TRANSNAV
http://www.transnav.eu
the International Journal
on Marine Navigation
and Safety of Sea Transportation
Volume 19
Number 2
June 2025
DOI: 10.12716/1001.19.02.31

The Use of Artificial Intelligence in Enhancing Navigation Safety in Case of GNSS Signal Fading or Interference

M. Chrzan
Kazimierz Pulaski University in Radom, Radom, Poland

ABSTRACT: Global Navigation Satellite Systems (GNSS) play a key role in modern navigation and transportation service delivery. Today it is difficult to imagine the daily operation of land, sea or air transportation without the positioning and timing provided by satellite systems [6, 8, 11]. In civil aviation, GNSS provides precision landing approaches and support for safety systems, in maritime navigation it enables open sea course determination and maneuvering, and on land it directs vehicle navigation and synchronization of telecommunications networks. Many of these applications are so-called PNT (Positioning, Navigation and Timing) systems, where uninterrupted and accurate position and timing information is critical to safe operations [8]. Unfortunately, satellite systems have recently become the target of hacking attacks. This paper will present AI methods for detecting GNSS anomalies, the role of inertial systems as an independent navigation source, and position correction techniques (e.g., using Kalman filters) supported by intelligent algorithms. An overview of current research and experiments in this field will also be presented, as well as conclusions on the effectiveness and development prospects of the technologies discussed.

1 INTRODUCTION

Paradoxically, the ubiquity of and trust in GNSS makes these systems vulnerable to interference. Signals transmitted by satellites reach Earth with a power of the order of picowatts - making them easily drowned out by stronger radio emissions [4]. In addition, open civilian GNSS signals (GPS, Galileo, GLONASS, BeiDou) are not encrypted or authenticated, which means there are no built-in safeguards against imitation. This raises two main threats: jamming and spoofing. Jamming involves intentionally generating radio interference on GNSS frequencies so that the receiver is unable to receive the true signal from the satellites [10]. The result of such an action is the loss or severe degradation of satellite navigation performance - the receiver may report a missing signal or determine a position with very low accuracy. Spoofing, on the other hand, is a more sophisticated attack in which an attacker broadcasts falsified signals that mimic real GNSS messages so that the receiver assumes them to be authentic [10]. In this way, erroneous location or time information can be fed to the receiver, potentially directing the "victim" to the wrong location or misinforming time-dependent systems (such as power grids or financial networks). Interference with GNSS signals is not just a theoretical threat, but a real problem noted with increasing frequency around the world. Reports from the maritime and aviation services indicate an increasing number of jamming and spoofing incidents, especially in geopolitically unstable regions [10]. For example, numerous GPS signal disruptions have been reported in recent years for ships in the Eastern Mediterranean, the Black Sea or the Persian Gulf. Civil aviation has also seen an alarming increase in spoofing attacks, with pilots reporting instances where onboard systems gave incorrect coordinates or altitude, posing an obvious risk to flight safety. Spoofing applied to an aircraft can result in erroneous navigation, and in extreme cases - if the crew does not figure it out in time - even lead to a violation of airspace or an attempted landing on a false path. In military applications, the consequences are equally serious: a spoofed signal can result in military units losing orientation or taking control of the unmanned aircraft, which is a significant breach of operational security [8, 10].

The reason for the vulnerability of GNSS systems to attacks is the lack of mechanisms to verify the reliability of the signal - most receivers trust the data received from satellites implicitly. Unlike, for example, computer networks, where there are firewalls and authentication systems or protocol verification procedures, a typical GNSS receiver has no way to distinguish a genuine signal from a crafted one until additional detection methods are put in place. The fact that full documentation of GNSS protocols is publicly available makes it easier for potential attackers to prepare hardware and software for an attack. What's more, advances in technology and engineering have made the "barrier to entry" for attackers significantly lower - nowadays, for a few hundred dollars, one can get a software-defined radio (SDR) capable of generating signals that interfere with or mimic GNSS [11]. While this used to require specialized knowledge and expensive equipment, today there are open-source tools and instructions available on the Internet. All of this demonstrates the importance of ensuring navigation safety despite GNSS interference.

Improving the resilience of navigation systems to GNSS interference has thus become a research and engineering priority in recent years. Multi-layered strategies are being introduced: from improving the receivers themselves (e.g., anti-jam antennas, signal authentication in new systems) to system approaches using redundant sources of position information and artificial intelligence algorithms to detect and compensate for anomalies. Particularly promising is the use of artificial intelligence (AI) - machine learning and deep learning techniques - to analyze navigation data to quickly catch unusual system behavior and sustain navigation in the event of satellite signal loss.

2 LITERATURE RESEARCH AND REVIEW

2.1 *Application of artificial intelligence in GNSS anomaly detection*

Effectively recognizing that a GNSS signal has been disturbed or falsified is the first step to ensuring navigation safety. Traditional GNSS receivers have limited mechanisms to warn of anomalies - Receiver Autonomous Integrity Monitoring (RAIM) systems, for example, can detect that a pseudo-distance measurement deviates from others, but against specialized spoofing attacks they are sometimes powerless. Therefore, more advanced detection methods are being developed, often using multi-sensor analysis and intelligent algorithms. In general, GNSS anomaly detection approaches can be divided into several categories: signal-based methods, bit/data-based methods, positional methods, and methods using machine learning [11].

