CHAPTER

Detection and mitigation of spoofing attacks in-based autonomous ground vehicle navigation systems

15

Sagar Dasgupta[1], Muhammad Sami Irfan[1], Mizanur Rahman[1] and Mashrur Chowdhury[2]

[1]Department of Civil, Construction and Environmental Engineering, The University of Alabama, Tuscaloosa, AL, United States [2]Clemson University, Clemson, SC, United States

15.1 Introduction

The evolution of ground transportation has brought us to the age of autonomous ground vehicles (AGV) which take over the task of control, guidance, and navigation from the human driver. In AGVs, these tasks are designated to individual modules that deal with perception, decision-making, control, and navigation. These modules rely on input from multiple onboard sensors, such as light detection and ranging (LiDAR), radio detection and ranging (radar), camera, inertial measurement unit (IMU), and ultrasonic sensor, in an AGV. The data from these sensors are necessary for determining both the relative and absolute positioning of an AGV within its environment. Relative positioning refers to determining an AGV's position in the local environment and nearby objects, while global positioning involves locating the vehicle on a global scale. Sensors, such as LiDAR, camera, and radar, are sufficient to perform relative positioning; however, global positioning requires the use of maps and global navigation satellite systems (GNSS)—a key technology in the development of ground vehicle navigation systems. Currently, over 100 million vehicles across the world rely on GNSS technology to perform navigation tasks [1]. GNSS also finds widespread applications across intelligent transportation systems in traffic management, vehicle safety systems, route planning and guidance, and freight tracking.

Despite the integral role of GNSS in navigation critical applications, its vulnerabilities are nontrivial and manifold, posing significant risks. Unintentional vulnerabilities in GNSS can arise from various sources: signal jamming due to physical obstructions like walls and ceilings in tunnels and garages, multipath distortions caused by high-rise urban buildings, atmospheric disturbances like scintillation and solar activities, and errors within the GNSS segment due to inaccurate data transmission or faults in satellite orbits. These threats, both dynamic and uncertain in nature, pose significant challenges to the reliability of GNSS services. Furthermore, intentional interferences (i.e., deliberate cyber threats), which include the generation of counterfeit GNSS signals that replicate authentic ones, or spoofing, lead to erroneous receiver data in terms of position, velocity, and timing. Jamming, which is the deliberate flooding of high-power radio signals near GNSS frequencies, can disrupt accurate positioning capabilities. Such targeted attacks are currently prevalent against aircraft systems and have been identified as a

Data Analytics for Intelligent Transportation Systems. DOI: https://doi.org/10.1016/B978-0-443-13878-2.00016-3
© 2025 Elsevier Inc. All rights are reserved, including those for text and data mining, AI training, and similar technologies.

significant threat to the industry [2]. Therefore the reliance of AGVs on GNSS systems for navigation makes them particularly vulnerable to attacks on GNSS.

This chapter is dedicated to the analysis of the vulnerability of ground transportation to GNSS spoofing events as well as the detection and mitigation of such attacks. In particular, we look at these aspects through the lens of data analytics, relating how data is involved in the entire chain, from developing spoofing attacks to defending against these attacks via detection and mitigation. In the rest of the chapter, we present an overview of GNSS-based positioning concepts and a discussion of the data involved in the attack generation, detection, and mitigation. Following this, we introduce the intentional and unintentional vulnerabilities of the GNSS-based navigation. Subsequently, the chapter delves into attack modeling, and detection strategies by leveraging statistical and artificial intelligence (AI) based data analytics. Following this discussion, mitigation techniques are explored, which integrate advanced technologies and practical strategies, and finally, the chapter concludes with a summary and future perspectives on enhancing GNSS-based navigation system security for AGV.

15.2 Global navigation satellite system-based positioning

15.2.1 What is global navigation satellite system?

GNSS refers to a satellite-based positioning and navigation system, encompassing satellite constellations that deliver geospatial positioning accessible worldwide. This technology enables users to determine their position (longitude, latitude, and altitude), velocity, and time. At present, four GNSS networks are fully functional: Global Positioning System (GPS) by the United States, GLObal NAvigation Satellite System (GLONASS) by Russia, BeiDou by China, and Galileo by the European Union [3]. All these systems operate on a fundamental concept where satellites in the medium altitude earth orbit send out signals that GNSS receivers capture to compute accurate locations. The most popular and extensively used GNSS system is GPS, which is run by the US Department of Defense. It is made up of a group of 31 satellites in the Earth's orbit. Russia's GLONASS is a second-generation dual-use GNSS system that was created during the Cold War. There are 24 operational GLONASS satellites in orbit and following three different orbital planes. The Galileo constellation, a collaborative endeavor by the European Space Agency and the European Commission, currently comprises 28 satellites in the Earth's orbit. China's GNSS system, known as BeiDou, gets its name from the Big Dipper constellation's Chinese moniker and is composed of 56 satellites, representing the largest GNSS constellation to date.

Each of the above GNSS shares similarities in their operational principle. GPS is presented here as an illustrative case. GPS has three primary segments: (1) space segment; (2) control segment; and (3) the user segment. The space segment represents the actual constellation of satellites that beam the GPS radio signals to users/receivers on the Earth. These satellites are at a 55° incline to the equatorial plane in a medium earth orbit. They are placed on six orbital planes at an altitude of 20,200 km above the Earth. With a period of 12 hours, each of these satellites circumnavigates the Earth two times a day. Within each satellite is a highly accurate rubidium or cesium atomic clock which is an essential component for supporting the Positioning, Navigation, and Timing (PNT) functionalities of the system. Control segment comprises of a network of ground stations that

routinely monitor the satellites within the space segment. Both the space segment and the control segments are developed, maintained, and operated by the United States Space Force. The control segment monitors the satellite positions and clock parameters and predicts them in the future. This information is then uploaded to the space segment through radio link and the space segment in turn retransmits it to the receivers. Finally, the user segment consists of individuals who use GPS receivers to receive signals. Receivers use reception antenna, processor, and stable quart clock for receiving and processing the GPS signal. Unlike the control segment, the receivers can only receive the signals from the space segment and utilize them for their applications, for example, autonomous vehicle navigation.

GPS signal consists of a carrier wave, a pseudorandom (PRN) code and the navigation message. The carrier wave is the radio frequency (RF) wave that carries the information to the receiver. The GPS satellites can transmit in at least two frequency bands, namely, the L1 band (1575.42 MHz), which has a bandwidth of 15.345 MHz and the L2 band (1227.6 MHz) with a bandwidth of 11 MHz. Signals on at least two frequencies are required to nullify the ionospheric effect on the position measurement. Newer satellites are also able to transmit in the L5 band which is at 1176.45 MHz and has a bandwidth of 12.5 MHz. Typically, due to the relative speed of the satellite and the GPS receiver, a Doppler shift occurs which can cause the received signal to deviate by $\pm$ 10 kHz. The carrier waves are in the form of pure sine waves and need to be modulated to carry the PRN code and navigation message information. To do this, GPS uses code division multiple access and phase shift keying modulation. The PRN code is a necessary piece of information that enables receivers to distinguish one satellite from others and lock on to the signal. The codes for each satellite are unique and the receiver uses it to find the correlation of its own locally generated signal with that of the received signal thereby enabling it to calculate the phase delay and the time the satellite transmitted the signal. There are two codes within the PRN code, one is the coarse acquisition (C/A) code having a shorter code length and is open for civilian usage. The other is the precise or P code which has a much longer length and has restricted usage, mainly limited to military applications. The navigation message component of the GPS consists of 25 frames of data, each having 5 subframes that carry the ephemeris, almanac information, time parameters and clock corrections, and satellite health information amongst other things. Each of these five subframes consists of 10 words. The size of each word is 30 bits; therefore a single message would require 37,500 bits. Hence at the data transmission rate of 50 bits/s, an entire message would take 750 s or 12.5 min.

15.2.2 Global navigation satellite system-based positioning concept

GNSS technology facilitates the following three fundamental measurement types for determining positions: pseudorange, carrier phase, and Doppler. Pseudorange, the most basic of these, calculates the distance between satellite and receiver by accounting for the time discrepancy between signal transmission and reception, adjusted by the speed of light. Carrier phase, another measurement type, assesses the signal's beat phase and cycle crossings relative to a nominal frequency, providing a higher precision of range alterations. Lastly, the Doppler measurement interprets frequency shifts due to relative motion to gauge the rate of distance change between satellite and receiver. In this chapter, we will only discuss the basics of pseudorange measurement.

For each satellite, the receiver calculates the distance traveled by the signal and hence the satellite's range by using the difference between the time the signal is transmitted from the satellite, t_s

and the time it is received at the receiver antenna, t_r. The value of range, r is achieved by multiplying the time difference by the speed of light, c, since GPS radio signals travel at the speed of light. As follows:

$$r = c(t_r - t_s) \tag{15.1}$$

A single measurement of the distance from a GPS receiver to a satellite indicates that the receiver is located somewhere on the surface of a sphere. This sphere is centered on the satellite and has a radius equal to the distance to the satellite. When a second measurement is taken to another satellite, the receiver similarly lies on the surface of another sphere, leading to two intersecting spheres that define a circle of possible receiver locations. The addition of a third range measurement introduces a third sphere, intersecting at two points. One point, being implausible in space, is disregarded, leaving the precise receiver location determined by these three intersecting spheres (see Fig. 15.1). Hence, at least three satellite signals are required to calculate the position of the receiver. The receiver's three-dimensional coordinates are deduced through an iterative process, refining the position solution by reconciling the calculated ranges with the satellite's known coordinates within an Earth-centered, Earth-fixed (ECEF) coordinate system. This iterative process, often involving linearization techniques, converges upon the receiver's precise location through successive approximations. The calculation of the receiver's position presumes that the clock of the receiver is synchronized with the satellite clock, the signal propagation is unaffected by atmospheric conditions, and the signal is free from any interference.

