 9, p. 5515, 2023. https://doi.org/10.3390/app13095515.

[12] S. Semanjski, I. Semanjski, W. De Wilde, A. Muls, "Cyber-threats analytics for detection of GNSS spoofing," Proceedings of the Seventh International Conference on Data Analytics DATA ANALYTICS 2018, IARIA 2018, pp. 136-140. https://personales.upv.es/thinkmind/dl/conferences/dataanalytics/data_analytics_2018/data_analytics_2018_9_20_68009.pdf.

[13] O. Jullian, B. Otero, M. Stojilović, J. J. Costa, J. Verdú, M. A. Pajuelo, "Deep learning detection of GPS spoofing," *LOD 2021. Lecture Notes in Computer Science*, vol 13163, 2022. Springer, Cham. https://doi.org/10.1007/978-3-030-95467-3_38.

[14] K. H. Park, E. Park, H. K. Kim, "Unsupervised intrusion detection system for unmanned aerial vehicle with less labeling effort," in: You, I. (eds) *Information Security Applications, WISA 2020, Lecture Notes in Computer Science*, vol 12583, 2020. Springer, Cham. https://doi.org/10.1007/978-3-030-65299-9_4.

[15] R. Peleshchak, V. Lytvyn, O. Mediakov, I. Peleshchak, "Morphology of Convolutional Neural Network with Diagonalized Pooling," In: Simian, D., Stoica, L.F. (eds) *Modelling and Development of Intelligent Systems. MDIS 2022. Communications in Computer and Information Science*, vol 1761, 2023. Springer, Cham. https://doi.org/10.1007/978-3-031-27034-5_11.

[16] S. Bao, S. Tang, P. Sun, T. Wang, "LSTM-based energy management algorithm for a vehicle power-split hybrid powertrain," *Energy*, vol. 284, 129267, 2023. https://doi.org/10.1016/j.energy.2023.129267.

[17] H. Huang, C. Qian, "Modeling PM2.5 forecast using a self-weighted ensemble GRU network: Method optimization and evaluation," *Ecological Indicators*, vol. 156, 111138, 2023. https://doi.org/10.1016/j.ecolind.2023.111138.

[18] J. Nunez, V. Tran, A. Katangur, "Protecting the unmanned aerial vehicle from cyberattacks," *Proceedings of the Steering Committee of the World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp)*, Athens, 2019. https://www.proquest.com/openview/444cac98c1c13da04b8d796e175ed3b6/1?cbl=1976342&pq-origsite=gscholar.

[19] R. Rukaiya, S. Ahmed Khan, M. U. Farooq, I. Matloob, "Communication architecture and operations for SDR-enabled UAVs network in disaster-stressed areas," *Ad Hoc Networks*, vol. 160, 103506, 2024. https://doi.org/10.1016/j.adhoc.2024.103506.

[20] M. Nayfeh, Y. Li, K. A. Shamaileh, V. Devabhaktuni, N. Kaabouch, "Machine learning modeling of GPS features with applications to UAV location spoofing detection and classification," *Computers & Security*, vol. 126, 103085, 2023. https://doi.org/10.1016/j.cose.2022.103085.

[21] W. Chen, Y. Dong, Z. Duan, "Accurately redirecting a malicious drone," *Proceedings of the 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*, 2022, pp. 827-834. https://doi.org/10.1109/CCNC49033.2022.9700664.

[22] J. Li, W. Li, Q. Fu, B. Liu, "Research progress of GNSS spoofing and spoofing detection technology," *Proceedings of the 2019 IEEE 19th International Conference on Communication Technology (ICCT)*, 2019, pp. 1360-1369. https://doi.org/10.1109/ICCT46805.2019.8947107.

[23] L. Lemieszewski, "Transport safety: GNSS spoofing detection using the single-antenna receiver and the speedometer of a vehicle," *Procedia Computer Science*, vol. 207, pp. 3181-3188, 2022. https://doi.org/10.1016/j.procs.2022.09.375.

[24] M. S. Kumar, G. S. Kasbekar, A. Maity, "Identification of GPS spoofing as a drone cyber-vulnerability and evaluation of efficacy of asynchronous GPS spoofing," IFAC-PapersOnLine, vol. 55, issue 22, pp. 394-399, 2022. https://doi.org/10.1016/j.ifacol.2023.03.066.

[25] Y. Zhi, Z. Fu, X. Sun, J. Yu, "Security and privacy issues of UAV: A survey," *Mobile Networks and Applications*, vol. 25, pp. 95-101, 2020. https://doi.org/10.1007/s11036-018-1193-x.

