remote sensing

MDPI

Review

A Survey of GNSS Spoofing and Anti-Spoofing Technology

Lianxiao Meng [1,2,†,‡], Lin Yang [2], Wu Yang [1,*] and Long Zhang [2,‡]

[1] Information Security Research Center, Harbin Engineering University, Harbin 150000, China
[2] National Key Laboratory of Science and Technology on Information System Security, Systems Engineering Institute, Beijing 10081, China
* Correspondence: yangwu@hrbeu.edu.cn;
† Current address: Network Information Research Institute, 13 Dacheng Road, Fengtai District, Beijing 10039, China.
‡ These authors contributed equally to this work.

Abstract: With the development of satellite navigation technology, the research focus of GNSS has shifted from improving positioning accuracy to expanding system application and improving system performance. At the same time, improving the survivability of satellite navigation systems has become a research hotspot in the field of navigation, especially with regard to anti-spoofing. This paper first briefly analyzes the common interference types of satellite navigation and then focuses on spoofing. We analyze the characteristics and technical mechanism of satellite navigation and the positioning signal. Spoofing modes are classified and introduced separately according to signal generation, implementation stage and deployment strategy. After an introduction of GNSS spoofing technology, we summarize the research progress of GNSS anti-spoofing technology over the last decade. For anti-spoofing technology, we propose a new classification standard and analyze and compare the implementation difficulty, effect and adaptability of the current main spoofing detection technologies. Finally, we summarize with considerations, prospective challenges and development trends of GNSS spoofing and anti-spoofing technology in order to provide a reference for future research.

Keywords: GNSS; spoofing; anti-spoofing; defense

check for updates

Citation: Meng, L.; Yang, L.; Yang, W.; Zhang, L. A Survey of GNSS Spoofing and Anti-Spoofing Technology. *Remote Sens.* **2022**, *14*, 4826. https://doi.org/10.3390/rs14194826

Academic Editors: Krzysztof Naus and Mieczysław Bakuła

Received: 12 August 2022
Accepted: 22 September 2022
Published: 27 September 2022

1. Introduction

Compared with traditional manned systems and equipment (MSE), unmanned systems and equipment (USE) such as unmanned aerial vehicles (UAVs) and unmanned ground vehicles (UGVs) has low cost, flexible use, can adapt to various dangerous situations, and can complete many tasks that manned equipment cannot complete [1]. Therefore, USE has achieved explosive development in many industries. Especially in the military field, USE has become a very important weapon in local war. USE has a strong dependence on satellite navigation, and its control is generally inseparable from the important position and speed data provided by the global navigation satellite system (GNSS). Generally speaking, the signal of USE navigation systems comes from GNSS; thus, the vulnerability of GNSS signals lead to vulnerability of the USE navigation system [2].

GNSS can provide all-weather position, velocity and time (PVT) serviced around the world. At present, major countries in the world are vigorously developing their own GNSS systems [3]. Global Positioning System (GPS) in the United States, Galileo in Europe, BeiDou navigation satellite system (BDS) in China and Global Navigation Satellite System (GLONASS) in Russia are the four major GNSS systems on earth. In addition, there are some small regional satellite navigation systems, including Indian Regional Navigation Satellite System (IRNSS) in India and Quasi Zenith Satellite System (QZSS) in Japan. In the real physical environment, when a USE flies close to complex environments of vegetation, water and/or cities, the GNSS signal is weakened or completely undetectable. This phenomenon is natural interference; it is difficult to predict and is not discussed in this paper [4]. In a hostile environment, attacks (denial of service, spoofing, jamming, link interference, etc.) based on navigation signals are easy to realize, the effect is obvious and the scope of action is wide; thus, the navigation system is generally the attack object that the enemy gives priority to. If the navigation system crashes due to intentional interference, this may affect the normal path of the USE and force it to deviate from the path without prior knowledge. In serious cases, this can cause the USE to crash or appear in an area that it should not be in and be taken over [5,6]. Therefore, at the beginning of the application of satellite navigation, many experts and scholars expressed concern about the safety of navigation signals. In 1995, MITRE (a U.S. company) made an in-depth analysis on the spoofing of civil satellite navigation systems [7]. In 2001, the U.S. Department of Transportation assessed the vulnerability of transportation facilities under civil GPS interference and issued a report on the vulnerability of GPS signals [8]. That report described civil GPS spoofing and suggested deeply studying the performance of spoofing so as to help put forward a strategy to detect spoofing. Since then, researches on satellite navigation spoofing and anti-spoofing technology have emerged one after another.

There are mainly two types of intentional interference of GNSS: jamming and spoofing [2]. Jamming generally refers to transmitting a certain bandwidth and high-power noise signal on the frequency of satellite navigation so that the signal-to-noise ratio of the receiver decreases and cannot work normally. Jamming is very simple to implement and relatively inexpensive, but it can easily to be detected by anti-radiation equipment [9]. Then, the interference source can be removed. Moreover, adaptive zeroing, beam forming, space–time two-dimensional filtering and other technologies and related products for anti-jamming have gradually matured. Thus the details of jamming are not discussed very much in this paper. Spoofing refers to replicating a false signal with exactly the same code phase, carrier frequency and Doppler frequency shift as the real navigation satellite signal to realize interference and capture. Thanks to the significant advantages of spoofing in interference concealment and interference efficiency, spoofing has gradually become the research hotspot for satellite navigation interference technology [10]. Thus, spoofing against USE is selected as the main problem to be discussed and analyzed in this paper.

Spoofing of GNSS is essentially broadcasting false spoofing signals in order to make the victim receiver misunderstand them as real signals. The victim may calculate the wrong position, the wrong clock offset, or both [11]. The calculation results in wrong position and/or wrong time and may induce dangerous behavior.

GNSS anti-spoofing technology attempts to detect attacks to warn victims that their navigation and clock are unreliable. The second goal of defense is to restore reliable navigation and timing solutions [12]. Commonly, an onboard receiver with receiver autonomous integrity monitoring technology (RAIM) uses redundant signals by default and then generates multiple GPS positions for comparison. The purpose of this is to determine whether the fault is related to a signal according to statistical methods [13]. However, back in 2001, the Volpe Center in the United States warned that some spoofing methods may exceed USE basic defense capability [14].

1.1. Contribution

With the development of technology, in order to ensure the security of USE in practical applications and maximize its application value, we need to understand the possible attack methods of spoofing and the characteristics of corresponding defense methods.

- This paper mainly introduces the current mainstream spoofing attack methods and defense methods and classifies and compares them separately.
- In order to facilitate the understanding and learning of USE spoofing and anti-spoofing techniques for later scholars, the review generally takes the form of a categorical summary presentation. While most of the past overviews have classified spoofing and anti-spoofing technologies according to their specific means of implementation, in this paper, we propose a classification method based on deception strategies in the context of a field in which all technologies are now becoming increasingly sophisticated.
- By analyzing the current state of technology, we propose separate proposals for the development of spoofing and anti-spoofing technologies.

1.2. Organization

In order to better explore anti-spoofing technology, this paper first introduces the development of satellite navigation spoofing technology. The rest of the paper is organized as follows.

Section 2 mainly introduces GNSS positioning principles and the vulnerabilities of GNSS. Section 3 first analyzes the characteristics of spoofing signals and the principles of spoofing attacks, and then introduces typical events related to satellite navigation spoofing. Section 4 classifies and discusses spoofing technology according to different standards. As for anti-spoofing technology, we put forward a new classification method in Section 5, and the research results in over the last ten years are summarized and compared. Section 6 focuses on the future research direction of spoofing and anti-spoofing technology. The conclusion of this research work are in Section 7.

2. Global Navigation Satellite System

2.1. GNSS Positioning Principle Synopsis

GNSS is a general term for a class of systems that mainly consists of four global positioning systems and two regional positioning systems [3], as shown in Figure 1. In order to better understand GNSS spoofing and anti-spoofing technology, we must first understand the basic working principle of GNSS. Positioning systems mentioned in this paper work on a similar principle. At present, GPS is widely used as the most mature system, so we take GPS as an example to illustrate the working principle of GNSS [15].