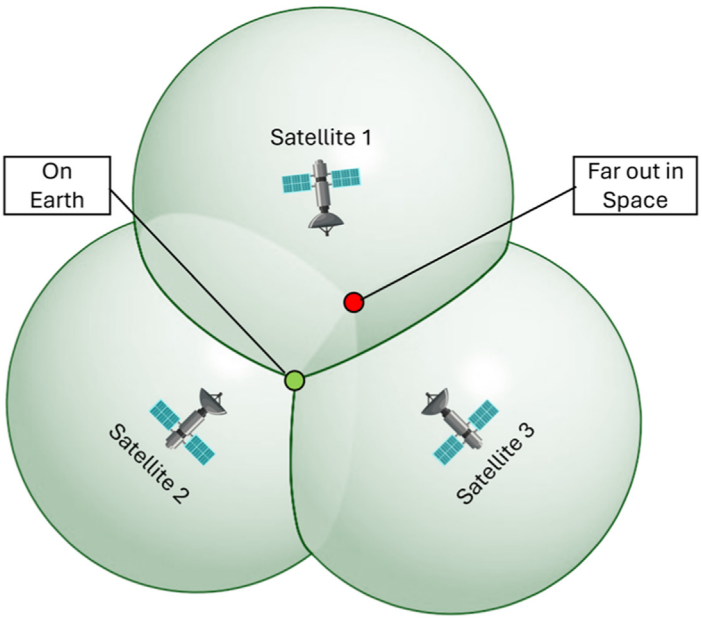

FIGURE 15.1

Receiver position determination using intersecting spheres.

However, in a real-world environment, the receiver clock is not synchronized with the satellite clock, which adds an error in the range calculation. Ground stations routinely monitor satellite clocks and relay corrective data for satellite clock biases and drift to receivers to adjust for these temporal discrepancies and enhance the accuracy of range estimations. However, receiver clock error is still unknown, resulting in four unknown variables: latitude, longitude, altitude, and the receiver clock bias. Therefore, signals from a minimum of four satellites are essential to accurately determine a receiver's location. The final computation of pseudorange corrects for delays caused by tropospheric and ionospheric conditions, as well as for distortions from multipath effects.

15.2.3 Navigation data and formats

GNSS data formats facilitate the transmission of GNSS data and products from satellites to receivers and ensure interoperability between providers of GNSS services and GNSS service users. Receiver formats are used to deliver GNSS observation and navigation information. On the other hand, metadata formats are utilized for information related to base station equipment and satellite

```
----|---1|0---|---2|0---|---3|0---|---4|0---|---5|0---|---6|0---|---7|0---|---8|

     3.02           N: GNSS NAV DATA    G: GPS              RINEX VERSION / TYPE
XXRINEXN V3         AIUB                19990903 152236 UTC PGM / RUN BY / DATE
EXAMPLE OF VERSION 3.02 FORMAT                              COMMENT
GPSA     .1676D-07    .2235D-07    .1192D-06    .1192D-06    IONOSPHERIC CORR
GPSB     .1208D+06    .1310D+06   -.1310D+06   -.1966D+06    IONOSPHERIC CORR
GPUT    .1331791282D-06  .107469589D-12 552960 1025          TIME SYSTEM CORR
    13                                                      LEAP SECONDS
                                                            END OF HEADER
G06 1999 09 02 17 51 44 -.839701388031D-03 -.165982783074D-10  .000000000000D+00
       .910000000000D+02  .934062500000D+02  .116040547840D-08  .162092304801D+00
       .484101474285D-05  .626740418375D-02  .652112066746D-05  .515365489006D+04
       .409904000000D+06 -.242143869400D-07  .329237003460D+00 -.596046447754D-07
       .111541663136D+01  .326593750000D+03  .206958726335D+01 -.638312302555D-08
       .307155651409D-09  .000000000000D+00  .102500000000D+04  .000000000000D+00
       .000000000000D+00  .000000000000D+00  .000000000000D+00  .910000000000D+02
       .406800000000D+06  .000000000000D+00
G13 1999 09 02 19 00 00  .490025617182D-03  .204636307899D-11  .000000000000D+00
       .133000000000D+03 -.963125000000D+02  .146970407622D-08  .292961152146D+01
      -.498816370964D-05  .200239347760D-02  .928156077862D-05  .515328476143D+04
       .414000000000D+06 -.279396772385D-07  .243031939942D+01 -.558793544769D-07
       .110192796930D+01  .271187500000D+03 -.232757915425D+01 -.619632953057D-08
      -.785747015231D-11  .000000000000D+00  .102500000000D+04  .000000000000D+00
       .000000000000D+00  .000000000000D+00  .000000000000D+00  .389000000000D+03
       .410400000000D+06  .000000000000D+00

----|---1|0---|---2|0---|---3|0---|---4|0---|---5|0---|---6|0---|---7|0---|---8|
```

FIGURE 15.2

A sample RINEX navigation file.

From https://files.igs.org/pub/data/format/rinex302.pdf.

Table 15.1 National Marine Electronics Association 0183 message structure.

ASCII	Hex	Dec	Use
<CR>	0x0d	13	Carriage return
<LF>	0x0a	10	Line feed, end delimiter
!	0x21	33	Start of encapsulation sentence delimiter
$	0x24	36	Start delimiter
*	0x2a	42	Checksum delimiter
,	0x2c	44	Field delimiter
\	0x5c	92	TAG block delimiter
^	0x5e	94	Code delimiter for HEX representation of ISO/IEC 8859−1 (ASCII) characters
~	0x7e	126	Reserved

calibration. Other data formats are used to transmit information on clock corrections, orbitals, etc. Some of the widely used nonproprietary data formats include Receiver INdependent EXchange (RINEX), BINary Exchange, and National Marine Electronics Association (NMEA) 0183. The RINEX format is not suited for real-time applications and contains only raw data, such as pseudoranges and no location information. RINEX formats comprise two files, which are the observation file and the navigation file. The observation file contains the phase, pseudorange, and receiver time information. On the other hand, the navigation file includes information related to satellite ephemeris, clock, position, and velocity. Fig. 15.2 is a sample RINEX navigation file.

As opposed to RINEX, the NMEA 0183 standard enables real-time data transmission at a bit rate of 4800/s. Therefore the NMEA standard is more suited for use in vehicle navigation tasks. In the standard message format, each message begins with a $ character after which a five-character talker ID is placed. Sentence within the NMEA standard can either be of type talker, query, or proprietary. The following table illustrates the message structure of a NMEA 0183 message (Table 15.1).

From a security point of view, these data formats present the information that is necessary to generate attacks or detect and mitigate them. For example, in the detection of an ongoing attack against an AGV, it will be necessary to work with navigation data in NMEA formats. In contrast, in the attack generation phase, an attacker may use prerecorded navigation information from a RINEX format file to launch an attack.

15.3 Vulnerabilities of global navigation satellite system-based navigation

GNSS have become integral to our modern world, supporting a wide range of applications from navigation and tracking to precise timing. However, the increasing reliance on GNSS technology has exposed vulnerabilities that threaten the security and reliability of these systems. As depicted in Fig. 15.3, GNSS vulnerabilities encompass a range of issues, spanning atmospheric effects, multipath errors, deliberate and unintended interference, and even segment errors, which can result in

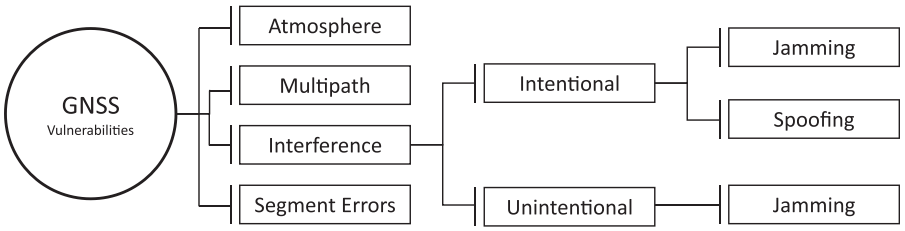

FIGURE 15.3

GNSS vulnerabilities.

inaccurate positioning and navigation errors, which could result in severe consequences in critical application areas, such as aviation, autonomous transportation, and telecommunications. In this context, understanding and addressing GNSS vulnerabilities have become crucial tasks to ensure the robustness and integrity of GNSS-based applications and services.

15.3.1 Atmosphere

The electromagnetic waves transmitted from GNSS satellites begin with their passage through the ionosphere before entering the neutral atmosphere, notably the troposphere. The propagation characteristics of these waves are profoundly influenced by the ionosphere and troposphere, each introducing delays and refractions that manifest as excess path delays [4]. The troposphere significantly influences GNSS signals, causing delays and phase advances due to its varying density, temperature, and humidity [5]. The primary tropospheric contributions are hydrostatic delays, predominantly associated with changes in air density, and wet delay that results from water vapor variability. To mitigate these effects, empirical models and mapping functions have been employed. Empirical troposphere models, such as the Saastamoinen model [6], provide zenith delays, and mapping functions transform these delays into slant delays at specific elevation angles. This enables the correction of tropospheric delays in postprocessing or real-time applications. Additionally, numerical weather prediction models, such as GPT2 [7] and VMF1 [8], offer improved accuracy by considering three-dimensional refractivity fields.