[26] Z. Yanyan, G. Shcherbakova, B. Rusyn, A. Sachenko, N. Volkova, I. Kliushnikov, S. Antoshchuk, "Wavelet transform cluster analysis of UAV images for sustainable development of smart regions due to inspecting transport infrastructure," *Sustainability*, vol. 17, issue 3, 927, 2025. https://doi.org/10.3390/su17030927.

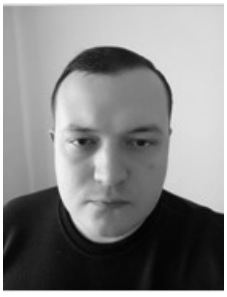
[27] T. E. Humphreys, J. A. Bhatti, D. Shepard, K. Wesson, "The Texas spoofing test battery: Toward a standard for evaluating GPS signal authentication techniques," *Proceedings of the Radionavigation Laboratory Conference*, 2012, pp. 1-15. https://core.ac.uk/reader/211343150.

[28] A. Joplin, E. G. Lightsey, T. E. Humphreys, "Development and testing of a miniaturized, dual-frequency GPS receiver for space applications," in Institute of Navigation International Technical Meeting, Newport Beach, CA, 2012. [Online]. Available at:. https://radionavlab.ae.utexas.edu/images/stories/files/papers/joplin_itm_2012.pdf.

[29] V. Lytvyn, I. Peleshchak, R. Peleshchak, I. Shakleina, N. Mozol, D. Svyshch, "Object image recognition using multilayer perceptron combined with singular value decomposition," *Proceedings of the Modern Machine Learning Technologies Workshop (MoMLeT 2024)*,

Lviv, Ukraine, 2024, pp. 225-234. https://ceur-ws.org/Vol-3711/paper13.pdf.
[30] B. Rusyn, O. Lutsyk, R. Kosarevych, O. Kapshii, O. Karpin, T. Maksymyuk, "Rethinking deep CNN training: A novel approach for quality-aware dataset optimization," *IEEE Access*, vol. 12, pp. 137427-137438, 2024. https://doi.org/10.1109/ACCESS.2024.341465.
[31] D. Naso, O. Pohudina, A. Pohudin, S. Yashin, & R. Bartolo, "Autonomous flight insurance method of unmanned aerial vehicles Parot Mambo using semantic segmentation data," *Radioelectronic and Computer Systems*, no. 1, pp. 147-154, 2023. https://doi.org/10.32620/reks.2023.1.12
[32] H. Fesenko, O. Illiashenko, V. Kharchenko, I. Kliushnikov, O. Morozova, A. Sachenko, S. Skorobohatko, "Flying sensor and edge network-based advanced air mobility systems: Reliability analysis and applications for urban monitoring," *Drones*, vol. 7, 409, 2023. https://doi.org/10.3390/drones7070409.

VASYL LYTVYN, *Doctor of Technical Sciences, a Professor at Department of Information Systems and Networks, Lviv Polytechnic National University.* ***Research Interests: Intelligent Systems, Machine Learning, Knowledge Engineering, Ontology Construction, Decision Support Systems.***
E-mail: vasyl.v.lytvyn@lpnu.ua
ORCID: https://orcid.org/0000-0002-9676-0180



IVAN PELESHCHAK, *PhD 124 System analysis, Department of Information Systems and Networks, Lviv Polytechnic National University. Research Interests: Intelligent Systems, Artificial Intelligence, Deep Learning, Hybrid Neural Networks, Pattern Recognition.*
E-mail: ivan.r.peleshchak@lpnu.ua
ORCID: https://orcid.org/0000-0002-7481-8628

YAROSLAV STEPANIAK, *Bachelor 124 System Analysis, Department of Information Systems and Networks, Lviv Polytechnic National University. Research Interests: Intelligent Systems, Artificial Intelligence, Computational Intelligence, Embedded AI Systems.*
E-mail: yaroslav.stepaniak.mnsam.2023@lpnu.ua
ORCID: https://orcid.org/0009-0007-3074-1132

ROMAN PELESHCHAK, *Doctor of Physical and Mathematical Sciences, Professor, Department of Information Systems and Networks, Lviv Polytechnic National University. Research Interests: Intelligent Systems, Artificial Intelligence, Magnetic Field Sensing, Landmine Detection.*
E-mail: roman.m.peleshchak@lpnu.ua
ORCID: https://orcid.org/0000-0002-0536-3252

OLEKSII ISHCHUK, *Postgraduate medical intern at The Specialist Hospital in Sanok Autonomous Public Healthcare Centre. Research Interests: Advanced Computer Technologies, Artificial Intelligence, Predictive Analytics in Healthcare.*
E-mail: forward1q@gmail.com
ORCID: https://orcid.org/0009-0001-2472-2759