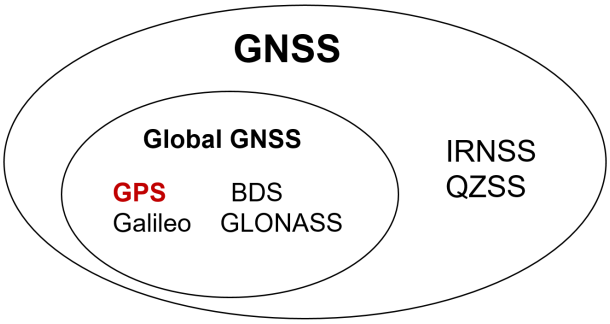


Figure 1. GNSS is a general term for a class of systems that mainly consists of four global positioning systems and two regional positioning systems. Among them, GPS is the most mature and widely used system.

GPS is a radio navigation and positioning system developed on the basis of the U.S. Navy navigation satellite system [16]. With omnipotent, global, all-weather, continuous and real-time navigation, positioning and timing functions, it can also provide users with precise PVT service [17]. Based on the GPS website (https://www.gps.gov/ accessed on 13 June 2022) (as of May 2021), there are currently 32 satellites in orbit in the GPS constellation, of which 31 are in operation and 1 is in maintenance. The space configuration of GPS satellites is shown in Figure 2. They continuously transmit broadcast signals, that is, navigation messages, which mainly carry the current timestamp and orbital coordinates of the satellite [18]. The time when the ground receiver receives the signal is subtracted from the time stamp carried by the message and then multiplied by the speed of light, c, to obtain the relative distance between the receiver and a single satellite. Therefore, when the ground receiver can receive more than three groups of GPS signals, the absolute position of the receiver on the earth can be solved directly according to the topological relationship of the satellites [19]. It is worth mentioning that the timestamp carried by the satellite is verified by the atomic clock, and the accuracy is much higher than that of the clock of the ground receiver [20]. In order to eliminate this error, a fourth satellite is generally introduced, and the current time is also used as a variable. This is the typical four-star positioning (Figure 3). The specific calculation process is as follows:

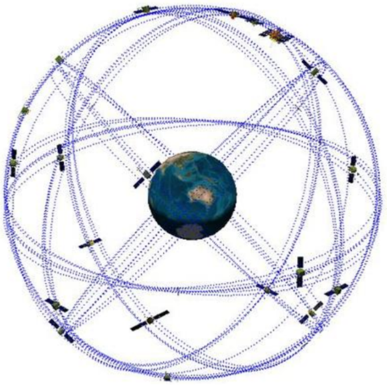


Figure 2. Deployment of GPS satellites: they are evenly distributed on six orbital planes and continuously transmit GPS signals.

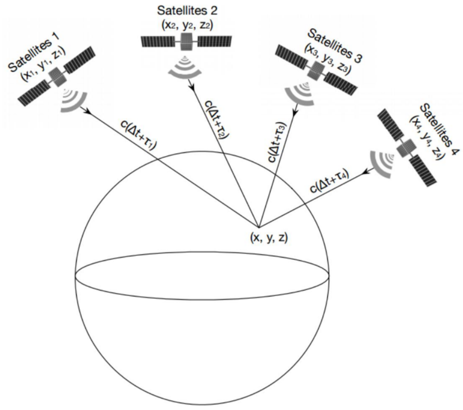

Satellites 1 (x1, y1, z1)
Satellites 2 (x2, y2, z2)
Satellites 3 (x3, y3, z3)
Satellites 4 (x4, y4, z4)
c(Δt+τ1)
c(Δt+τ2)
c(Δt+τ3)
c(Δt+τ4)
(x, y, z)

Figure 3. Topological relationship between GPS signal receiver and satellites: typical four-star positioning.

According to the timing characteristics of the satellite signal received by GPS in Figure 4, the formula can be obtained for the signal of satellite **i** in the spatial coordinate system:

$$(\Delta t + \tau_i) * c = P(x_i, y_i, z_i) - P(x, y, z) \tag{1}$$

where $\Delta t = T - T_0$, T_0 is the transmission time of the satellite signal, T is the reference receiving time, τ_i is the time delay of the received satellite i signal relative to the reference time, c represents the speed of light, $P(x_i, y_i, z_i)$ are the space coordinates of satellite i, and $P(x, y, z)$ are the space coordinates of the GPS receiver. The two vectors are subtracted into distance.

For four satellites, there are equations as follows:

$$\begin{cases} (\Delta t + \tau_1) * c = P(x_1, y_1, z_1) - P(x, y, z) \\ (\Delta t + \tau_2) * c = P(x_2, y_2, z_2) - P(x, y, z) \\ (\Delta t + \tau_3) * c = P(x_3, y_3, z_3) - P(x, y, z) \\ (\Delta t + \tau_4) * c = P(x_4, y_4, z_4) - P(x, y, z) \end{cases} \tag{2}$$

Thus, the quaternion equation can be solved and the receiver coordinates, $P(x, y, z)$, can be obtained as long as the coordinate position of each satellite is known and the relative propagation delay of each satellite signal is measured. This achieves accurate positioning of the receiver.

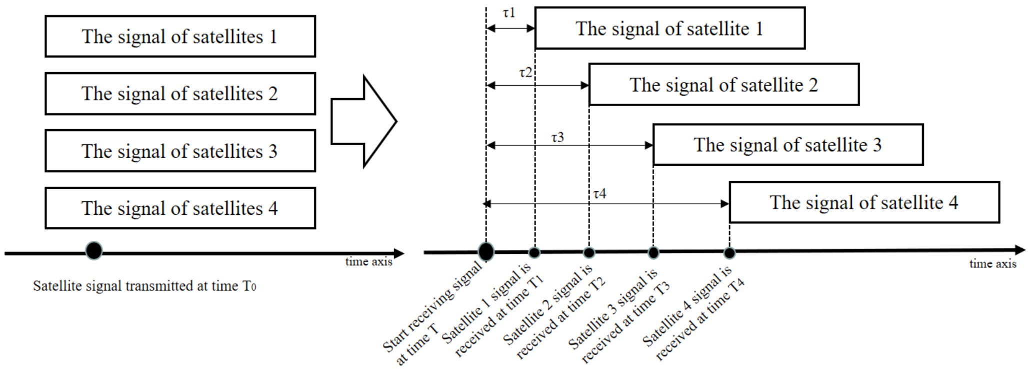

The signal of satellites 1
The signal of satellites 2
The signal of satellites 3
The signal of satellites 4
Satellite signal transmitted at time T0
time axis
τ1
The signal of satellite 1
τ2
The signal of satellite 2
τ3
The signal of satellite 3
τ4
The signal of satellite 4
Start receiving signal at time T
Satellite 1 signal is received at time T1
Satellite 2 signal is received at time T2
Satellite 3 signal is received at time T3
Satellite 4 signal is received at time T4
time axis

Figure 4. Example timing diagram of signal received by GPS receiver in four-star positioning.