Signal methods involve monitoring the parameters of the GNSS signal received by the antenna - such as signal power, signal-to-noise ratio (C/N0), or reception characteristics on multiple antennas. Jamming interference often manifests itself as a sharp drop in C/N0 across all channels and loss of satellite tracking, while spoofing can cause unnatural changes in power (e.g., a sudden increase in signal strength seemingly from all satellites simultaneously) or abnormal behavior of the receiver's synchronization block. Signal detection can use simple threshold tests or more complex signal processing algorithms - such as observing the signal spectrum in the GNSS band to identify additional unwanted signals.

Bitwise methods focus on the content of navigation data demodulated from the signal. The receiver can verify that the almanac/efemerid data or time marks are consistent and as expected. False signals may contain minor deviations in the data (e.g., invalid satellite identifier, repeated data string - characteristic of meaconing, i.e., retransmission of a real signal with a delay). Analysis of this data, supported, for example, by correlation techniques between multiple signals, makes it possible to detect certain types of attacks. For example, one method uses monitoring the cross-correlation of multiple GNSS observations (pseudo-distance, carrier phases, etc.) and looking for statistical outliers, which then serve as input features to a machine-learned detector [12]. In experiments, it has been shown that a trained classifier (e.g., SVM - Support Vector Machine) fed with such features can distinguish spoofing/meaconing situations from normal ones, effectively alerting to an attack. Importantly, this approach was verified on real incident data - the algorithm learned on simulation data also recognized recordings of real disturbances with high efficiency [12].

Positional methods are based on checking the consistency of the determined position with other information. For example, a vessel equipped with GNSS and radar or lidar can compare independent position measurements: if the GPS shows that the vessel has moved a few hundred meters, while the radar still sees the shore at a constant distance - that's a sign of a problem. Another approach is dynamic control: monitoring whether the calculated movement trajectory is physically possible (e.g., no sudden "jumps" in position that exceed the vehicle's achievable acceleration). In practice, many such symptoms are used: a loss-of-position alarm, sudden course deviations observed on an electronic map compared to the course from radar, jumps in speed or coordinate readings while the HDOP is low (which normally means good satellite geometry) - all of these warning signals can indicate GNSS interference [3]. Operators and systems can also cross-check position from different systems (e.g., GNSS vs. local systems like LORAN or cellular network position) to look for discrepancies.

Methods using artificial intelligence (AI) often combine elements of the above approaches, simultaneously analyzing multiple parameters and signals to detect subtle anomalies invisible to the naked eye. Machine learning, particularly deep learning (DL), has proven to be extremely effective in GNSS interference detection tasks in recent years [8, 11]. These algorithms can learn from large data sets characteristic patterns indicative of jamming or spoofing. For example, a neural network can simultaneously take into account temporal changes in signal power, pseudo-distance errors, trajectory deviations, and other characteristics, and on this basis classify the state of the system as normal or attacked. Various machine learning (ML) models have been compared in the literature for spoofing detection - results indicate that already relatively simple models, such as decision trees (CART), achieve very good performance in identifying attacks, outperforming classical methods based on rigid thresholds [11]. More advanced approaches use convolutional or recurrent Long Short-Term Memory (LSTM) networks to analyze raw streams of signals or strings of observations. The latest experiments using deep networks have already achieved nearly 99% success rate in detecting jamming attacks on available datasets, a few percent improvement over earlier algorithms. Such high results show that AI is capable of very accurately distinguishing between real and jamming signals based on even small deviations in patterns.

In practice, AI-based GNSS anomaly detection systems can operate in continuous receiver monitoring mode. For example, on board an aircraft, an intelligent module analyzes the data stream from a GPS receiver (position, speed, time, signal parameters) and compares it with data from an inertial navigation system or other sensors. If the AI detects discrepancies beyond normal conditions (e.g., much larger differences between the position from GPS and inertial than usual, or the simultaneous shift of all pseudo-distances characteristic of spoofing), it can alert the system to a suspected attack in a fraction of a second. This approach is much faster and more reliable than manual observation by an operator, especially since combined attacks (e.g., simultaneous jamming and spoofing) can manifest themselves in complex ways that are difficult to catch with traditional methods [11]. Artificial intelligence enables learning by example in this context - the system can be trained on a variety of attack scenarios, so it will know what the symptoms of a given threat look like.

It is worth noting that the effectiveness of AI methods strongly depends on the availability of adequate training data. The scientific community has several public GNSS attack datasets (e.g., TEXBAT and OAKBAT containing recordings of various spoofing scenarios) used for algorithm validation [11]. However, there is still a lack of open datasets covering a wider range of situations (different types of simultaneous interference, other environmental conditions, etc.), which is the subject of active work. Despite these challenges, current research results show that the application of AI significantly improves the ability of navigation systems to quickly detect and classify GNSS anomalies, thus providing a foundation for activating emergency mechanisms to protect traffic safety.

2.2 *Role of the inertial systems in navigation*

When a GNSS signal fades, the natural salvation is to resort to other sources of motion information. For decades, a standard component of professional navigation systems has been an inertial system (INS) - that is, a device that measures vehicle acceleration and angular velocity based on a set of motion sensors [6].