The ionosphere influences GNSS signals through its dispersive, absorptive, birefringent, and anisotropic properties [9]. As electromagnetic waves traverse the ionosphere, the refractivity index variations introduce frequency-dependent delays. The dispersive nature leads to frequency-dependent phase and group delays, causing signal dispersion. Absorption contributes to signal damping, affecting signal strength and quality. Birefringence results in two distinct values for the index of refraction, implying the possibility of dual-ray paths with different phase and group velocities. Anisotropy introduces orientation-dependent variations in the refractivity index. To mitigate these ionospheric effects, precise models and correction techniques are imperative. Differential techniques, exploiting dual-frequency measurements, enable the cancellation of first-order ionospheric errors [10]. Additionally, advanced algorithms, such as the group and phase ionosphere correction method [11,12] utilize the unique relationship between code and carrier phases to reduce ionospheric noise levels.

15.3.2 Multipath

Multipath is a phenomenon that arises when satellite signals encounter reflective surfaces on their way to the receiver antenna, causing the reception of both the direct and reflected signals (see Fig. 15.4). This leads to variations in the signal path lengths and introduces errors in the observed measurements. The effects of multipath include inaccuracies in pseudorange and carrier-phase measurements, resulting in position errors, lower precision, and degraded signal quality. Antenna design and placement play pivotal roles in mitigating multipath effects, with careful consideration given to reducing the number of reflective surfaces near the antenna. Additionally, receiver architecture choices influence the susceptibility to multipath, with modernized designs incorporating advanced tracking algorithms and filtering techniques to mitigate multipath-induced errors [13]. Real-time mitigation strategies often involve

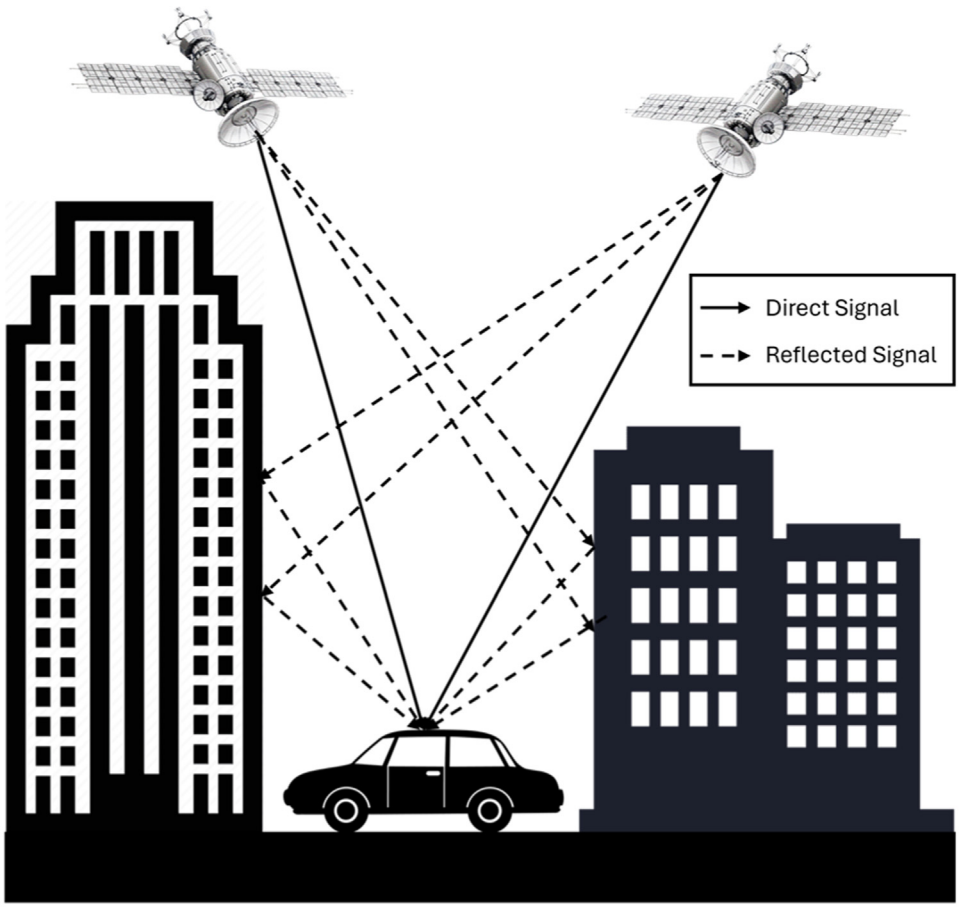

FIGURE 15.4

Multipath.

elevation-angle-dependent weighting in least-squares solutions or Kalman filter (KF) [14]. These techniques capitalize on the principle that multipath contamination is generally inversely proportional to satellite elevation angles. Moreover, for dynamic receivers operating in real time, monitoring the presence of multipath is crucial. Metrics derived from comparing raw pseudorange measurements with carrier-smoothed pseudorange outputs provide a real-time indication of multipath impact, allowing for adaptive deweighting of affected measurements.

15.3.3 Interference

GNSS interference refers to the intentional or unintentional disruption of GNSS signals that can lead to inaccurate positioning, navigation errors, and potential safety hazards. This interference can originate from a variety of sources, including jamming devices, unintentional RF emissions, and natural phenomena. Spoofing, an intentional attack, entails the generation of counterfeit GNSS signals to deceive the target receiver (see Fig. 15.5). Adversaries meticulously replicate authentic satellite signals, transmitting them with enhanced power to mislead the victim receiver. This manipulation unfolds in distinct phases, commencing with the acquisition of the target's attention, followed by continuous transmission to ensure signal tracking, and culminating in the injection of false location or timing information into the compromised receiver. Robust mitigation strategies against spoofing encompass advanced receiver authentication through cryptographic protocols, sophisticated signal processing techniques to detect anomalies, and the deployment of antenna arrays with spatial processing capabilities for the identification and rejection of spoofed signals [15–20].

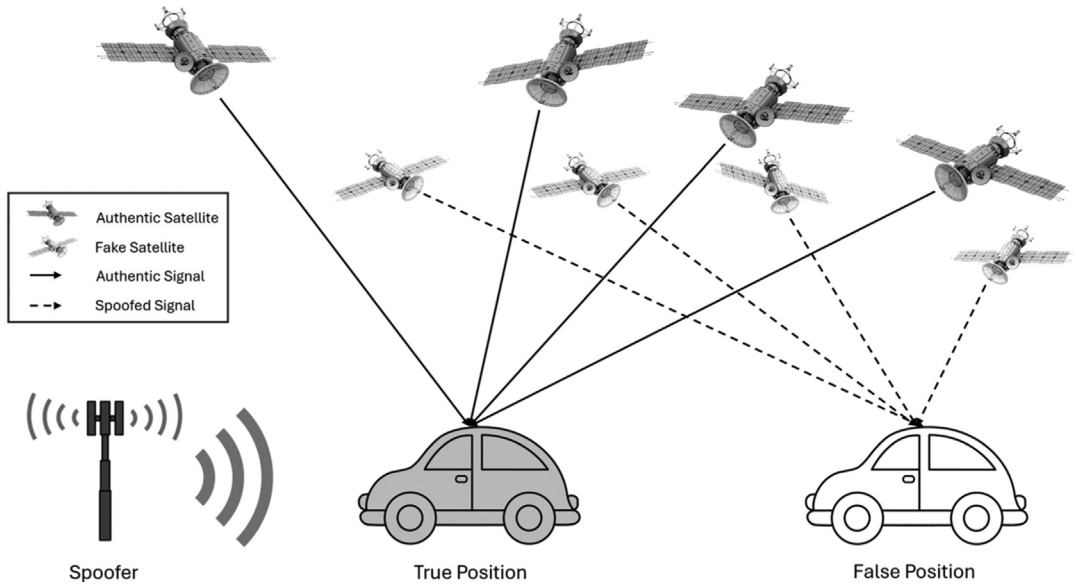

FIGURE 15.5

Spoofing.

In contrast, as shown in Fig. 15.6 during an intentional GNSS jamming attack, attacker disrupts satellite signals by inundating the spectrum with overpowering RF signals. Attackers execute continuous or pulsed jamming, presenting challenges for GNSS receivers to adapt to the interference. Mitigating jamming threats involves the use of antijamming filters to attenuate interference, frequency diversity to operate on multiple bands, and null steering capabilities in advanced antenna arrays to dynamically nullify jamming signals [21]. Integrated defense strategies encompass the implementation of spoofing detection algorithms, machine learning (ML) models for anomaly detection, and redundant systems, such as multiple GNSS receivers and alternative navigation sensors, to ensure continued accuracy even in the face of compromised systems. As these threats persist and evolve, the development of robust, multilayered defense strategies remains imperative to safeguard the reliability and security of GNSS applications across diverse operational scenarios. Furthermore, situations may arise where satellite signals are not available or visible, such as in locations like tunnels or areas with tall buildings that can obstruct signals, leading to unintentional jamming.