2.2. GNSS Vulnerability Analysis

The vulnerability of GNSS itself is the basis of GNSS spoofing. The vulnerability of GPS mainly includes:

1. Navigation signal format disclosure: GNSS currently uses three public frequencies *L1*, *L2* and *L5* to broadcast navigation signals [21,22]. The spectrum characteristics, signal modulation format and pseudo-random code sequence of each frequency point have been disclosed. Similarly, taking GPS *L1* signal as an example, its signal parameters and characteristics are per Table 1:
   Because the main signal parameters have been disclosed, this means that there is no "secret" for the spoofer. Spoofers can often take targeted spoofing actions according to relevant signal parameters and characteristics [14].
2. Navigation data format disclosure: GNSS navigation message data usually include ephemeris, almanac, satellite clock parameters, ionosphere/troposphere and other important parameters [23]. These parameters play a very important role in accurate user positioning. However, in order to facilitate the use of relevant users, GNSS disclosed the arrangement mode, data definition and application method of its navigation message from the beginning [24]. This also means that a spoofer can easily and pertinently intercept and tamper with relevant navigation data, which means relevant users can receive wrong navigation data for the location solution without being aware, so as to achieve the purpose of spoofing.
3. Unprotected broadcast channel: in order to ensure the convenience of users, GNSS adopts a broadcast communication mode, that is, directly broadcast navigation signals to the majority of users [25]. This mode actually makes its communication channel directly exposed in the social space and vulnerable to interference, monitoring and tampering. In addition, because the GPS signal is extremely weak when it reaches the ground (the average signal power is often -150 dbw~-160 dbw) [26], only low directional power is needed in order to interfere with and suppress the legal GNSS signal, which objectively leads to a more fragile GNSS signal in practice [27].

Table 1. Signal parameters and characteristics, taking GPS L1 as an example.

Spread spectrum code type	C/A
Modulation mode	BPSK
Carrier frequency	1575.42 MHz
Spread spectrum code rate	1.023 MHz

3. GNSS Spoofing Synopsis

The concept of GNSS spoofing was first borrowed from spoofing attacks in the field of information security [5]. In the field of information security, the purpose of a spoofing attack is to obtain intelligence by using a person or a program successfully disguised as another person or another program through data tampering [28]. Overall, GNSS spoofing comes down to the same line. However, when GNSS spoofing acts on a USE, it is not satisfied with this. The attacker eventually expects to obtain control of the target through spoofing. GNSS spoofing means that the signal transmitter transmits a signal with the same structure and similar or stronger power as the satellite signal through an airborne or ground device so that the target mistakenly thinks it is a real signal and searches for and captures it. Jamming uses strong power to prevent satellite navigation terminals from receiving signals, which has the characteristics of large attack range; spoofing, on the other hand, is conducted by simulating satellite navigation signals [29]. Generally, for a specific attack object, spoofing has strong concealment and greater destruction and threat.

3.1. Data Level Characteristics of GNSS Spoofing Signal

In principle, the spoofing signal needs to have certain data characteristics that match those of the real satellite signal before it can be mistaken for the real signal and received by the attacked target [30].

The following is a mathematical expression of the typical GNSS signal [31]:

$$y(t) = Re\sum_{i=1}^{N} A_i D_i(t-\lambda_i(t))C_i(t-\lambda_i(t))e^{j(\omega_c t-\phi_i(t))} \tag{3}$$

where N is the number of signals constituting the spreading code; A_i is the carrier amplitude of the ith signal; $D_i(t)$ is the data bit stream of the ith signal; $C_i(t)$ is its extension code, usually a binary phase-shift keying (BPSK), pseudo random noise (PRN) code or bindery offset carrier (BOC)/PRN code; $\lambda_i(t)$ is the coding phase of the ith signal; ω_c is the nominal carrier frequency; and $\phi_i(t)$ is the ith beat carrier phase.

The mathematical expression of the spoofing signal can be obtained based on Formula (3) [31]:

$$y_s(t) = Re\sum_{i=1}^{N_s} A_{si}\hat{D}_i(t-\lambda_{si}(t))C_i(t-\lambda_{si}(t))e^{j(\omega_c t-\phi_{si}(t))} \tag{4}$$

Generally speaking $N_s = N$; that is, the number of spoofed signals is equal to the number of real signals. In order to spoof the receiver, each spoofed signal must have the same spreading code $C_i(t)$ as the corresponding real signal, and its best estimation of the same data bit stream $\hat{D}_i(t)$ is usually broadcast. For $i = 1,2,3,\ldots,N_s$, the spoofing amplitude, coding phase and carrier phase are A_{si}, λ_{si} and ϕ_{si}, respectively. These values may differ from the actual values because they are related to the type of attack initiated. During a spoofing attack, the maximum total semaphore that the receiver may receive is:

$$y_{total}(t) = y(t) + y_s(t) + v(t) \tag{5}$$

where $v(t)$ is other noise signals that may exist.

3.2. Influence of Spoofing on Satellite Navigation Signal Processing

The signal processing of a satellite navigation receiver usually includes three stages: RF front-end processing, baseband IF signal processing and navigation information output [32]. A typical GNSS receiver workflow is shown in Figure 5. Signal acquisition mainly completes the two-dimensional rough search of signal recognition, carrier frequency and code phase. In order to capture the satellite signal, the local receiver needs to reproduce the satellite code and carrier at the same time, integrate and accumulate with the received signal, and compare the accumulated result with the detection threshold to determine whether the satellite signal exists or not [10,33]. The signal tracking part uses the coarse carrier frequency and code phase obtained by the acquisition to complete finer carrier and code synchronization. The focus of current acquisition research is to discuss the influence of spoofing power conditions; tracking mainly studies the process of spoofing attack, that is, the guidance law of spoofing signal to the receiver tracking loop under the condition of critical power.

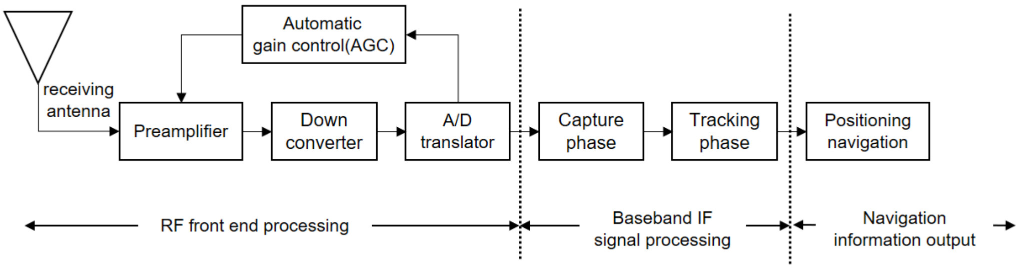


Figure 5. Typical GNSS receiver workflow.

Wuxing Su gave the expression for acquisition probability of a GNSS receiver in [34]. It is pointed out that forward spoofing must be suppressed first. Through analysis of the acquisition probability model, it is considered that when the spoofing signal and the normal signal exist at the same time, the interference signal only needs to be 7–10 dB larger than the normal signal to have a good acquisition and interference effect.

Yi Gao et al. gives the expression of two branch outputs of a C/A code receiver [35]. According to the output expressions of the acquisition and the tracking code and carrier loop, the influence of spoofing interference on the acquisition and tracking link of the receiver is discussed. It focuses on the spoofing effect corresponding to different phases of spoofing interference.

Jianyong Zhai et al. pointed out that in the signal acquisition link, if the correlation peak between the spoofing signal and the real signal exceeds 1.5 chips, the correlation function will have multi-peak characteristics [36]. In the case of stable tracking of the receiver, the critical interference signal ratio power condition of spoofing interference damaging the tracking state of the receiver is 24 dB.