A typical INS consists of an inertial measurement unit (IMU) containing a three-axis accelerometer and a three-axis gyroscope, whose readings are processed in real time by a navigation computer. Operating completely independent of external signals, the INS performs so-called dead-reckoning navigation - from a known initial position, using measurements of acceleration and rotation, it calculates the new position, speed and orientation of the vehicle in real time through a process of integrating (integrating) these accelerations over time [2]. As a result, INS provides continuous navigation information even in the complete absence of external signals (GPS, radio beacons, etc.), making it invaluable in conditions of interference or where satellite systems do not reach (e.g. underwater, in tunnels) [6].

Inertial systems come in different classes of accuracy. High-end INS, used, for example, in commercial aviation or submarines, are based on laser or fiber-optic gyroscopes and have very low drift - their position error builds up slowly, on the order of a meter every few minutes or an hour. Low-cost INS based on MEMS technologies (micro-mechanical sensors used, for example, in smartphones or drones) unfortunately have much worse stability - errors in acceleration measurements mean that after just a few tens of seconds without correction, the position can have an error of several meters, and after a few minutes even hundreds of meters. In general, a fundamental limitation of any INS is that its accuracy decreases over time due to the accumulation of measurement errors during integration [2]. Even the most accurate inertial systems suffer from a certain level of bias (drift) of accelerometers and gyroscopes, which, if not periodically corrected, leads to an increasing deviation of the calculated position from the actual position. In the literature, this phenomenon is referred to as unbounded growth of error - without external correction, the INS will sooner or later "lose its way" to the point where its indications become navigationally useless [2].

Despite this disadvantage, autonomy and immunity to external interference make INS serve as a key backup navigation source. For example, in modern passenger aircraft, several inertial navigation platforms (IRS) are installed to determine the machine's movement parameters throughout the flight. When a GPS signal is available, the data from the INS is calibrated and corrected on an ongoing basis, but if it is lost, it is the INS that assumes the burden of maintaining knowledge of the flight's position and direction for the time needed, for example, to return safely to the airport [9]. Similarly, in maritime navigation - modern ships are equipped with AHRS/INS systems that can navigate without GPS for a period of time, relying solely on gyroscopes and speed logs. In autonomous vehicles, INS (sometimes in a reduced form, the so-called RISS - Reduced Inertial Sensor System, e.g., with the replacement of some of the sensors with a wheel odometer) assists in maintaining traffic awareness in dense urban areas where the GNSS signal is weak or fades among tall buildings [9].

However, practice shows that GNSS and INS are complementary - they have complementary properties [2]. GNSS provides absolute position reference with a current time-independent error (e.g., a few meters horizontally), but is susceptible to interference and fading. INS, on the other hand, is continuous and difficult to disturb, but its relative error increases over time. For this reason, the integrated use of GNSS and INS has become standard, so as to combine the advantages of both. In a typical navigation system, GNSS provides periodic accurate position and velocity corrections, resetting INS's growing error, while INS provides a bridge during periods when current GNSS data is unavailable [2]. This approach creates a navigation system that is both accurate in the long run (thanks to GNSS) and resilient to short-term reception problems (thanks to INS).

The disadvantage of integration based solely on occasional “resetting” of the INS with GPS data (the so-called loosely coupled system) is that when the GNSS signal interruption lasts too long or the number of available satellites falls below the minimum (e.g., less than 4, making it impossible to determine the position), the system switches to a standalone INS anyway and the error starts to grow rapidly [2]. This is why tightly integrated GNSS/INS systems are used in practice, where the two systems work together continuously - the INS continuously corrects itself even with partial GNSS data, and in return can help track satellite signals during difficult conditions (e.g., in tightly coupled systems, the INS can help sustain satellite tracking when the signal is on the verge of fading). Regardless of the detailed integration architecture, however, the role of the INS is crucial as a navigation safeguard: it is through it that the system is able to sustain position determination when GNSS signals are disrupted or lost. Sections 2.3 and 2.4 discuss how artificial intelligence can further enhance this integration, reducing INS errors and effectively extending the time for safe navigation without GNSS.

2.3 *Position correction mechanisms using AI and filtering*

For years, the Kalman filter has been the primary mathematical tool used to combine GNSS and INS data into coherent navigation information. A Kalman filter is a state estimation algorithm that, based on a motion model and a measurement model, can optimally estimate the current error and correction based on the available data, even if it is subject to noise [6]. In the context of GNSS/INS integrated navigation, the Kalman filter usually acts as an INS error estimator - it compares the position and velocity calculated by the INS with GNSS measurements and calculates corrections to the inertial solution based on this [1, 2]. In other words, when a GNSS signal is available, the filter continuously corrects INS drift, minimizing the differences between the two sources. At times when the GNSS signal dies, the filter enters predictive mode: it continues to estimate the state based only on the INS model, and its uncertainty gradually increases, but thanks to the earlier calibration of INS errors, it slows the accumulation of these errors compared to the stand-alone INS [15].