15.3.4 Segment errors

Segment errors are categorized into three types: (1) space segment error; (2) user segment error; and (3) control segment error. The space segment error encompasses orbital errors, which result from discrepancies between the calculated and actual satellite positions, as well as clock errors that

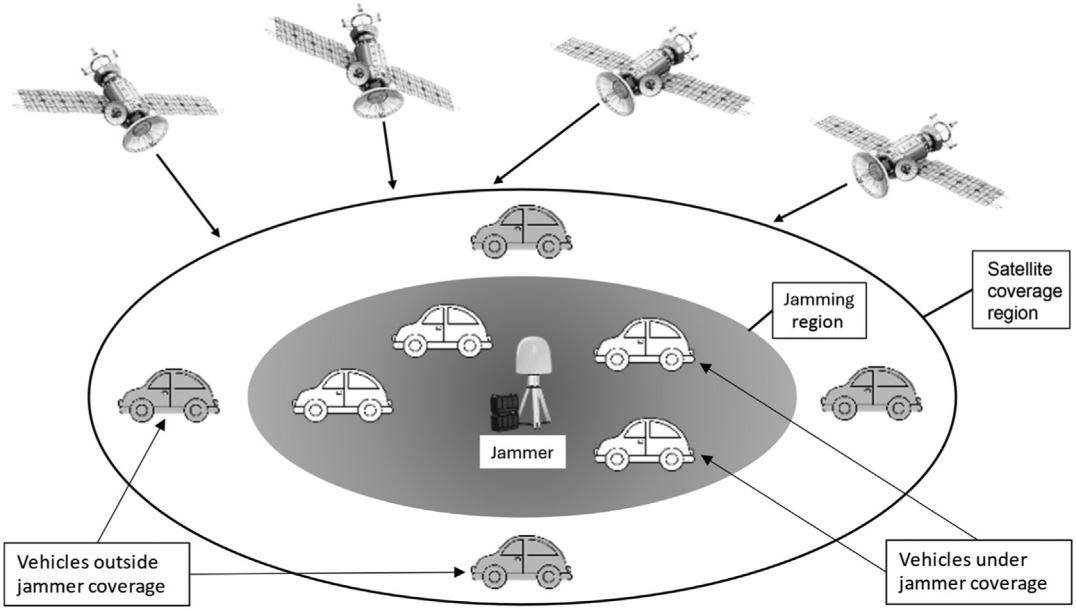

FIGURE 15.6

Jamming.

can occur due to drifts or offsets in the onboard atomic clocks. User segment errors, on the other hand, emanate from the GNSS receiver itself, encompassing issues, such as receiver clock inaccuracies, signal processing errors, multipath interference, and the receiver's capability to handle atmospheric effects [22,23]. Additionally, antenna errors, including variations in the antenna's phase center and alignment errors, can introduce inaccuracies. Lastly, the control segment transmits ephemeris data and monitors each satellite's health. Errors in the transmitted ephemeris data or incorrect satellite health information can lead to user position calculation errors. Understanding and mitigating these segment errors are essential for achieving precise GNSS positioning and navigation, with techniques, such as GNSS augmentation systems and differential corrections playing vital roles in enhancing overall accuracy. Addressing space segment errors involves advanced satellite clock synchronization techniques, precise orbit determination methods, high-quality atomic clocks, and sophisticated orbit prediction models. For user segment errors, mitigation strategies focus on refining receiver designs, compensation algorithms, integration methodologies, and bias correction techniques, validated through rigorous testing using GNSS simulators [24]. Control segment errors are mitigated through continuous refinement of navigation message protocols, precise orbit determination techniques, and the utilization of advanced ionospheric models with real-time monitoring.

15.4 Spoofing attack modeling

15.4.1 Attack modeling approaches

Spoofing attack modeling is the process of simulating and analyzing potential attacks on GNSS signals and receivers to understand their vulnerabilities and develop countermeasures. Spoofing involves generating false GNSS signals that appear indistinguishable from authentic ones, misleading the GNSS receiver. Fig. 15.7 shows GNSS spoofing attack modeling framework. The first stage, attack type specification, involves identifying and defining different types of spoofing attacks such as synchronous, asynchronous, attacks with multiple transmitters, and meaconer attacks. This stage requires a deep understanding of the technical aspects of each attack type, including signal characteristics like strength, synchronization, and frequency bands.

In a synchronous GNSS spoofing attack, the attacker meticulously aligns the spoofer's signals with those from authentic GNSS satellites, both in phase, Doppler shift coordinates and timestamp creating a nearly perfect imitation. The spoofed signal also needs to mimic authentic almanac and ephemeris data. Phase refers to the position of a point in time on a waveform cycle. In GNSS signals, phase alignment ensures that the spoofed signal's wave pattern aligns precisely with that of the satellite's signal at any given moment. This alignment is crucial because GNSS receivers use phase information to calculate precise distances from satellites. Doppler shift is the change in frequency or wavelength of a wave as perceived by a receiver moving relative to the correspoding source of the wave. GNSS signals experience a Doppler shift as satellites move relative to the Earth. A successful spoofing attack requires the imitated signals to match this Doppler shift accurately, ensuring the spoofed signal's frequency appears consistent with the movement of the GNSS satellites from the perspective of the receiver. A nuanced aspect of synchronous attacks is controlling the power of the spoofed signal. For a GNSS receiver to transition to the spoofer's signal, the spoofed signal must be stronger than the authentic satellite signals. Typically, a power superiority of about 4 dB (decibels) is sufficient. This power level ensures that the

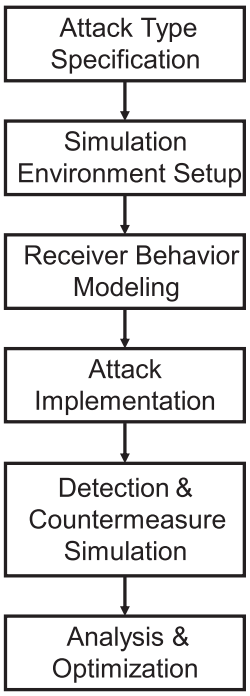

FIGURE 15.7

Spoofing attack modeling framework.

spoofed signal dominates over the legitimate signals, compelling the GNSS receiver to lock onto the stronger, spoofed signal. However, this power level must be carefully managed. If the power is too high, it might raise suspicions or trigger antispoofing mechanisms in the receiver.

In an asynchronous or deliberate coherent GNSS spoofing attack, the initial step involves disrupting the receiver's ability to track genuine satellite signals. This disruption is typically achieved by significantly increasing the spoofer's signal power. Technically, this means generating signals at the phase center of the receiver's antenna that are 40−50 dB higher in power than the signals from authentic satellites. This dramatic increase in signal strength serves two purposes. Firstly, it overpowers the genuine signals, causing the GPS receiver's tracking algorithms to lose their lock on these weaker signals, effectively drowning them in the noise of the stronger spoofed signals. Secondly, this loss of tracking forces the GPS receiver into a "search mode," where it seeks out new signals to lock onto. In this vulnerable state, the GPS receiver inevitably locks onto the now-dominant counterfeit signals. Achieving such a significant power differential is a complex task, requiring a powerful transmitter and precise calibration to avoid immediate detection or triggering protective measures in sophisticated receivers. The spoofer must also ensure that the signal structure, including correct modulation and plausible data content and timing, is maintained, even though the spoofed signals do not perfectly align with the authentic signals in phase and timing.

Executing a meaconing attack involves recording signals from GNSS satellites and then replaying them, either in a synchronous or asynchronous manner. This attack can be particularly effective due to its ability to manipulate genuine satellite signals. A key component in this attack is the field-programmable gate array (FPGA). An FPGA is used to modify the recorded signal in real time before it is rebroadcast. This capability is crucial, as it allows the attacker to introduce specific distortions to the signal. For instance, the FPGA can be programmed to alter the timing of the signal, effectively shifting the perceived position or time reported by the GPS receiver. One of the most significant advantages of meaconing attacks using FPGAs is their ability to target receivers that rely on signals with cryptographic protection. Since the attack is based on rebroadcasting actual satellite signals, it can bypass any encryption. This makes meaconing a potent threat even to more secure GPS systems.

Synchronous spoofing attacks employing multiple transmitters represent a sophisticated escalation in spoofing techniques, where detection becomes significantly more challenging. In such attacks, the key limitation of single-transmitter attacks – detection through the angle of arrival (AoA) of RF signals – is overcome. Instead of all satellite signals originating from a single direction, which is a clear giveaway of spoofing, multiple transmitters are used, each accurately synchronized to mimic the signal of an individual satellite. These transmitters are strategically placed around the target, creating a scenario where signals appear to come from various directions, mirroring the real satellite constellation. Executing such an attack is very expensive.

The next stage, simulation environment setup, is focused on establishing a controlled environment to simulate the attacks and assess their impacts. This involves using software-defined radios (SDRs) or GNSS simulators, GNSS jammers, RF amplifiers, and directional antennae. The setup aims to mimic real-world conditions by configuring parameters like signal strength and considering environmental factors. Numerous readily available SDRs are on the market, including options like HackRF One, ADALM-Pluto, bladeRF, and LimeSDR, all priced at less than $500 each. GPSPATRO [25] achieved synchronized spoofing attack using a $1470 setup. Islam [26] used Orolia Skydel software-defined GNSS simulator for generating spoofed dataset. Warner and Johnston used a GS720 GPS simulator, Hamphreys used a C/A code spoofer, where an authentic GPS signal with delay adjusting pseudorange measurements was replayed [27]. All these attacks are targeted at the GNSS physical layer. Along with signal level modeling, the environmental factors that affect signal propagation, like atmospheric conditions, urban settings, or terrain are also modeled. By modeling these conditions, one can understand how a spoofer might exploit them to enhance the efficacy of an attack.

Receiver behavior modeling is the third stage, where the focus is on simulating how a GNSS receiver processes both legitimate and spoofing signals. This stage involves implementing algorithms that emulate the receiver's signal processing, tracking, and navigation solution computation. One of the key challenges here is to accurately model the receiver's vulnerabilities and how it handles signal processing anomalies. The fourth stage, attack implementation, involves executing the spoofing attack as defined earlier. In asynchronous attacks, the primary focus is on overpowering legitimate signals, while in synchronous attacks, ensuring precise synchronization of the signals is crucial.

Detection and countermeasure simulation, the fifth stage, tests the effectiveness of various detection methods and countermeasures against the spoofing attacks. This involves implementing techniques such as AoA estimation, signal-to-noise ratio monitoring, and cross-verification with

other GNSS systems. Additionally, countermeasures such as multiconstellation reception, antijamming techniques, and advanced signal analysis are tested for their effectiveness. Attack detection methods are discussed in detail in the next section.