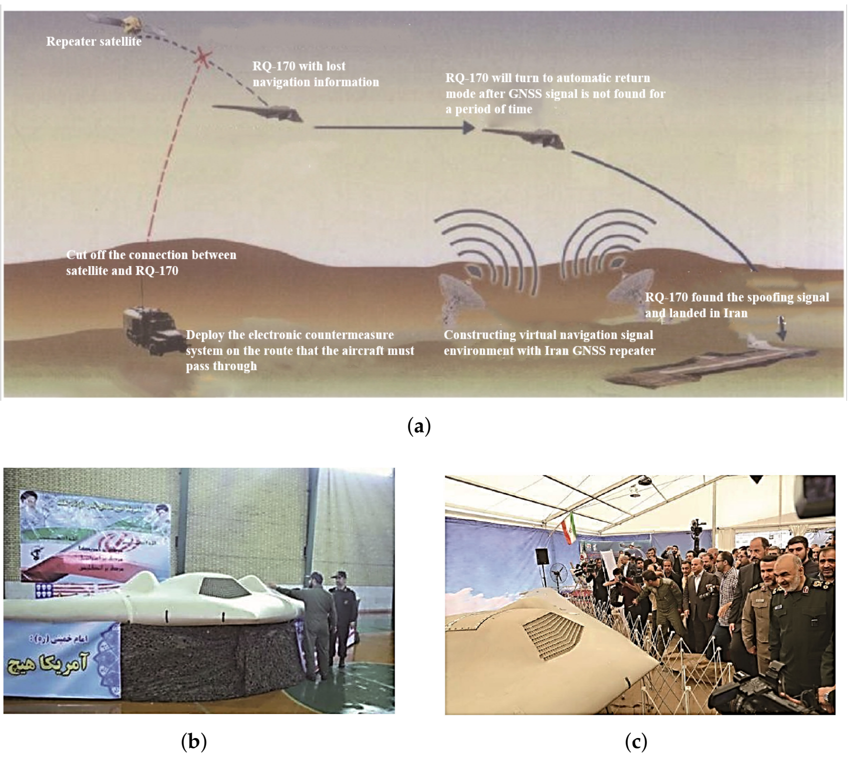
Zhicheng Lv et al. proposed a self-synchronous spoofing jamming signal generation method through the tracking loop of the traction target receiver [37]. This method can successfully cheat a typical GNSS receiver within 50 min when the spoofing signal power is 4dB higher than that of the real signal. Further, it can complete spoofing without suppression, which improves the concealment of spoofing.

This shows that the conditions required for successful spoofing are different in different working stages of the receiver. In the stable tracking state of the navigation receiver, the power condition of successful spoofing is higher than that of the acquisition state [11]. Of course, in order to realize covert spoofing of the receiver, the implementation method and effect of spoofing need to be further studied when the interference power conditions are close.

3.3. Typical Events Related to Satellite Navigation Spoofing Attacks

On 4 December 2011, Iran announced the capture of a U.S. stealth unmanned reconnaissance aircraft RQ-170 [38]. A participating Iranian engineer said they took advantage of the weakness of the UAV navigation system. First, through interference, they shielded the communication link of the UAV, cut off its connection with the ground command and control center, and cut off the data connection with the GNSS satellite, forcing the UAV to enter automatic driving state. Then, they sent navigation spoofing signals and reconstructed the coordinates of the GNSS [39]. By such means, they induced the drone to land in the Tabas desert area of Iran, 140 km away from the U.S. military base, but the drone mistakenly thought it was landing at the U.S. military base designated by the U.S.

military. Figure 6a shows the simulation process of Iran capturing the RQ-170; Figure 6b,c are the news report pictures of the U.S. drone captured by Iran [9].


Repeater satellite
RQ-170 with lost navigation information
RQ-170 will turn to automatic return mode after GNSS signal is not found for a period of time
Cut off the connection between satellite and RQ-170
RQ-170 found the spoofing signal and landed in Iran
Deploy the electronic countermeasure system on the route that the aircraft must pass through
Constructing virtual navigation signal environment with Iran GNSS repeater
امام خمینی (ره):
آمریکا هیچ

(**a**)

(**b**) (**c**)

Figure 6. On 4 December 2011, Iran announced that it had captured a U.S. RQ-170 drone: (**a**) Simulation of Iran capturing RQ-170; (**b**,**c**) The pictures taken from the news report of American drones captured by Iran. (https://www.guancha.cn/Project/2011_12_20_63306.shtml accessed on 16 June 2022).

Although the U.S. has repeatedly denied it, Figure 6 shows that the UAV is intact. Even Western military experts and relevant scholars studying GNSS believe that this is true. Robert Densmore, a former U.S. Navy electronic warfare expert, also believes that even modern combat-level GNSS is very easy to manipulate [16]. Of course, it is possible to recalibrate the GNSS on the UAV and change its flight route. This navigation spoofing application is considered the most successful [40]. Coincidentally, in December 2012, Iran once again captured a U.S. military UAV called a "ScanEagle" in the Persian Gulf [41].

In 2012, the Humphreys team [38] conducted a navigation spoofing test on the UAV at the White Sands Missile Range in the U.S., which was a complete success [42,43]. The test first interferes with the navigation receiver of the UAV and then transmits the navigation spoofing signal to guide the UAV. In 2013, at the invitation of Captain Schofield, the Humphreys team tested navigation spoofing of the White Rose yacht [43]. First, yachts rely on GNSS for safe navigation. In the process of navigation, the false analog signal is used to cover the satellite navigation signal to carry out a GNSS spoofing attack on the yacht. By adjusting the coordinates, Humphreys made the crew think that the wind changed the course. When the crew reset the course, they unknowingly drove onto the deviation route. During the journey from Monaco to Rhode Island, Greece, they successfully used the spoofing signal to replace the real signal received by the receiver and offset the yacht by 3° to the left.

On 12 January 2016, two U.S. patrol boats carrying 10 soldiers deviated from their course on the way from Kuwait to Bahrain for training, entered Iranian waters and were detained by Iran [44]. It seems that no U.S. official can reasonably explain the reason for the deviation from the course, but simply responds to the well-trained crew becoming "lost". The incident inevitably makes people speculate that Iran may have performed a GNSS spoofing attack on the U.S. patrol boat to induce the ship to deviate from its course and enter Iranian waters. In November 2018, Iran once again captured a large U.S. military MQ-9 UAV and released a video of the captured MQ-9 UAV [45].

Iran captured U.S. UAVs one after another. The test of U.S. UAVs and yachts being attacked by spoofing also shows that satellite navigation has great vulnerability and is vulnerable to jamming and spoofing. Compared with the suppression through jamming that makes satellite navigation unavailable, spoofing is very hidden [46]. It makes users use false information without being aware of it, which is more harmful. At present, in addition to the use of satellite navigation for mobile carriers in the air, water and land, some or all of the key systems such as communication, securities trading, financial systems and smart grids also use satellite navigation for accurate timing [47]. It is conceivable that targeted satellite navigation spoofing can lead to communication interruption, financial chaos, power paralysis and even more serious situations. Satellite navigation spoofing attackers can even manipulate each other's equipment, make aircraft or ships collide, make each other's weapons attack each other and so on [48]. If signal spoofing can be reliably detected, navigation spoofing can be further weakened or eliminated. Therefore, the research of satellite navigation spoofing detection is of great significance for satellite navigation to provide services safely and reliably.

We classify and elaborate spoofing technologies according to different classification standards such as spoofing signal and spoofing strategy.

4. Classification and Research Progress of Spoofing Technology

4.1. Traditional Classification of Spoofing Types Based on Signal-Generation Mode

It is a typical classification method to classify the types of spoofing according to the generation mode of the spoofing signal [49,50]. This is generally divided into two categories: production spoofing and forwarding spoofing.

- Production spoofing
  Production spoofing usually refers to transmitting the signal generated by the signal generation equipment itself directly to the USE receiver so that the target USE produces the wrong position solution to achieve the purpose of cheating the USE by the attacker [51]. Its advantage is that the navigation signal and transmission time have their own flexible decision, which can lag or advance the transmission time of the signal and can also give wrong location information in the navigation message. In 2003, Professor Warner built a navigation spoofing device using a GNSS signal simulator [52]. This was the first successful attempt of this technology. The disadvantage is that it is necessary to understand the structural characteristics of signals and navigation messages, and it is difficult to act on special signals such as military navigation signals. The universality is not strong.
- Forwarding spoofing
  As its name implies, forwarding spoofing collects the real satellite signals then enhances them and delays forwarding so that the target receiver tracks the deception signal and gets the wrong navigation and positioning result [53]. Compared with production spoofing, this type does not need to master the structure and setup of the signal in advance. Further, the essence of forwarding spoofing is to forward the real signal, which has strong consistency with the real signal, so it has good spoofing effect on GNSS civil code and military code receivers. Ledvina et al. described the basic structure of this spoofing type [54]. Moreover, experts and scholars speculate that Iran captured U.S. drones two times using this deception [55]. However, at the same time, because its implementation is based on forwarding of the real phase signal, the delay processing of the signal can only be greater than the delay of the real signal. So the generation of the deception signal is less flexible and more restrictive. This also determines that it is not easy to achieve more complex deception purposes in the deception mode, and the enhancement processing before transmitting the deception signal also amplifies the noise [5].