A key challenge is maintaining accuracy during longer GNSS signal gaps. The standard Kalman filter assumes a specific INS error model (e.g., gyro drift modeled as a first-order Gauss-Markov process, etc.) and uses limited information for prediction, so that at long gaps (tens of seconds or more) its predictions begin to diverge from reality. In recent years, however, ideas have emerged to support classical filtering with artificial intelligence methods that can learn more complex error and motion patterns than the simple linear model used in the Kalman filter. AI can be involved in several ways: to predict corrections during periods of GNSS absence, to adaptively tune filter parameters, or as a separate sensory fusion module parallel to the classical approach.

One interesting strategy is to predict GNSS observations from INS data using machine learning models. Such a mechanism has been proposed, among others, by Chen et al. (2022), where they used a hybrid method based on partial least squares regression (PLSR) and regression with Gaussian process (GPR) [5]. The model learns the relationship between INS errors and GNSS observations (when these are available) to predict, during satellite fading, what the GNSS data (e.g., pseudo-distance or position) would look like based on INS alone. These “synthetic” observations are then fed into the Kalman filter instead of real GNSS data, allowing it to continue to correct INS errors despite the absence of an actual satellite signal. In experiments with four GNSS fades during a test flight, it was shown that the use of such prediction significantly improved navigation accuracy compared to the usual mode without corrections - the Kalman filter “supported” by PLSR/GPR prediction maintained smaller trajectory deviations than the traditional one, proving the effectiveness of the approach. In other words, the intelligent module learned to predict certain GNSS receiver behavior based on traffic history and INS errors, thus filling in data gaps during disturbances.

Another line of research focuses on directly correcting INS readings using AI algorithms. An example is the use of adaptive neuro-fuzzy systems (ANFIS) to calibrate lower-cost inertial systems. In the work of Mahdi et al. (2024) presented a system in which a reduced RISS inertial system (using, among other things, an odometer and one gyroscope) was integrated with GNSS using ANFIS as an error correction learning block [9]. ANFIS, combining elements of neural network and fuzzy logic, was trained to predict INS-generated position errors based on vehicle movement patterns and previous differences between INS and GNSS. As a result, the INS so calibrated provides much more accurate information during interruptions in GPS reception. Tests using actual vehicle runs, during which GNSS signal fades lasting between 50 and 150 seconds were simulated, showed a reduction in 2D position error (RMSE) of about 43.8% relative to traditional RISS/GNSS integration without such calibration [9]. Maximum position deviations were also reduced by about 47%, meaning that the vehicle, even for two minutes without GNSS, stayed much closer to the actual trajectory than would have been possible with the classical system [9]. This is a big step forward, given that we're talking about a system made of low-cost MEMS sensors - thanks to AI, precision close to that which would be provided by much more expensive inertial systems was achieved.

Also, deep neural networks are finding applications in improving inertial navigation in the absence of GNSS. Long Short-Term Memory (LSTM) models, a variation of recurrent neural networks capable of learning temporal dependencies, have been used to predict vehicle movements and trajectories based on history from inertial sensors. Research indicates that LSTM networks can effectively stabilize INS drift error: in field tests, it was shown that the use of such a model can significantly improve positioning accuracy during GNSS fading (e.g., 30 or 90 seconds) compared to unassisted stand-alone INS. A network learned from data from periods when GNSS is operational can then predict on-the-fly corrections to the INS-calculated position when GNSS fades. In practice, this can look like this: an autonomous vehicle equipped with an LSTM network, when the GPS signal is lost, switches to a mode where each new position from the INS is corrected by a neural network predicting how much error is likely to have occurred. It's a bit like a virtual GPS acting on past experience. Such an approach, while sounding futuristic, is already yielding tangible results, and further development of the models (e.g., combining LSTM with convolutional networks that analyze camera data - which combines inertial and visual navigation) could further improve the reliability of GNSS-free navigation.

Artificial intelligence can also support position correction more indirectly - for example, through adaptive tuning of the Kalman filter. Filter parameters (covariances of model and measurement noise) are often fixed rigidly or according to simple adaptations, which do not always reflect the actual error dynamics. Methods of using learning algorithms to continuously adapt these parameters on the fly are being investigated, so that the Kalman filter can better respond to changes in conditions (e.g., rapid vehicle maneuvers that increase INS model error). For example, a neural network could learn from observed deviations between INS and GNSS to adjust the filter's Q and R covariance matrices, making it more resilient to unusual situations. Such approaches are at the research stage, but early results suggest that combining a physics-based model (Kalman filter) with a learning model yields better results than each alone. In other words, AI does not have to replace proven navigation algorithms - it can complement them, compensating for their limitations (e.g. nonlinearities, model uncertainty).

In summary, GNSS interference position correction mechanisms are increasingly using a hybrid approach: classical filters and models are combined with AI components that provide additional information or adaptivity. Experimental results prove that this makes it possible to significantly improve the accuracy and reliability of navigation during prolonged interruptions in satellite signal reception. As a result, the navigation system becomes more resilient - it can rely on itself for longer without external data, increasing overall safety.

2.4 *Overview of actual research, implementation and experiments*

The topic of enhancing the safety of navigation using AI under GNSS interference is being intensively researched around the world. A large number of experimental works, prototype implementations and simulation studies have appeared in the literature of the last decade, which confirm the usefulness of the methods described. The following is an overview of selected developments and initiatives in this area, divided into the issues of anomaly detection and maintaining navigation during signal fading.