In the final stage of the framework, the analysis and optimization of the attack are carried out. This is done by studying the impact of the attack under varying conditions and constraints. Furthermore, the attacks are evaluated against a suite of existing countermeasures to detect and/or mitigate similar attacks. Consequently, based upon these evaluations, the attack strategies and parameters are fine-tuned such that optimal values may be identified.

15.4.2 An application of attack framework

Advanced data analytics can play a crucial role in creating sophisticated spoofing attacks. The attack can be synchronous or asynchronous; for all types of attacks, navigation data or the signal characteristics need to be optimized to achieve the attack where advanced data analytics can play a crucial role. Fig. 15.8 presents a GPS spoofing attack modeling framework where advanced data analytics can be used to emulate spoofing signal information to carry out a slow drifting attack where the spoofer gradually shifts the perceived location of the target. In such an attack, a spoofer must have prior knowledge of spoofed path and closely monitor the target's position to share the same satellite observations. The spoofer's receiver records genuine GPS signals, including navigation data from the RINEX file and pseudorange information. To create spoofed pseudorange values, the spoofer combines real pseudorange data with predefined spoofed locations using the Spoofed Pseudorange Emulator (SPE). The SPE uses correlations or ML techniques to calculate estimated spoofed pseudoranges for a desired location. These spoofed pseudoranges, combined with genuine CEI variables from navigation data, are input into the GPS receiver's location calculation algorithm to compute the spoofed location. If they align with the intended spoofed location, the spoofed pseudoranges are transmitted to the spoofer GPS signal simulator. During this phase, GPS signals are manipulated by modifying the signal generation time and carrier phase to ensure a smooth

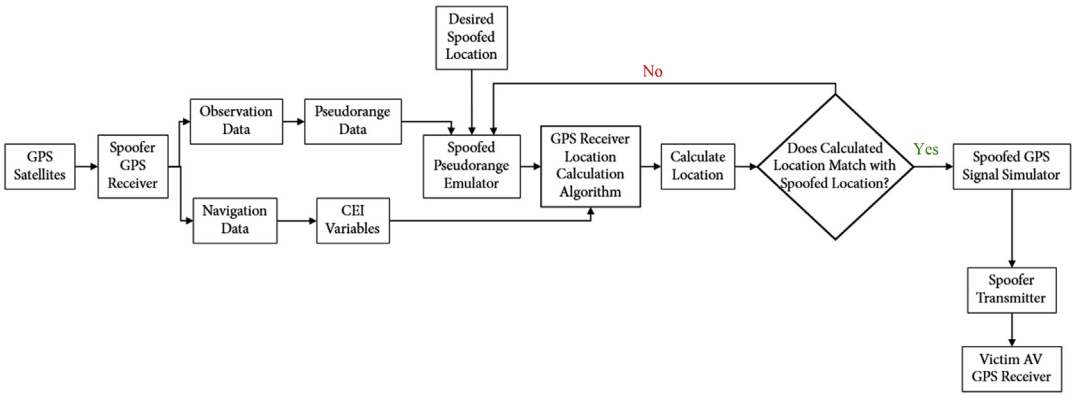

FIGURE 15.8

Attack modeling framework.

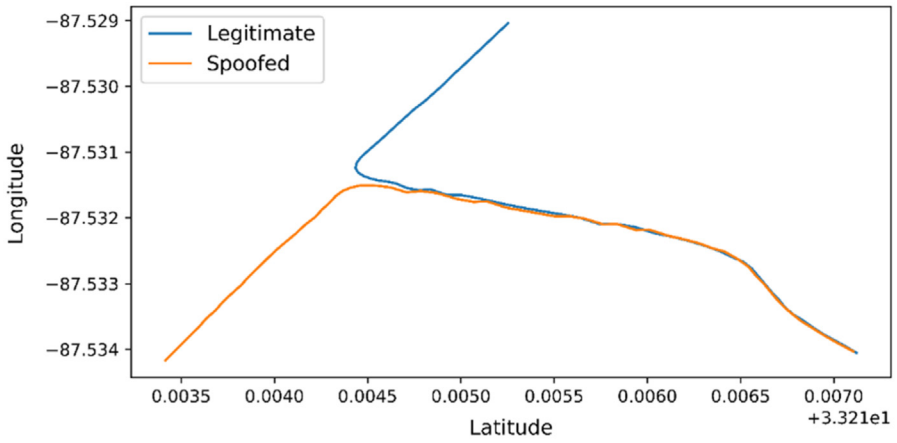

FIGURE 15.9

Legitimate and spoofed route.

transition, maintaining consistent signal properties without sudden changes once the spoofer locks onto the target's receiver. The set frequency of changes in the spoofed location simulates a gradual deviation from the target's actual path. Finally, the simulated GPS signals are sent to the target's GPS receiver, carrying out the stealthy slow drift attack and enabling its detection.

Data from prior tests can be used for training ML models or determining correlation between the spoofed and legitimate route as shown in Fig. 15.9.

15.5 Attack detection

15.5.1 Attack detection approaches

Detecting GNSS spoofing attacks is challenging due to their complexity and diversity. A significant challenge arises from the subtlety of these attacks; to an untrained receiver, spoofed signals can appear remarkably like legitimate ones. This issue is compounded by the easy availability of low-cost spoofing devices, which lowers the barrier for potential attackers, thereby increasing both the risk and frequency of such attacks. Another challenge lies in the diversity of spoofing techniques employed. Attackers might manipulate various aspects of the signal, such as its strength or timing, making it hard to develop a universal detection strategy. This variability demands tailored solutions, which can be resource-intensive to implement. Fig. 15.10 categorizes GNSS spoofing attacks into three distinct levels: at the signal level, through advanced receiver techniques, and at the system level.

At the signal level, the mitigation of GNSS spoofing attacks hinges significantly on encryption and authentication techniques. These methods play a crucial role in ensuring the authenticity of the signals received by GNSS receivers and safeguarding them against unauthorized tampering.

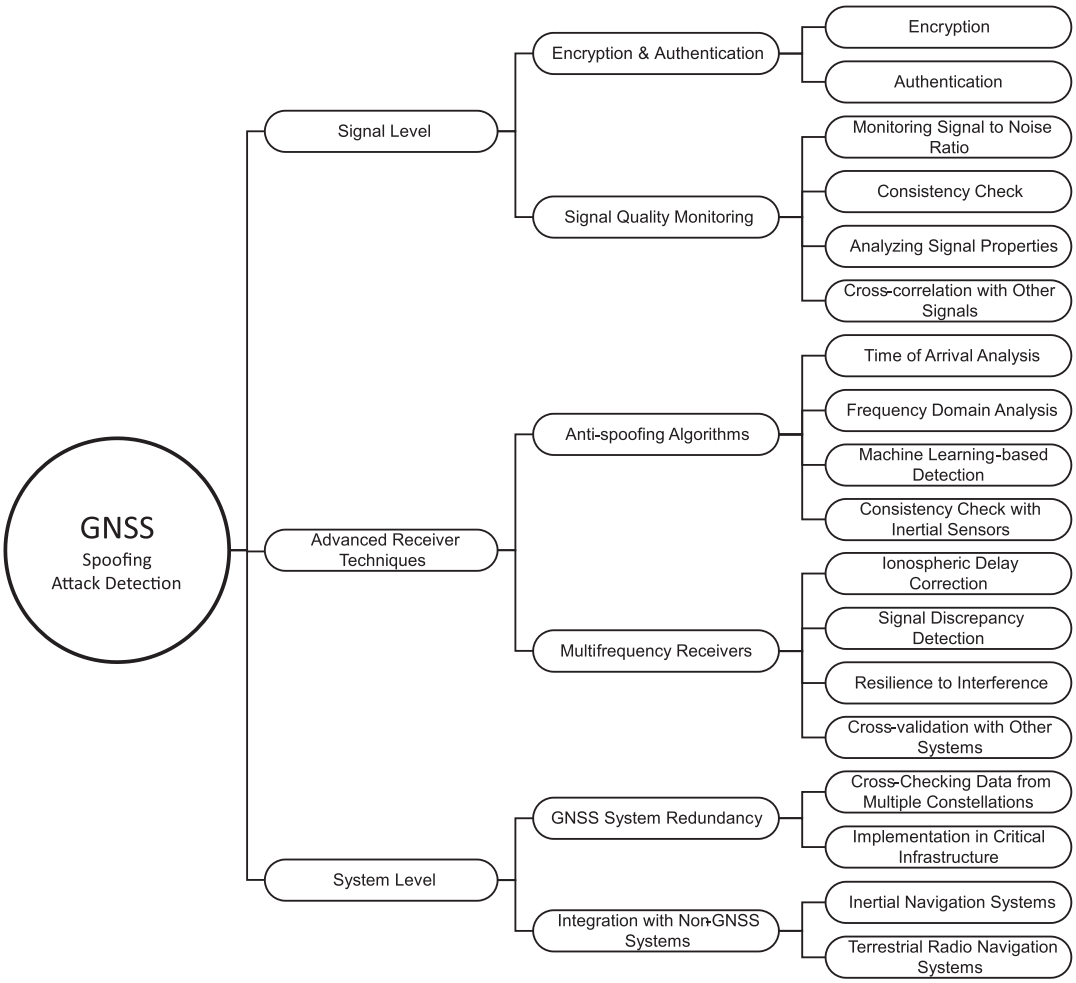

FIGURE 15.10

GNSS spoofing attack detection techniques.