- Gradual self-synchronization spoofing
  Under this classification standard, in addition to the above two traditional types, there has been a gradual self-synchronization spoofing developed in recent years that deceives the receiver tracking loop [56,57] and is classified as an advanced type of spoofing in the relevant literature [58]. After receiving the real signal, the spoofer carries out range delay and Doppler modulation according to the dynamic performance of the target receiver so as to control the satellite delay when the target is not aware [12]. This method can realize the gradual guidance deception of booking location or path [59]. It is a new concealed and efficient deception method. In 2008, Todd Humphreys of the University of Texas in the United States increased the spoofing software module and transmission hardware module on the basis of a GNSS software receiver [15]. They designed and manufactured a spoofing source and demonstrated the feasibility of spoofing. Moreover, that was the first true GNSS gradual spoofing source. The key to the realization of gradual self-synchronization spoofing technology is how to effectively invade the target receiver to realize covert synchronization spoofing. For civil and military receivers, the technical implementation difficulty is different [60]. For the civil receiver, due to disclosure of the civil pseudo-random code system, the pseudo-random code periodic signal can be repeatedly generated locally. When the spoofing signal has Doppler offset, it can move to the same code phase of the real signal within a period of time, so as to realize spoofing. For the military receiver, because the military pseudo-random code is unknown, it is necessary to use an antenna with strong directionality to isolate different satellite signals and spoof by forwarding indirect control [61]. Moreover, it is difficult to predict the general position and motion trend of the target in advance to obtain the spoofing phase conditions [62,63]. Gradual self-synchronization spoofing technology will be the research focus of GNSS spoofing in the future.

4.2. Classification of Spoofing Types Based on Spoofing Implementation Stage

Another attack classification method is based on the receiving state of the GNSS signal by the receiver. The receiving of GNSS signals by the receiver is mainly divided into two stages: capture signal and tracking signal. The attacker's spoofing attack behavior can be expanded according to the characteristics of the receiver in different phases of receiving signals.

- Capture-phase spoofing
  In the capture phase, as the receiver has not locked the signal, it needs to implement three-bit searches in a large range. The receiver needs to traverse 1023 code phases for each satellite signal (taking GPS C/A code as an example) to search for a wide range and carrier frequency [64]. At this time, the deception signal power only needs to be slightly stronger than that of the real signal to successfully realize the deception attack, that is, to let the target receiver lock the deception signal (as shown in Figure 7). Because it does not need strong power and does not need to consider the synchronization of the phase and carrier frequency between the deception signal and the real signal number at the beginning, the implementation of a deception attack is easier [65]. For a target receiver that has normally tracked the real signal, the target receiver can lose lock and recapture by suppressing interference to realize a deception attack.
- Tracking-phase spoofing
  When the receiver finishes locking the signal and enters the tracking stage, the receiver will no longer carry out fuzzy search over a large range as in the capture stage [66]. If the carrier frequency and code phase of the spoofing signal are not aligned with the real signal, even a strong spoofing signal cannot easily affect the normal tracking of the receiver, so it is difficult to achieve the goal of spoofing. At this time, the synchronization of code phase and carrier frequency must be considered [62]. The feasible method is to realize the traction of the tracking loop of the target receiver

by sliding-step self-synchronization; the principle is shown in Figure 8. It is worth mentioning that this can also be called the gradual self-synchronization spoofing method, which was mentioned in Section 3.

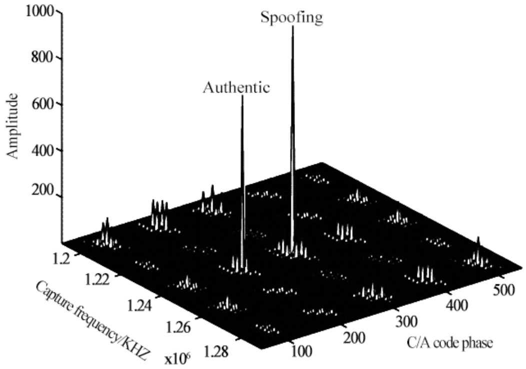


Figure 7. Spoofing attack in capture stage.

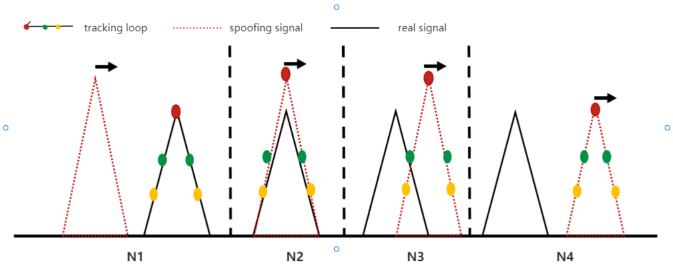


Figure 8. Schematic diagram of sliding self-synchronization mode of spoofing attack in tracking stage. N1: Align the phase of the spoofing signal number with the real signal; N2: Carrier ring of control receiver; N3: Introduce code phase change to spoofing signal; N4: Properly reduce the power of spoofing signal and complete the tracking loop control of receiver.

4.3. New Classification of Spoofing Types Based on Spoofing Strategies

With the development of anti-spoofing technology, spoofing attacks are no longer carried out in a single way; rather, they have become gradually diversified and complex [47]. This paper proposes a new classification method by analyzing the spoofing strategies taken by attackers to achieve their goals. The new classification method puts forward three new classification indexes.

- Self-consistent spoofing

  Self-consistent spoofing is generally used to cheat the traditional RAIM strategy of considering pseudo range residuals [67]. This method provides the desired position/timing for the potentially deceived receiver by synthesizing the false code phase and maintaining a small pseudo-range residual. In this method, the calculation required in the phase stage of synthesizing error code is very simple. The change of the false beat carrier phase is usually designed to be consistent with the phase of the false deception code [68]. Otherwise, the potentially deceived receiver may issue a warning due to unusual C/A differences or may lose the lock on the spoofing signal.

  The main difficulty of self-consistent spoofing is how to induce the potentially deceived receiver to lock the false signal it provides. There are two main ways to achieve this goal.

  The first is to interfere with the victims, destroy their original normal signal acquisition and induce them to try to obtain a new signal. If the deception signal power is significantly stronger than the real signal power, the receiver will most likely lock onto the deception signal during signal re-acquisition. Another method is to send false signals from low power to make them code match and Doppler match with the real signal at the position of the victim receiver antenna [69]. The power of deception starts low and then increases until it is sufficient to capture the tracking loop. Finally, the deceiver completes the deception of the coding phase and carrier phase to the deceived receiver in a self-consistent way.