GNSS interference detection: As early as around 2015-2020, work began to appear demonstrating the effectiveness of machine learning in spoofing detection. The authors in [12] presented a system that used supervised machine learning algorithms (including SVM) to detect false GNSS signals. A unique element was the use of real incident data - the authors used sets of meaconing and spoofing records from real tests, which made it possible to test the algorithm under near-real conditions. The results showed that the classifier learned from laboratory data recognizes attacks in field data with high efficiency, which is significant evidence of the practical usefulness of AI. Other research teams have also confirmed the effectiveness of the ML/DL approach: in 2021 and 2022, research results were published in which various models (from decision trees, to convolutional neural networks analyzing the signal, to hybrid methods based on ensemble learning) achieved efficiencies of 95-99% in detecting GNSS interference on shared datasets [8]. The ~99% accuracy result mentioned earlier was achieved on two different jamming and spoofing datasets, demonstrating the versatility of the approach used [8]. It is interesting to note that the best results were obtained by combining different techniques - the aforementioned work used both deep learning methods and elements of signal analysis and even vision techniques (e.g., a camera analyzing the environment for sources of interference). This indicates a trend that multi-sensor fusion involving AI can yield the most reliable sensing systems - for example, combining data from a GNSS receiver, inertial sensors, cameras and other sources into a single platform supervised by learning algorithms. Such solutions are currently being tested in aeronautical or maritime applications: next-generation prototype GNSS receivers can collect dozens of diagnostic parameters, which are then analyzed by an embedded AI module and signal the crew or autopilot in real time when a potential anomaly is detected. For example, research projects co-funded by European Union agencies are testing systems where the aircraft is equipped with a dual GNSS set (one primary, the other monitoring) and INS - data from both receivers and INS is compared by an intelligent algorithm that can detect even subtle attacks (e.g., those that slowly move position, hoping not to be noticed by standard alarms).

Importantly, the aviation and transportation industries recognize the seriousness of the problem. Organizations such as EASA (European Union Aviation Safety Agency) and IATA are sounding the alarm about the increasing number of GNSS jamming incidents and are launching initiatives to make systems more resilient. Post-conference recommendations point to the need to equip aircraft with improved GNSS jamming detection and warning mechanisms, as well as to maintain traditional navigation aids as back-ups (e.g., aviation VOR/DME beacons) [7].

As for maintaining navigation during GNSS fading, numerous experiments have been reported in this area as well, confirming the effectiveness of AI methods. Chen, L., et. all [5] conducted flight tests in which the aircraft experienced four targeted GNSS signal outages at different phases of flight. The navigation accuracy of the GNSS/INS system with a classical Kalman filter and the system assisted by the AI prediction module (PLSR/GPR) were compared. The results clearly showed that the AI-assisted version maintained the correct trajectory much better - the average position error during GNSS fading was significantly smaller than in the traditional system. What's more, the AI system showed greater stability under different maneuvers (the flight included both calm stretches and sharp turns); the classical filter gave a larger deviation at certain points, while the system with AI prediction still kept close to the true path. This is important evidence that intelligent methods improve not only static accuracy, but also robustness to different dynamic conditions.

In the field of land navigation, especially for autonomous vehicles, a number of tests have been conducted in urban conditions. For example, the authors [9], in their experiment, drove a vehicle along urban routes, where GNSS signals were deliberately turned off for set periods of time (from tens to over a hundred seconds). The car then relied only on its own sensors (IMU, odometer) - once with and once without ANFIS correction enabled. The comparison showed that without AI the vehicle "lost position" from the real one quite quickly (the error grew exponentially with time), while with ANFIS the trajectory reconstructed by the system remained close to the real one - the differences in distances of tens of meters were able to be reduced to a few tens of meters, which can be decisive for maintaining continuity in the lane or avoiding a collision at a critical moment [9]. It is worth mentioning that these tests took into account different scenarios: straight driving, sharp turns (where INS errors usually increase faster), and speed changes. In all cases, neuro-fusion integration improved the results, making it a promising technique for the automotive industry. Already, some so-called dead reckoning GPS systems in cars use simple forms of machine learning for self-calibration (e.g., learning the bias of a MEMS gyroscope when the car is at a traffic light). Future on-board navigation systems can be expected to incorporate even more advanced learning algorithms, especially in autonomous vehicles, where full redundancy (GNSS, INS, lidar, camera) is standard - AI will play the role of integrator of all these sources.

For ships, systems are being developed that integrate INS, GNSS and local sensors like logs and gyrocompasses, where AI manages how much weight to assign to each source at any given time. Under conditions of GNSS interference, the system can automatically switch to "INS + optical" mode, using, for example, cameras and lidar to track the shoreline (known as terrestrial navigation), and machine learning helps compare this information with the map. These are, however, solutions just crawling in research. Military projects are more advanced - armies have long used high accuracy INS, and are now testing AI to correct these INS without GNSS, such as by matching observed maneuver runs to known models. The details are often not public, but it is conceivable that military vehicle navigation systems will become a testbed for many of the techniques described (AI for spoofing detection, fusion with magnetometers, IR cameras, etc.).