Encryption is a process that encodes GNSS signals in a way that only receivers with the correct decryption key can decode them. This method is especially prevalent in military applications, where GPS signals are encrypted using codes such as the P(Y)-code. This encryption prevents easy replication or interference by unauthorized entities, thereby enhancing signal security and making it difficult for attackers to generate believable spoofed signals without access to these encryption keys. Authentication serves as an additional security layer, verifying that the signals received are indeed from legitimate sources. A common technique involves digital signatures; GNSS satellites can digitally sign their signals, which are then verified by receivers equipped with the appropriate public keys. A notable example is the European Galileo system's plan to implement the Open

Service Navigation Message Authentication, aimed at authenticating signals for civilian usage. This service will enable receivers to validate the authenticity of navigation messages, significantly complicating the spoofing process. Signal quality monitoring (SQM) is another foundational approach in detecting potential spoofing. This includes monitoring the signal-to-noise ratio (SNR) of the signals. Receivers can identify abrupt changes in SNR, which are often indicative of spoofing. Spoofed signals typically exhibit a higher SNR than authentic ones, and receivers with advanced programming can flag such anomalies. Consistency checks compare incoming signal characteristics with expected norms, such as arrival time and power level. Deviations from these expected parameters can signal a spoofing attempt. Moreover, analyzing signal properties like carrier phase and AoA helps discern the legitimacy of signals. Techniques like directional antenna systems or multiple antenna arrays aid in determining the direction of incoming signals, distinguishing between legitimate satellite signals and ground-based spoofers. Finally, cross-correlation with other signals involves comparing the GNSS signal with signals from different satellites or systems to spot inconsistencies, further aiding in spoofing detection.

In GNSS spoofing mitigation, advanced receiver techniques play a crucial role. Modern receivers are increasingly equipped with sophisticated antispoofing algorithms designed to scrutinize incoming signals for any anomalies that might suggest spoofing attempts. One key algorithm is the ToA analysis, which assesses the arrival times of signals from various satellites. In spoofing scenarios, these times often misalign with the expected satellite positions, and by comparing the actual ToA with a database of expected positions, receivers can pinpoint potential spoofing. Another technique, frequency domain analysis, delves into the frequency components of the signals. Here, spoofed signals might present unusual frequency traits or shifts, detectable through spectral analysis. Furthermore, the integration of ML-based detection methods allows for the training of algorithms on datasets comprising both authentic and spoofed signals. Once trained, these algorithms adeptly distinguish between genuine and counterfeit signals in real time. Some receivers also incorporate consistency checks with inertial sensors. These sensors, providing an independent source of navigation data, can be cross-referenced with GNSS data. Significant deviations from inertial sensor data could flag potential spoofing incidents. Another innovative approach is the use of multifrequency receivers. These receivers, by processing signals across multiple frequencies, can execute checks that are beyond the capability of single-frequency receivers. They play a pivotal role in correcting ionospheric delays, a natural occurrence affecting signal timing. Spoofed signals often fail to accurately mimic these delays, enabling multifrequency receivers to spot inconsistencies. Additionally, these receivers can compare signal content across different frequencies to detect discrepancies, a common shortfall in spoofing attacks. Their ability to switch frequencies to avoid interference or spoofing on a specific band further enhances their resilience. Moreover, these receivers can cross-validate data with other navigation systems like Galileo or GLONASS, bolstering the reliability of their spoofing detection capabilities.

System-level mitigation approaches in GNSS spoofing involve comprehensive strategies that extend beyond just individual receivers or signals, focusing instead on the broader GNSS infrastructure and its integration with complementary systems. These approaches are designed to fortify the overall GNSS ecosystem, enhancing its robustness and resilience against spoofing attempts. A key aspect of this is GNSS system redundancy. Redundancy plays a vital role in bolstering the resilience of GNSS systems against spoofing attacks by employing multiple GNSS constellations, such as GPS, Galileo, GLONASS, and BeiDou. This setup provides

overlapping coverage and enables cross-verification of data, allowing for the identification of discrepancies that may arise from spoofing in one system. This redundancy is particularly crucial in critical infrastructures like aviation navigation, financial systems, and power grid timing, where using multiple GNSS sources ensures not only continuity of service but also an additional layer of security. Another significant strategy is the integration with non-GNSS systems. By combining GNSS with other non-GNSS technologies, the overall reliability of positioning and timing solutions is substantially enhanced, especially in scenarios where GNSS signals are compromised. One such integration involves inertial navigation systems (INS), which, when combined with GNSS, provide continuous navigation solutions even in the absence or unreliability of GNSS signals due to spoofing. INS systems can maintain accurate tracking independently for a certain period, thereby allowing for effective cross-checking with GNSS data. Additionally, terrestrial radio navigation systems such as eLORAN or GBAS offer alternative navigation signals. These systems can either validate GNSS data or serve as substitutes, thus providing an additional safeguard against GNSS signal compromise. Together, these system-level approaches cover all the GNSS spoofing attack detection strategies.

15.5.2 An application of attack detection framework

Fig. 15.11 presents an example of a robust GNSS spoofing attack detection framework where advanced data analytics is used. It utilizes a dual-strategy approach by fusing data from in-vehicle low-cost sensors—including GNSS, accelerometer, steering wheel angle, and speedometer. This integrated approach enhances the detection of GNSS spoofing attacks by leveraging both vehicle state predictions and maneuver recognition. The first strategy involves creating a predictive model for the vehicle's state, which estimates changes in location by synthesizing data from various in-vehicle sensors. Using speed, acceleration, and steering angle data, a deep recurrent neural network (RNN), specifically a long short-term memory (LSTM) model, is trained to predict the vehicle's location change over time. The LSTM's capacity to remember long-term dependencies in time-series data enables accurate prediction of these shifts. In parallel, the vehicle's motion state is continually verified through the speedometer readings, ensuring that any discrepancy between the speedometer and GNSS data that falls outside an acceptable error threshold flags a potential attack, aiding in identifying scenarios where the vehicle is unexpectedly stationary or moving too rapidly.

The second strategy employs steering angle data to detect the type of turning maneuvers being executed—left or right turns. Steering angle sensor can yield turn maneuver data. Given the variations in driving patterns and roadway turn curvatures, the duration of steering angle data may vary between turns. To classify these maneuvers, a dynamic time warping algorithm, trained on various turn sequences from a turning dataset, assesses the similarity between time series data, while a k-NN classifier algorithm categorizes the turns. To ensure accuracy, this detection system cross-references inertial sensor outputs with GNSS turn information. It accounts for scenarios where the vehicle might appear to be turning—evident from steering wheel data—while stationary, such as during parking adjustments. In these cases, the speedometer data are consulted; if the vehicle's speed is above a certain error threshold as shown in Fig. 15.11, a turn is confirmed, otherwise, it is disregarded.

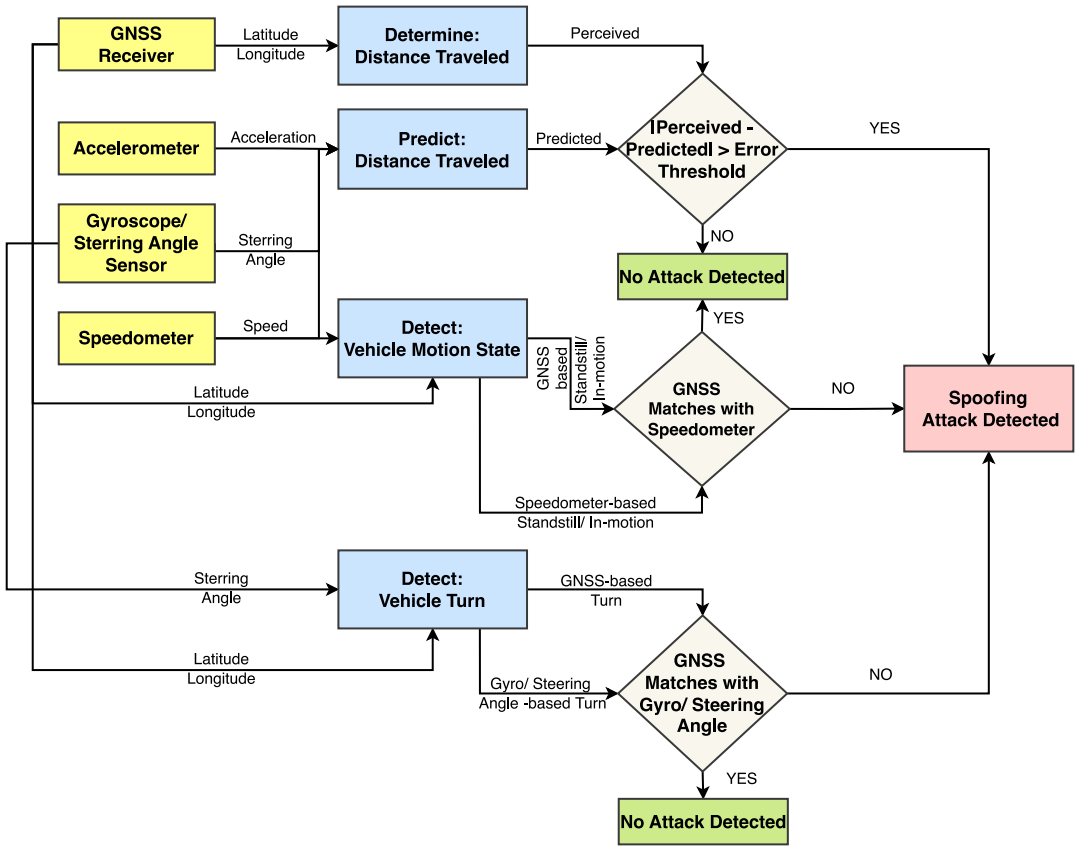

FIGURE 15.11

Global navigation satellite system spoofing attack detection framework. Adapted from [15].