- Signal estimation and replay spoofing
  The deception method described in self-consistent spoofing must recreate the spread spectrum code $C_i(t)$ to be transmitted and the data bit stream $C_i(t)$ to be transmitted. If they are completely predictable, they are easy to synthesize [68]. However, the enhanced civil GNSS signal will adopt orthogonal modulation and protect the unpredictable part of the short segment in the spread spectrum code $C_i(t)$.
  In this case, one of the choices of the deceiver is signal interference. The signal jammer records the real GNSS signal as in a conventional receiver and replays the signal through a transmitter with sufficient gain to drown the real signal on the antenna of the victim receiver [70]. The deceiver may deceive any GNSS signal, even encrypted military signals [71].
  If the unpredictable part of the signal is only in the low-rate $C_i(t)$ bit, it is possible to complete deception without interference. Instead, spoofers can use a secure code estimation and replay (SCER) attack: spoofers estimate unpredictable $C_i(t)$ bits and broadcast them immediately after obtaining reliable estimates. Before broadcasting them, it can broadcast random guesses of these bits or its own best estimates.
- Advanced-form spoofing
  Nowadays, with the continuous advancement of the research works of various spoofing defense technologies, the means of spoofing are also improving daily.
  An advanced technique is called zeroing [72]. The spoofer sends two signals for each spoofing signal.
  One is the spoofing signal, which works in conjunction with all other spoofing signals to cause incorrect location/timing positioning. The other is the negative value of the real signal, which is used to cancel the real signal at the receiver. The zeroing attack will delete all traces of the real signal. However, the principle of many current defense measures is to look for signs that two signals from the same satellite are received. They may look for different signals with sufficient spread between their coding phases or carrier Doppler shifts. Alternatively, they may look for interfering signals with similar code phase and carrier Doppler shift. In either case, clearing will eliminate all signs of duplicate signals, and defense measures relying on these signs will not be able to detect such attacks. The other is used to combat advanced spoofing with multiple-antenna victim receivers [73]. This method generally uses multiple independent spoofing transmitting antennas and matches each antenna to the corresponding receiver antenna. Moreover, the deceiver must be close enough to the victim, and the gain pattern of each antenna must be obtained and reduced sufficiently so that each victim antenna receives only the signal from the deceiver antenna [62]. This technology will enable the deceiver to control the difference between the beat carrier phase of each spoofing signal received at different antennas of the victim receiver in the time axis.
  These and other high-level forms of spoofing usually do not change the location or time of the victim too quickly. Otherwise, the victim can identify the attack through physical properties. For example, an inertial measurement unit (IMU) can be used as a physical anti-spoofing detection, which further limits the possible growth rate of deception navigation [74]. If the growth rate is too high to be suspected, the conventional IMU drift level cannot be used to explain this anomaly. The same is true of the increase in the clock offset of the victim receiver.

4.4. Related Literature Summary

In this subsection, we classify and summarize the spoofing technologies proposed in the relevant literature over the last decade according to the different classification standards mentioned in this chapter. We present the classification results in the form of tables, as shown in Table 2. As can be seen from the timeline in Table 2, the technology of spoofing has become more and more complex.

Table 2. Classification of GNSS spoofing technology.

		Based on Signal Generation Mode			Based on Spoofing Implementation Stage		Based on Spoofing Strategies		
Literature	**Year**	**Produce Spoofing**	**Forward Spoofing**	**Gradual Self-Synchronization Spoofing**	**Capture Phase Spoofing**	**Tracking Phase Spoofing**	**Self-Consistent Spoofing**	**Signal Estimation and Replay Spoofing**	**Advanced-form Spoofing**
Carroll [52]	2003	✓			✓				
Ning, Z. [54]	2010		✓			✓		✓	
Yi, G. [35]	2013			✓	✓			✓	
Yangjun, G. [75]	2015		✓		✓				✓
Yanfeng, H. [3]	2015			✓	✓				✓
Hyoungmin, So [76]	2016	✓			✓		✓		
Bian, S.F. [6]	2017		✓						
Mosavi, M.R. [44]	2017	✓				✓	✓		
Khan, A.M. [77]	2017	✓				✓			
Meng, Z. [78]	2018	✓				✓			
Liu [79]	2018	✓					✓		
Ledvina, B.M. [80]	2018	✓							
He, T. [33]	2019		✓		✓				✓
Baziar, A. [81]	2019	✓			✓				
Schmidt, E. [60]	2019			✓	✓			✓	
Guo, Y. [82]	2019			✓		✓			✓
Gao, Y. [83]	2019			✓		✓		✓	✓
Rothmaier, F. [84]	2021		✓					✓	
Jetto, J. [85]	2021			✓					✓

Remark: All the technologies mentioned in the table have successfully implemented spoofing attacks on GNSS-dependent devices. Through analysis and investigation, the technologies in these research documents are classified according to the different classification standards mentioned in this paper. Refer to the text for specific technical features.

5. Overview of Anti-Spoofing Technology

Spoofing defense must first detect the attack and then recover the verified real location/timing. At present, most anti-spoofing detection focuses on detecting attacks.

In 1995, Key et al. [7] analyzed the details of spoofing and anti-spoofing technology in an internal memorandum of the MITRE company and gave the following possible satellite navigation spoofing detection technology methods:

1. Signal amplitude detection;
2. Signal arrival angle detection;
3. Signal arrival time detection;
4. Consistency verification with other navigation equipment;
5. Signal encryption authentication;
6. Signal polarization direction detection;
7. Vector tracking loops detection.

Since then, some other scholars have summarized and divided the spoofing detection technology and methods according to their own opinions [5,6,60,72,86,87]. However, they are not much different. Moreover, all current technologies are becoming increasingly sophisticated and are indistinguishable in terms of effectiveness. In real confrontation situations, whether on the side of spoofing or on the side of defense, technology is only a means to an end, and it is the strategy of achieving one's own end that is of greater concern today.

This section mainly introduces the defense strategies for detecting attacks. In our opinion, all receiver-based spoofing detection strategies rely on one or both of the following two methods.

One method is to detect the difference between the spoofing signal and the real signal. These differences can be detected by the receiver of the potential victim. Although the civil GNSS signal formula is disclosed, there are usually significant synthetic signal differences unless there are complex and expensive tools being used.

Another method is to find the interaction between real signals and spoofing signals. Except for the following two cases, interaction is inevitable for the spoofer. One is invalid attack. Another situation is a serious and overwhelming attack. However, a strong attack is obviously different from the expected power of the real signal.

Under such cognition, this paper reclassifies the existing anti-spoofing technologies as show in Table 3.

Table 3. Defense strategies of anti-spoofing technology under reclassification.

Types	Difference between Spoofing Signal and Real Signal	Interaction between Real Signal and Spoofing Signal
A: Anti-spoofing technology based on signal processing	✓	
B: Anti-spoofing technology based on encryption	✓	✓
C: Anti-spoofing technology based on drift	✓	
D: Anti-spoofing technology based on signal/geographical location	✓	
E: Complementary strategy of multiple anti-spoofing technologies	✓	✓

5.1. Anti-Spoofing Technology Based on Signal Processing

This kind of technology looks for distortion or interference during signal spoofing and detects unreasonable jumps in carrier amplitude, coding phase and carrier phase, especially at the beginning of the attack [88]. One approach is to use received power monitoring (RPM). This views the total received power in absolute proportion. This requires viewing all received carrier amplitude values and automatic gain control (AGC) set points at the RF front-end of the receiver. Since the spoofer needs a substantial power advantage, a sudden power jump may indicate an attack, especially when the increase is more than 1 or 2 dB [89,90]. Such methods are more suitable for strong and short-lived scenarios because such distortion occurs only during the initial drag spoofing [13].

Another approach is detection technology based on signal processing, which can work long after the initial drag deception [21,91]. This technology constantly tries to regain all its tracking signals. It performs a robust search for each signal over the entire range of possible code phases and carrier Doppler shifts [21]. However, due to brute force acquisition and search, it brings a heavy signal processing burden to the receiver.

5.2. Anti-Spoofing Technology Based on Encryption

Such technologies use encryption to create unpredictable parts of the transmission signal that make it difficult for the deceiver to make the above estimation and replay the deception. The strongest defense measure is to encrypt the whole extension code $C_i(t)$ with a symmetric key.