Despite numerous successes, operational implementations of these technologies are just beginning. So far, most of the AI systems described have been demonstrated in test or prototype conditions. However, there are early swallows: for example, Honeywell has announced work on a GNSS receiver integrated with an AI module capable of self-learning the interference environment for general aviation. In automotive, manufacturers of GPS systems for the automotive class are beginning to add learning-based features (like the aforementioned INS self-calibration). Commercial software platforms are also emerging that allow the implementation of custom AI algorithms on GNSS receiver data (e.g., receivers with access to raw observations and the ability to upload user software) - this is important because it will allow the user community to create dedicated anti-spoofing solutions for their own needs.

In summary, research and experiments conducted over the past few years clearly confirm the effectiveness of using AI both in detecting GNSS threats and in maintaining navigation when they occur. Impressive results have been achieved in laboratory conditions (close to 100% attack detection, significant increase in safe navigation time without GNSS). In real-world conditions, the prototypes are also performing very well, although they are, of course, still subject to intensive testing in various scenarios. The next step is to translate these achievements into industrial standards and procedures, which is already beginning to happen with the cooperation of scientific institutions, manufacturers and regulators.

3 MATHEMATICAL MODEL OF GNSS/INS/AI SYSTEM

GNSS systems are crucial for precise navigation, but their signals are susceptible to interference (e.g., spoofing, jamming) and atmospheric disturbances. To increase the reliability of position estimation, additional inertial systems (INS) and adaptive filtering methods are used. Integration of these systems while monitoring anomalies in the GNSS signal enables dynamic error correction. This analysis presents mathematical modeling of the state estimation process, an adaptive anomaly detection algorithm and detailed simulation results.

3.1 *The extended state model*

Assume that the state of the system is described by a vector:

$$\boldsymbol{x_k} = \begin{bmatrix} p_k \\ v_k \\ b_k^a \\ b_k^g \end{bmatrix}$$

where:
p_k – position,
v_k – speed,

b_k^a– drift (bias) of the accelerometer,
b_k^g– gyro drift.

For a discrete dynamic system, the model can be written as:

$$\boldsymbol{x}_{\boldsymbol{k}+1} = \boldsymbol{F}_k \boldsymbol{x}_{\boldsymbol{k}} + B_{\boldsymbol{k}} u_k + w_k$$

whereby:
$\boldsymbol{F}_k$ – state transition matrix, taking into account the dynamics of movement and evolution of drifts,
$B_k u_k$ – Control model, where u_k to controlled acceleration (e.g., correction from INS),
$w_k \sim N(0,Q_k)$– process noise.

An example of the form of the $\boldsymbol{F}_k$ matrix (for a 1D model with Δt sampling) might look as follows:

$$\boldsymbol{F}_{\boldsymbol{k}} = \begin{bmatrix} 1 & \Delta t & -\frac{\Delta t^2}{2} & 0 \\ 0 & 1 & -\Delta t & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

where the negative members associated with drifts model the systematic effect of INS errors on the estimation [14].

3.2 *Measurement model*

The GNSS signal provides the position measurement directly. We write the measurement model as:

$$\boldsymbol{z}_{\boldsymbol{k}} = \boldsymbol{H} x_k + v_k$$

where:
H=[1 0 0 0]– observation matrix,
$v_k \sim N(0,R_k)$– measurement noise, whose covariance R_k may undergo adaptive modifications under anomalous conditionsi.

3.3 *Anomaly detection using an AI system*

3.3.1 *Innovation and statistical test*

The basis of anomaly detection in the Kalman filter is innovation vector analysis:

$$v_k = z_k - \boldsymbol{H}\hat{x}_{k|k-1}$$

where: $\hat{x}_{k|k-1}$ is the predicted state. For the standard Kalman filter, the innovation covariance matrix is:

$$S_k = \boldsymbol{H} P_{k|k-1} \boldsymbol{H}^T + \boldsymbol{R}_k$$

Anomaly detection test is based on statistics:

$$d_k^2 = v_k^T S_k^{-1} v_k$$

which under normal conditions has a chi-square distribution with mmm degrees of freedom (where m is the measurement dimension). Threshold γ is selected to take care of a certain level of significance of the test (e.g. α=0.05):

$$d_k^2 > \gamma \Rightarrow \text{anomaly detected}$$

If an anomaly is detected, the system can modify the matrix $\boldsymbol{R}_k$ or initiate a filter reset procedure.

3.3.2 *Adaptive AI-based mechanisms*

Machine learning algorithms (e.g., deep neural networks, SVMs) can be trained on historical data to classify signals as "normal" or "disturbed." In a hybrid approach, the result of the classification (denoted, for example, as $\delta_k \in \{0,1\}$) affects the filter parameters:
- if δ_k=1 (anomaly), element of the matrix increases $\boldsymbol{R}_k$, which reduces the weight of measurement GNSS,
- additionally, it is possible to use adaptive algorithms (e.g., drift recalibration) to minimize system errors.

The adaptation model can be formalized by:

$$\boldsymbol{R}_k^{adapt} = \boldsymbol{R}_k + \lambda \delta_k \boldsymbol{I}$$

where:
λ is an adaptive parameter,
$\boldsymbol{I}$ – unit matrix [10].