15.6 Attack mitigation

15.6.1 Attack mitigation approaches

GNSS spoofing attack mitigation techniques primarily fall into two categories. The first involves the detection and classification of spoofing signals, distinguishing them from authentic signals. This process is critical for isolating and excluding spoofed signals, thereby ensuring that position estimation relies solely on authentic signals. This is achieved through techniques such as array antennas. The second category involves navigating without relying on GNSS services, using alternative methods, such as inertial navigation systems or other non-GNSS-based technologies to maintain location accuracy even when GNSS signals are compromised or unreliable.

In most of the GNSS spoofing attacks, spoofers often transmit multiple spoofed GNSS signals from a single antenna, resulting in spatially correlated spoofing signals. During such attacks, two

distinct scenarios may arise: one where the target receiver receives only spoofed signals, and another where it receives a mixture of spoofed and authentic signals. In the sole presence of spoofed signals, multiple antennas cannot be employed for mitigation. However, in situations where both authentic and spoofed signals are present, an array of antennas can result in effective and efficient mitigation solution. This configuration allows for the discrimination between genuine and falsified signals by implementing temporal, spatial filters, beamforming, power level monitor, phase difference monitor, pairwise correlation monitor, and clock bias variation monitor using moving receivers. Despite their effectiveness, these solutions come with drawbacks, including high computational demands and the need for costly hardware. Moreover, antenna array processing can introduce biases, which are particularly problematic in high-precision GNSS applications.

However, if no authentic GNSS signal is available during the spoofing attack, GNSS-independent navigation techniques, such as INS, visual odometry (VO), LiDAR-based navigation, and sensor fusion-based navigation, using a 3D map or signal of opportunity (SOP) can take over the navigation function. INS work by using accelerometers and gyroscopes to track the motion and orientation of a vehicle. Accelerometers track linear acceleration, whereas gyroscopes gauge angular velocity. By integrating these measurements over time, INS can calculate the vehicle's current position and orientation, starting from a known initial point. However, INS has limitations, such as error accumulation over time (drift) due to small inaccuracies in the sensors. These errors can grow significantly, leading to decreased accuracy the longer the system operates without GNSS.

VO estimates the position and orientation of a vehicle by analyzing sequences of camera images. It tracks the motion of the vehicle by observing changes in the positions of specific points or features between frames. As the vehicle moves, the apparent motion of these features across the camera's field of view is used to infer the vehicle's trajectory. However, VO is limited by its reliance on visual data; it can be less effective in low-light or featureless environments and can suffer from cumulative errors over time, requiring periodic recalibration or integration with other navigation systems for improved accuracy.

LiDAR-based navigation involves using LiDAR sensors to generate detailed 3D maps of the environment. These sensors emit laser beams and measure the time taken for the light to return after reflecting off surrounding objects, thereby determining distances. By continuously scanning the environment, LiDAR constructs a real-time map, allowing the vehicle to locate itself and navigate within it. However, LiDAR systems can be limited by environmental factors like fog, rain, or dust that interfere with laser propagation, and they often involve high costs and substantial computational resources for processing the data.

Sensor fusion-based navigation without GNSS combines data from multiple sensors like accelerometers, gyroscopes, magnetometers, radars, cameras, and LiDAR. This approach aggregates and processes these diverse data streams to determine a vehicle's position and orientation, compensating for the limitations of individual sensors. However, sensor fusion systems can be complex, requiring sophisticated algorithms for data integration and error handling. The effectiveness of the system depends on the quality and calibration of the sensors, and it may still accumulate errors over time, necessitating periodic recalibration or external reference points. All these methods can only provide local position estimates and the error diverges at some point as it is a dead-reckoning type sensor.

3D map-based navigation uses preexisting or dynamically created 3D maps of the environment. This approach involves sensors like LiDAR or cameras to continuously map the surroundings and compare it with the 3D map to determine the vehicle's location and navigate accordingly.

However, this method's accuracy depends heavily on the updated quality of the 3D maps. Changes in the environment that are not reflected in the maps can lead to navigation errors. Furthermore, processing the vast amount of data from these sensors for real-time navigation requires significant computational power and can be challenging in dynamic, unstructured environments.

SOP-based navigation uses existing nonnavigation signals, like AM/FM radio, WiFi, TV, cellular signals, or low earth orbit satellite signals, as makeshift beacons for positioning. The system estimates the vehicle's position by measuring signal characteristics, such as time of arrival or signal strength from multiple known transmitter locations. While SOP offers a viable alternative in GPS-denied environments, its accuracy depends on the density and distribution of signal sources. Additionally, urban environments with complex signal propagation, such as reflections off buildings, can introduce errors, limiting the reliability of SOP navigation.

15.6.2 An application of attack mitigation framework

Fig. 15.12 demonstrates a GNSS spoofing mitigation framework to navigate the target vehicle combining geographic information system and landmark-based in GNSS-denied urban environments. The framework harnesses data from the in-vehicle systems to achieve accurate navigation along its desired path. A dual-stage approach employing two distinct strategies is used. The first strategy relates to estimating the location of an AGV along its planned route and the second strategy continually makes corrections to the estimated locations by recognizing landmarks along the planned route of the AGV.

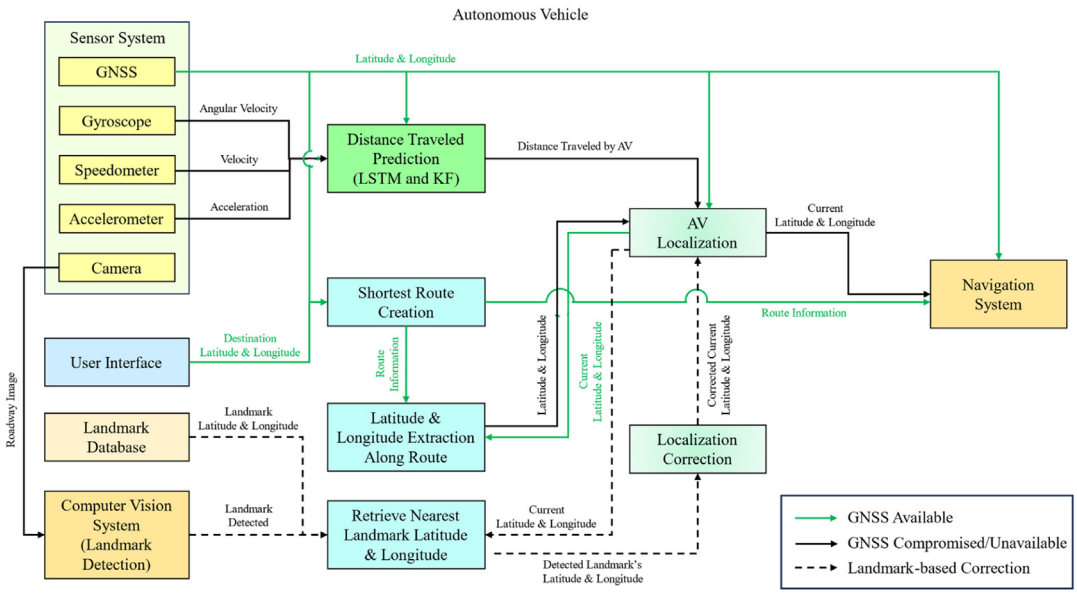

FIGURE 15.12

Global navigation satellite system spoofing attack mitigation framework.

The first strategy performs a fusion of the in-vehicle sensor data, that is, GNSS receiver, accelerometer, speedometer, and gyroscope data to maintain reliable AGV navigation. The strategy identifies the shortest route between the AGV's current location and its destination. In the event of a GNSS compromise, the data from the GNSS receiver becomes unavailable. Localization is then performed by fusing the data from the other sensors. At each timestep, the distance moved in the next timestep is predicted using a ML model and a KF. In particular, a specialized form of a RNN named LSTM is employed for this application due to its popularity in time-series prediction. The LSTM model is trained using uncompromised GNSS and in-vehicle sensor data prior to deployment. In a complimentary approach, a KF-based distance traveled estimation is also performed using the same sensor data. The estimated or predicted distances traveled are then used to locate the vehicle along its navigation path.

Due to inherent errors and biases within sensors, the distance estimation approach accumulates errors continually over time, which can hinder its applicability to navigation correction. The second strategy aims to perform corrections at frequent intervals such that the effects of accumulated errors are mitigated. Landmarks, such as traffic intersections and large parking lot entry and exit points are chosen and their accurate positions are stored in a database. Considering the AGV's reliance on accurate and detailed maps for navigation, it can be assumed that the map would accurately represent these landmarks. The camera sensors and the computer vision system on an AGV will enable it to identify landmarks along the way. After each landmark identification, the position of an AGV will be corrected using the accurate landmark position. Thus the twofold strategy can successfully locate an AGV and enable dependable navigation.