One method is to use symmetric encryption [12]. A GNSS signal encrypted with a symmetric key can be used to detect spoofing in a civil GNSS receiver without accessing the private key. It is not necessary to distribute the key to the civil receiver, but it can use the known relationship between the open civil extension code and the encrypted military code. In GNSS, they are quadrature modulated on the same carrier [92,93]. Under this method, the receiver uses its civil code tracking system to record the noisy baseband version of encryption coding. This is done on a potential victim receiver and another receiver that can prevent spoofing. The two noisy versions of the encrypted code are then interacted to find the correlation peak that will exist if the signal in the potential victim is real. If the correlation peak is very high, it indicates that the signal is true; otherwise, an alarm will be issued [14]. However, this needs a secure receiver network to generate a noisy "real" version of the encrypted code. It also requires a secure communication network to bring real and unverified versions of the encrypted code to a common signal processing unit that can check the correlation. The purpose of this is to check the authenticity of the signal [94].

Another method is to use delayed symmetric key encryption. In the spreading code, the short segment of the symmetrically encrypted spread spectrum security code (SSSC) is interleaved with the long segment of the predictable spreading code. The receiver uses the known part to track the signal and records the unknown part. Shortly after the unpredictable SSSC is broadcast, bitstream data containing the key arrives, which can be used to generate the SSSC. The key is digitally signed, so it can be reliably traced back to the relevant GNSS control segment [21,91]. After verification, the key is used to synthesize the unknown spreading code, and the receiver associates the code with its recorded signal part to verify the authenticity of the signal. However, the technology using this method will involve a large number of detection delays when waiting for a complete digital signature, which may take a few seconds to a few minutes.

The third method is asymmetric private/public key navigation message authentication (NMA). A subset of the broadcast data stream $C_i(t)$ contains an unpredictable digital signature generated using the private key of the control segment. This signature signs the rest of the data in $C_i(t)$ [95]. The receiver knows the position of these bits in the demodulated data stream. It collects all the numbers needed to check the signature and verifies it with a known public key. The implementation of a delayed symmetric key SSSC method and asymmetric private key/public key NMA method are needed to modify the satellite signal. This is difficult or impossible for existing GNSS satellites and expensive for future satellites.

5.3. Anti-Spoofing Technology Based on Drift

Drift-based anti-spoofing technologies aim to find abnormal changes in receiver position or clock. If spoofing causes the receiver clock error to change too fast, the victim receiver can detect that the clock drift rate is greater than a reasonable value of its oscillator category [96,97]. IMU or other motion sensors can impose similar constraints on the reasonable drift rate of the position [98]. Similarly, the rolling constraint of the vehicle and its known maximum values of speed, acceleration and turn rate can be used to check whether there is excessive drift [99]. As with clock drift, if an untrue motion track is detected, the receiver will issue a deception alarm. However, the deceiver can avoid being detected by the drift detection method by slowly establishing the wrong clock offset and wrong position.

5.4. Anti-Spoofing Technology Based on Signal/Geographical Location

Signal location techniques monitor the direction of arrival of the signal by considering the received beat carrier phase [84,100]. As shown in Figure 9, the receiver can use interferometry by using three or more different antennas to sense $\Delta d(t)$ offsets or by using the direction of arrival vector as measured by a single antenna's $\Delta d(t)$ motion curve.

A well-designed receiver can usually ψ_i measure to an accuracy of about 1/40 cycle. In this way, the receiver can only use a short baseline $\Delta d(t) = 0.1$ m to measure ρ to an accuracy of about 3° [101]. Under normal circumstances, the ρ_i direction vector is distributed around the sky. However, a simple low-cost deceiver will broadcast all his signals from the same direction [11,102]. A typical geometry-based spoofing detection system tests that the data received on multiple antennas' ψ_i phase is the same as the real signal expected diversity of ρ_i direction or if it is more consistent with single transmitter deception from the same direction [28].

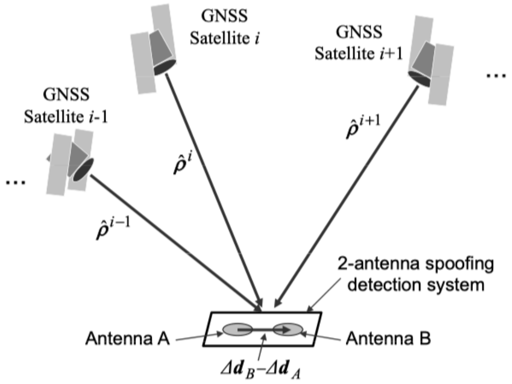


Figure 9. Schematic diagram of interferometry model.

5.5. Complementary Strategy of Multiple Anti-Spoofing Technologies

At present, in order to avoid the likelihood of the target detecting the attack to the greatest extent, spoofers usually use a complex attack method combining multiple spoofing strategies rather than a single method [1]. Based on this situation, it is a relevent yet difficult point for researchers to develop more effective detection methods that can adapt to complex spoofing scenes.

For example, one of the combination strategies is that the spoofer can choose to use a higher carrier amplitude to avoid the obvious distortion of complex correlation function in the process of drag off. If the defense object checks the complex correlation at many stages when implementing RPM, it can detect the beginning of the attack, regardless of how much power the spoofer uses [103]. If the clock offset drift rate and position drift rate are also monitored, the spoofer will be forced to perform a slow drag-off operation so that the receiver has more time to detect the distortion of the complex correlation function or the high received power level.

Another combination strategy is to use the unpredictable data bits of NMA to monitor the distortion of those bits, plus IMU and clock drift monitoring [104]. IMU and clock drift monitoring will force spoofer to launch attacks slowly. This restriction will prevent the formation of dangerous position or timing errors in the latency of NMA-based spoofing detection. If the spoofer implements an SCER attack to estimate and replay unpredictable NMA bits, the victim will be able to detect the initial uncertainty of these bits [105,106]. Because clock-drift monitoring will limit the initial ability of the spoofer to use the delay, this will allow a reliable estimation of the bits before starting the broadcast [107].

5.6. Anti-Spoofing Technology Comparison and Literature Summary

In 2012, Jafarnia-Jahromi et al. summarized and analyzed the main spoofing detection methods and the performance and characteristics of each method at that time [15]. On this basis, combined with the technical classification proposed in this paper and the research results of scholars at home and abroad in recent years, we give the comparison of main GNSS spoofing detection methods in the last decade, as shown in Table 4. In the literature research, we found that with the gradual complexity of spoofing scenes, the defense means of combined strategy will be the future direction of anti-spoofing technology.

Table 4. Comparison and literature summary of anti-spoofing technology under reclassification.

Types: Anti-Spoofing Technology	Literature	Detection Method	Spoofing Signal Characteristics	Configuration Required	Implementation Difficulty	Detection Effect	Adaptability
A: Signal processing	[13,88–90]	Signal power monitoring; vector tracking loops	Higher signal amplitude	Signal power monitoring	low	middle	high
	[14,94]	C/N monitoring	Higher C/N	C/N monitoring	low	middle	middle
	[21,91]	Power comparison of L1 and L2	Spoofing source without L2 signal	L2 signal acceptance	middle	low	low
B: Encryption	[12,74,92,93,95]	Message encryption	Unauthorized	Authentication means	high	high	high
	[39,47,108]	Spread spectrum code encryption	Unauthorized	Authentication means	high	high	high
C: Drift	[1,20,109]	Time-of-arrival identification	Forwarded spoofing has additional delay	Time-of-arrival analysis	middle	middle	low
	[40,96–99]	Signal quality monitoring	Distortion of correlation peak of real signal	Multi-correlator	middle	middle	low
	[110–112]	Correlator output distribution	Change of correlator output distribution caused by spoofing	Correlator output distribution analysis capability	low	middle	middle
	[113,114]	GNSS clock difference consistency	Spoofing is inconsistent with the real clock difference	—-	low	middle	middle
	[30,48,115–117]	Consistency verification with other airborne equipment	Spoofing signal leads to inconsistent positioning solutions	Different navigation sensors	high	high	high
D: Signal/geographical location	[28,61,84,100–102]	Antenna array detection	The direction of multiple deception signals is consistent	Configure multiple antennas	high	high	high
	[11,118,119]	Pairwise correlation detection of synthetic aperture antenna array	The direction of multiple deception signals is consistent	Measure the correlation coefficient of output of different tracking channels	high	high	high
E: Complementary strategy	[1,41,103–107,120]	Adjusted according to the specific spoofing combination strategy	Dependent on the specific spoofing	—-	high	high	high

Remark: Refer to the text above for specific policy deployment and technical features.