3.4 *Implementation and simulation*

The following simulation parameters were assumed:
- Sampling time: Δt=0.1 s,
- Number of steps: 1000 iterations (simulation lasting 100 s),
- Noise parameters:
  - The noise of the process: Q_k = diag(q_p, q_v, q_b^a, q_b^g) with typical values e.g.. $q_p=10^{-4}$, $q_v = 10^{-4}$, $q_b^a = 10^{-6}$, $q_b^g = 10^{-6}$
  - Measurement noise GNSS: $\boldsymbol{R}_k = \sigma^2_{GNSS} z \sigma_{GNSS} \approx 1$
- Interference conditions: Random interference was introduced in the simulation to simulate spoofing - in random iterations, a large deviation was added to the z_k.

3.5 *Estimation algorithm*

A classical Kalman filter was used for GNSS/INS data fusion. Stages of the filter:
1. Prediction:

$$\hat{\boldsymbol{x}}_{\boldsymbol{k}|\boldsymbol{k}-1} = F_k \hat{\boldsymbol{x}}_{\boldsymbol{k}-1|\boldsymbol{k}-1} + B_k u_{k-1}$$

$$P_{k|k-1} = F_k P_{k-1|k-1} F_k^T + Q_k$$

2. Update (with adaptation):

$$\boldsymbol{K}_k = \boldsymbol{P}_{k|k-1} \boldsymbol{H}^T \left(\boldsymbol{H} \boldsymbol{P}_{k|k-1} \boldsymbol{H}^T + \boldsymbol{R}_k^{adapt} \right)^{-1}$$

$$\hat{\boldsymbol{x}}_{\boldsymbol{k}|\boldsymbol{k}} = \hat{\boldsymbol{x}}_{\boldsymbol{k}|\boldsymbol{k}-1} + \boldsymbol{K}_k \left(z_k - \boldsymbol{H}\hat{x}_{k|k-1} \right)$$

$$\boldsymbol{P}_{k|k} = \left(\boldsymbol{I} - \boldsymbol{K}_k \boldsymbol{H} \right) \boldsymbol{P}_{k|k-1}$$

The anomaly detection module monitors d_k^2i and, if the threshold is exceeded, modifies R_k according to the adaptive model presented earlier.

3.6 *Simulation results*

Simulation conducted using the Monte Carlo method (500 runs) made it possible to determine the statistical properties of the estimation. The results are shown in Table 1:

Table 1. Simulation results

Scenario	Mean position error [m]	Standard deviation [m]
GNSS without correction	3.5	1.2
GNSS/INS + classical Kalman filter	1.2	0.5
GNSS/INS + Kalman filter with AI anomaly detection	0.7	0.3

In addition, analysis of the covariance matrix $\mathbf{P}_{k|k}$ showed a significant reduction in estimation uncertainty in the hybrid system. Graphical presentation of the estimated trajectory as a function of time showed that at moments of disturbance (detected by the AI module) there is immediate adaptation of the system, which minimizes the impact of anomalies on the estimation.

3.7 *Discussion and interpretation of results*

INS and GNSS data integration: Data fusion makes the system resilient to short-term GNSS signal interference - INS provides continuity of motion dynamics information.

Adaptive $\boldsymbol{R}_k$ matrix correction: The inclusion of an anomaly detection module allows the dynamic increase of measurement uncertainty when a disturbance is detected, resulting in less impact of erroneous data on the estimation.

Effectiveness of AI algorithms: Trained models detect abnormal patterns in the innovation vector, enabling the system to respond quickly. The use of a hybrid approach reduces the average position error by more than 40% compared to a classic filter.

4 CONCLUSIONS

The mathematical analysis and simulations conducted indicate that:

- GNSS/INS integration using an extended state model and an adaptive Kalman filter significantly improves navigation precision even under signal interference conditions.
- Adaptive anomaly detection mechanisms based on innovation vector analysis and complemented by artificial intelligence algorithms enable dynamic correction of filter parameters.
- Simulation results confirm that the hybrid approach reduces position error to levels on the order of 0.7 m, which is important for critical applications (e.g., autonomous systems, aviation, shipping, rail transportation).

The analyses and examples presented here clearly indicate that artificial intelligence has great potential for enhancing navigation safety under unreliable GNSS systems. AI methods, particularly machine and deep learning, have proven capable of detecting satellite interference with a speed and precision unattainable by traditional algorithms [8]. At the same time, intelligent data integration techniques allow the system to maintain correct navigation for much longer in the absence of a signal - thanks to AI, the system can adapt to changing conditions and quickly correct errors before they grow to dangerous proportions. In other words, AI makes the navigation system more aware: it can recognize on its own that "something is wrong" (e.g., that the data being used may be false or faulty) and react accordingly, whether by alerting the operator or switching to an alternative mode.