15.7 Conclusions

In the realm of GNSS security, sophisticated data analytics is increasingly playing a dominant role. This chapter has introduced several recent approaches to GNSS attack modeling, detection, and mitigation using data analytics. Nonetheless, the topic of GNSS security remains a dynamic field and thus further research is needed to make autonomous ground transportation resilient against the prevailing as well as unknown threats against GNSS-based navigation. With consideration to AGVs, several future research thrusts need to be explored. As GNSS attacks involve the manipulation of both the radio signal and the navigation message, newer receivers are becoming more adept at distinguishing between legitimate GNSS transmissions and naively fabricated GNSS signals. Therefore alongside the consideration of manipulating the navigation message to create an attack, researchers should also look at crafting the spoofed signals intelligently to evade signal-level detection. Future attacks need to craft their signals along with the navigation message in such a way as to appear indistinguishable from a satellite-based GNSS transmission. Furthermore, although the signals for military usage are encrypted, such encryption standards may not remain as secure in the future as quantum computing promises to break encryption protocols that are secure against classical computing hardware. In the detection approaches for GNSS attacks, there is a need to address detection at three distinct levels, that is, the radio signal level, navigation solution level, and sensor-fusion level. At the radio signal level, SQM-based methods are used to detect spoofed signals from legitimate signals. For the navigation solution level and sensor fusion level, various state estimation algorithms are utilized that use data from multiple sensors and sources to determine

accurate vehicle state even when there is an ongoing spoofing attack. Future research should investigate the vulnerability of these fusion and state estimation algorithms in the event of a sophisticated GNSS attack. For this purpose, data augmentation methods like Generative Adversarial Networks can be explored. Finally, for mitigation of GNSS attacks, the challenges of map matching methods that utilize high-definition maps are the high cost of computation and the requirement of frequent map updates. Methods relying on landmark-based navigation are emerging as a solution to this challenge. In this regard, research should investigate the relationship between data from the AVs INS and perception systems and the roadway landmark to establish an accurate vehicle position even if the GNSS signal is spoofed or unavailable. The synergistic outcome of these future research thrusts would ensure the security of future autonomous vehicle navigation and maintain the reliability and security of ground transportation in the face of evolving digital threats.

Questions and exercise problems

1. Explain the difference between intentional and unintentional threats on GNSS-based navigation systems.
2. Identify and discuss potential intentional GNSS vulnerabilities.
3. Do a comparative analysis between different navigation systems for AGV.
4. What are the four steps for cyber-resilient navigation systems development? Explain it.
5. Describe the contents of the navigation and observation file with examples.
6. Describe the following terms in the context of autonomous ground vehicle navigation: attack modeling, attack detection, and attack mitigation.
7. The GNSS pseudorange equation can be expressed as shown in Eq. (15.1). Given that $c = 299,792,458$ m/s. Suppose that the difference between the time the signal is transmitted and the time that the signal is received, that is, $(t_r - t_s)$ is 0.0673 s.
   a. What is the calculated pseudorange of the satellite to the receiver?
   b. Receiver clocks are not as accurate as the satellite clocks and unlike the satellite clocks, they are not routinely monitored for clock corrections. Suppose now that due to errors in the receiver clock, the time difference between transmission and reception is determined as 0.067 s. What is the pseudorange in this instance?
   c. What is the absolute error in pseudorange between the two instances?
   d. How can data from four or more satellites help to correct this difference?

References

[1] GPS: Technology that Truly Changed the World [Online]. Available from: https://www.forbes.com/sites/dianafurchtgott-roth/2023/09/26/gps-technology-that-truly-changed-the-world/?sh = 717c19b5a20c (accessed 03.03.24).

[2] The Serious Threat of GPS Spoofing: An Analysis | Aviation Week Network [Online]. Available from: https://aviationweek.com/business-aviation/safety-ops-regulation/serious-threat-gps-spoofing-analysis (accessed 11.12.23).

[3] C. Cai, C. He, R. Santerre, L. Pan, X. Cui, et al., A comparative analysis of measurement noise and multipath for four constellations: GPS, BeiDou, GLONASS and Galileo, Surv. Rev. 48 (349) (2016) 287–295.
[4] S. Kumar, S.S. Rao, M. Mondal, A.K. Singh, Study of the atmospheric and ionospheric phenomenon using GPS-based remote sensing technique, Atmos. Remote Sens. (2023) 261–282. Available from: https://doi.org/10.1016/B978-0-323-99262-6.00019-5.
[5] Z. Baldysz, G. Nykiel, D.B. Baranowski, B. Latos, M. Figurski, Diurnal variability of atmospheric water vapour, precipitation and cloud top temperature across the global tropics derived from satellite observations and GNSS technique, Clim. Dyn. 62 (3) (2023) 1965–1982. Available from: https://doi.org/10.1007/S00382-023-07005-0/TABLES/2.
[6] J. Saastamoinen, Atmospheric correction for the troposphere and stratosphere in radio ranging satellites, Use Artif. Satell. Geod. 15 (1972) 247–251.
[7] K. Lagler, M. Schindelegger, J. Böhm, H. Krásná, T. Nilsson, GPT2: empirical slant delay model for radio space geodetic techniques, Geophys. Res. Lett. 40 (6) (2013) 1069–1073. Available from: https://doi.org/10.1002/grl.50288. *Wiley Online Library*.
[8] Y. Yuan, L. Holden, A. Kealy, S. Choy, P. Hordyniec, Assessment of forecast Vienna mapping function 1 for real-time tropospheric delay modeling in GNSS, J. Geod. 93 (9) (2019) 1501–1514. Available from: https://doi.org/10.1007/S00190-019-01263-9.
[9] S. Bora, Ionosphere and radio communication, Resonance 22 (2) (2017) 123–133. Available from: https://doi.org/10.1007/S12045-017-0443-8/METRICS.
[10] A.J. Mannucci, C.O. Ao, W. Williamson, "GNSS radio occultation," Position, Navigation, Timing Technologies in the 21st Century, pp. 971–1013, 2020, https://doi.org/10.1002/9781119458449.CH33.
[11] O. M.-A. S. and Technology and undefined 2003, Kinematic GPS Positioning of LEO Satellites Using Ionosphere-Free Single Frequency Measurements, vol. 7, Elsevier, 2003, pp. 396–405. Available from: https://doi.org/10.1016/S1270-9638(03)00034-8.
[12] T.P. Yunck, Coping with the atmosphere and ionosphere in precise satellite and ground positioning (2013) 1–16 (March). https://doi.ortg/10.1029/GM073P0001.
[13] X. Liu, Y. Du, G. Huang, D. Wang, Q. Zhang, Mitigating GNSS multipath in landslide areas: a novel approach considering mutation points at different stages, Landslides 20 (11) (2023) 2497–2510. Available from: https://doi.org/10.1007/S10346-023-02117-4/FIGURES/12.
[14] S. Xin, J. Geng, L.T. Hsu, Factor graph optimization-based GNSS PPP-RTK: an alternative platform to study urban GNSS precise positioning, IEEE Trans. Aerosp. Electron. Syst. (2024). Available from: https://doi.org/10.1109/TAES.2024.3360380.
[15] S. Dasgupta, M. Rahman, M. Islam, M. Chowdhury, A sensor fusion-based GNSS spoofing attack detection framework for autonomous vehicles, IEEE Trans. Intell. Transp. Syst. 23 (12) (2022) 23559–23572. Available from: https://doi.org/10.1109/TITS.2022.3197817.
[16] J. Qiao, et al., A survey of GNSS interference monitoring technologies, Front. Phys. 11 (2023) 1133316. Available from: https://doi.org/10.3389/FPHY.2023.1133316/BIBTEX.
[17] L. Crosara, F. Ardizzon, S. Tomasin, N. Laurenti, Worst-case spoofing attack and robust countermeasure in satellite navigation systems, IEEE Trans. Inf. Forensics Secur. 19 (2024) 2039–2050. Available from: https://doi.org/10.1109/TIFS.2023.3340061.
[18] J. Lee, E. Schmidt, N. Gatsis, D. Akopian, Detection and mitigation of spoofing attacks against time synchronization and positioning, IEEE Access 11 (2023) 138986–139003. Available from: https://doi.org/10.1109/ACCESS.2023.3341028.
[19] A. Altaweel, H. Mukkath, I. Kamel, GPS spoofing attacks in FANETs: a systematic literature review, IEEE Access 11 (2023) 55233–55280. Available from: https://doi.org/10.1109/ACCESS.2023.3281731.
[20] O. Sharifi-Tehrani, M.H. Ghasemi, A review on GNSS-threat detection and mitigation techniques, Cloud Comput. Data Sci. 4 (2023) 161–185. Available from: https://doi.org/10.37256/CCDS.4320231678.

[21] M. Ding, W. Chen, W. Ding, Performance analysis of a normal GNSS receiver model under different types of jamming signals, Measurement 214 (2023) 112786. Available from: https://doi.org/10.1016/J.MEASUREMENT.2023.112786.
[22] A. Hauschild, O. Montenbruck, P. Steigenberger, Short-term analysis of GNSS clocks, GPS Solut. 17 (3) (2013) 295−307. Available from: https://doi.org/10.1007/S10291-012-0278-4/FIGURES/6.
[23] O. Montenbruck, P. Steigenberger, A. Hauschild, Comparing the 'Big 4' − a user's view on GNSS performance, 2020 IEEE/ION Position, Location and Navigation Symposium, PLANS 2020, pp. 407−418, 2020, https://doi.org/10.1109/PLANS46316.2020.9110208.
[24] Springer Handbook of Global Navigation Satellite Systems, 2017. https://doi.org/10.1007/978-3-319-42928-1.
[25] GNSS Spoofing Scenarios with SDRs | GPSPATRON.com [Online]. Available from: https://gpspatron.com/gnss-spoofing-scenarios-with-sdrs/ (accessed 08.12.23).
[26] S. Islam, M.Z. H. Bhuiyan, I. Pääkkönen, M. Saajasto, M. Mäkelä, et al., "Impact analysis of spoofing on different-grade GNSS receivers.," in *2023 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, 2023, pp. 492−499.
[27] T.E. Humphreys, B.M. Ledvina, M.L. Psiaki, B.W. O'Hanlon, P.M. Kintner, "Assessing the spoofing threat: development of a portable GPS civilian spoofer," Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008), 2008, 2314−2325.