The effectiveness of existing AI solutions has been confirmed in numerous studies. In the context of GNSS anomaly detection, the attack classification accuracies achieved often exceed 95%, and in the best cases approach 99%. This means that these systems very rarely mistake normal conditions for an attack (low false alarm rate) and at the same time almost always capture the actual threat (high sensitivity). This is important because in safety-critical applications, while a false alarm is undesirable, failing to notice an actual attack is absolutely unacceptable. AI seems to be able to meet these requirements better than classical methods - by analyzing multiple sources and features at once, it is less likely to be fooled by interference masquerading as a normal signal. In the field of navigation maintenance (fusion of GNSS/INS and other sensors), on the other hand, AI has proven that it can drastically reduce positioning error during long gaps. Reductions of 30-50% in error achieved in automotive and aviation tests translate into real improvements in safety - for example, a ship will stay in a safe navigation corridor, an aircraft will stay closer to its intended path, and an autonomous vehicle will not lose its lane. All this brings us closer to the goal of resilient navigation (resilient PNT).

It should be noted, however, that despite promising results, large-scale implementation of this technology comes with challenges. First, AI methods must be properly validated and certified, especially in fields such as aviation, where safety requirements are very stringent. It is necessary to prove that the learning algorithm works reliably under all predicted conditions, and to understand its behavior in unforeseen situations. This is not always easy, because AI models (especially deep neural networks) are sometimes treated as "black boxes." That's why one of the directions of development is so-called XAI (Explainable AI) - methods to look inside the model and explain why it made such a decision and not another. In the context of navigation, this can increase trust in the system and facilitate certification. Second, current solutions often require large training data sets representing a variety of disturbance scenarios.

BIOBLIOGRAPHY

[1] Bonar B., Buratowski T.: Extended Kalman filter supported by logical conditions for inertial navigation. W: Systemy mechatroniczne : zagadnienia wybrane : praca zbiorowa / pod red. Michała Mańka. — Kraków : Katedra Robotyki i Mechatroniki. Akademia Górniczo-Hutnicza w Krakowie, 2022. — ISBN: 978-83-965598-2-1. — S. 51–59.

[2] Boguspayev, N., Akhmedov, D., Raskaliyev, A., Kim, A., Sukhenko, A. (2023): A Comprehensive Review of GNSS/INS Integration Techniques for Land and Air Vehicle Applications. Applied Sciences, 13(8), 4819. https://doi.org/10.3390/app13084819

[3] Britannia P&I Club - Global Marine P&I Insurance. https://britanniapandi.com/wp-content/uploads/2024/10/Navigational-Risks-at-Sea-Jamming-and-Spoofing.pdf [C: 16 October 2024]
[4] Clausnitzer, Ch., Alexander K,.(2024): GNSS Jamming/Spoofing and Continued Operational Safety International Committee on GNSS Interference Detection &Mitigation Workshop 15 April 2024
[5] Chen, L., Liu, Z., Fang, J.(2022): A novel hybrid observation prediction methodology for bridging GNSS outages in INS/GNSS systems. Journal of Navigation. 2022;75(5):1206-1225. doi:10.1017/S037346332200025X
[6] Chrzan, M., Jackowski, S. (2016): Współczesne systemy satelitarne w transporcie kolejowym. Politechnika Radomska im. Kazimierza Pułaskiego w Radomiu
[7] EASA partners with IATA to counter aviation safety threat from GNSS spoofing and jamming | EASA. (b. d.). EASA. https://www.easa.europa.eu/en/newsroom-and-events/press-releases/easa-partners-iata-counter-aviation-safety-threat-gnss-spoofing#:~:text="GNSS%20systems%20offer%20tremendous%20advantages,is%20a%20priority%20for%20the] – [C: 10.03.2025]
[8] Ghanbarzade, A., & Soleimani, H. (2025): GNSS/GPS Spoofing and Jamming Identification Using Machine Learning and Deep Learning. arXiv preprint arXiv:2501.02352.
[9] Mahdi AE, Azouz A, Noureldin A, Abosekeen A.(2024): A Novel Machine Learning-Based ANFIS Calibrated RISS/GNSS Integration for Improved Navigation in Urban Environments. Sensors (Basel). 2024 Mar 20;24(6):1985. doi: 10.3390/s24061985.
[10] Pardhasaradhi, B., Yakkati, R. R. Cenkeramaddi, L. R.(2022): Machine Learning-Based Screening and Measurement to Measurement Association for Navigation in GNSS Spoofing Environment in IEEE Sensors Journal, vol. 22, no. 23, pp. 23423-23435, 1 Dec.1, 2022, doi: 10.1109/JSEN.2022.3214349
[11] Radoš, K., Brkić, M., & Begušić, D. (2024): Recent Advances on Jamming and Spoofing Detection in GNSS. Sensors, 24(13), 4210. https://doi.org/10.3390/s24134210
[12] Semanjski, S., Semanjski, I., De Wilde, W., & Muls, A. (2020): 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. https://doi.org/10.3390/s20041171
[13] Simon, D., "Optimal State Estimation: Kalman, H Infinity, and Nonlinear Approaches", John Wiley & Sons 2006.
[14] Titterton, D. H. i Weston, J. L., (2004): Strapdown Inertial Navigation Technology, Radar , Sonar and Navigation Series 17. 2004.
[15] Zhang, Y., A (2019): Fusion Methodology to Bridge GPS Outages for INS/GPS Integrated Navigation System. IEEE Access. 2019;7:61296–61306. doi: 10.1109/ACCESS.2019.2911025