6. Outlook

6.1. GNSS Spoofing Technology Outlook

With the wide application of GNSS technology, GNSS spoofing technology has also developed rapidly, and its threat is increasing. From the development trend, the following points deserve attention:

1. The difference between the spoofing signal generated or forwarded by the navigation spoofer and the real navigation signal is becoming smaller and smaller. Especially for the complex closed-loop spoofer, the spoofing strategy is more and more advanced. It can overcome most spoofing detection, gradually guide the target receiver and achieve complete control of the target receiver. The concealment of spoofing signals is becoming stronger and stronger.
2. With the development of electronic and software radio technology, the threshold of GNSS spoofing technology is getting lower and lower, and miniaturized, low-cost and portable satellite navigation spoofing and jamming equipment are becoming easier and easier to realize.
3. With the development of unmanned equipment and spoofing detection technology, it is more and more difficult for a single spoofing source to achieve its purpose. GNSS spoofing is developing from a single spoofing signal source to a relay or array of multiple spoofing signal sources.

6.2. GNSS Anti-Spoofing Technology Outlook

GNSS security has gradually become the focus of attention. If the GNSS is insecure, it will even become a tool used by the enemy and finally become a sharp weapon to hurt itself. For the application of GNSS, spoofing detection should be carried out first so that the GNSS information can be used safely and reliably. In general, anti-spoofing technology should pay attention to the following points:

1. Research spoofing signal recognition methods before signal acquisition. Before the receiver captures the signal, if the spoofing signal can be identified, the corresponding methods can be studied to eliminate the spoofing signal so that the receiver can directly capture the real satellite navigation signal.
2. The combination method of multiple spoofing detection technologies should be deeply studied. With the development of spoofing technology, spoofing detection is becoming more and more difficult. No matter how excellent spoofing detection technology is, it is difficult to detect all deceptions. At present, there is little research on combination methods. We should deeply study the combination methods of multiple spoofing detection technologies and deeply integrate different detection methods to improve the success rate of spoofing detection.
3. Establish standard data. GNSS spoofing is developing more and more rapidly, which requires scholars engaged in GNSS applications to study navigation spoofing detection from the perspective of application. Nian Xue et al. have built a set of datasets, but it is only applicable to the visual angle [121]. Therefore, a set of standard data test sets should be established for researchers to study GNSS spoofing detection technology.

7. Conclusions

The vulnerabilities of GNSS provide a market for GNSS spoofing technology, and its development is endless. Based on the introduction of typical satellite navigation spoofing attacks, this paper focuses on the classification of satellite navigation spoofing technology. This paper expounds the research progress and characteristics of spoofing from different classification angles. Accordingly, this paper analyzes the characteristics of the current anti-spoofing technology and compares anti-spoofing technology from the aspects of implementation difficulty, effect and adaptability. Finally, the GNSS spoofing and anti-spoofing technology are prospected. GNSS spoofing is very harmful, and the development and application of its related technologies deserve the attention of those engaged in navigation technology. Moreover, the authors have been committed to improving the defense and support capabilities of UAVs in the navigation denial environment, and there have been some research achievements before. Now, we are combining the idea of mimicking defense to realize the dynamic defense capability of UAV groups against unknown threats, and we are hoping to contribute to the field in this way.

Author Contributions: Conceptualization, L.M. and L.Y.; methodology, L.M.;formal analysis, L.M. and W.Y.; investigation, L.M. and L.Z.; writing—original draft preparation, L.M.; writing—review and editing, L.M. and W.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research is supported by the National Natural Science Foundation of China (grants no. U2003206, 61831007 and 61971154).

Conflicts of Interest: The authors declare no conflict of interest

References

1. Luo, Z.; Deng, Z. *Positioning Method without GNSS for Unmanned Systems Based on Fusion of IMU, TOA and AOA*; Springer: Singapore, 2022.
2. Zhang, W.X.; Hou, H.T.; Wang, W.P. Research on GNSS's security-protection. *Comput. Eng. Sci.* **2013**. Available online: https://xueshu.baidu.com/usercenter/paper/show?paperid=4617a6395298d048e5ea0ccbef99db4a (accessed on 11 August 2022).
3. Hu, Y.; Bian, S.; Cao, K.; Feng, G. Spoofing power control strategy for GNSS receive. *J. Chin. Inertial Technol.* **2015**, *23*, 5.
4. Bhowmick, J.; Singh, A.; Gupta, H.; Nallanthighal, R. A Novel Approach to Computationally Lighter GNSS-Denied UAV Navigation Using Monocular Camera. In Proceedings of the 2021 7th International Conference on Automation, Robotics and Applications (ICARA), Prague, Czech Republic, 4–6 February2021.
5. Broumandan, A.; Jafarnia-Jahromi, A.; Lachapelle, G. Spoofing detection, classification and cancelation (SDCC) receiver architecture for a moving GNSS receiver. *Spinger* **2015**,*19*, 475–487.
6. Bian, S.F.; Hu, Y.F.; Chen, C.; Li, Z.M.; Ji, B. Research on GNSS repeater spoofing technique for fake Position, fake Time and fake Velocity. In Proceedings of the 2017 IEEE International Conference on Advanced Intelligent Mechatronics (AIM), Munich, Germany, 3–7 July 2017.
7. Key, E. *Techniques to Counter GPS Spoofing. Internal Memorandum*; MITRE Corporation: Bedord, MA, USA; 1995.
8. Humphreys, T.E.; Ledvina, B.M.; Psiaki, M.L.; O'Hanlon, B.W.; Kintner, P.M. Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer. In Proceedings of the International Technical Meeting of the Satellite Division of the Institute of Navigation, Savannah, Georgia, 16–19 September 2008.
9. Jahan, F. Implementation of GNSS/GPS Navigation and its Attacks in UAVSim Testbed. Ph.D. Thesis, The University of Toledo, Toledo, OH, USA, 2015.
10. Vervischpicois, A.; Samama, N.; Taillandierloize, T. Influence of GNSS Spoofing on Drone in Automatic Flight Mode. In Proceedings of the ITSNT 2017: 4th International Symposium of Navigation and Timing, Toulouse, France, 14–17 November 2017; pp. 1–9..
11. Shi, R.; Xu, J.; Yan, J. Detection on Navigation Deception Signals Based on Direction Finding by Nulling Antenna and Angle Contrast. *Mod. Navig.* **2017**, *8*, 193–198.
12. Humphreys, T.E. Detection Strategy for Cryptographic GNSS Anti-Spoofing. *IEEE Trans. Aerosp. Electron. Syst.* **2013**, *49*, 1073–1090.
13. Wesson, K.D.; Evans, B.L.; Humphreys, T.E. A combined symmetric difference and power monitoring GNSS anti-spoofing technique. In Proceedings of the 2013 IEEE Global Conference on Signal and Information Processing (GlobalSIP), Austin, TX, USA, 3–5 December 2013.
14. Dehghanian, V.; Nielsen, J.; Lachapelle, G. GNSS spoofing detection based on receiver C/N0 estimates. In Proceedings of the International Technical Meeting of the Satellite Division of the Institute of Navigation, Nashville, TN, USA, 17–21 September 2012.
15. Jafarnia-Jahromi, A.; Broumandan, A.; Nielsen, J.; Lachapelle, G. GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. *Int. J. Navig. Obs.* **2012**, *2012*, 127072.1–127072.16.
16. Kaplan, E. *Understanding GPS: Principles and Applications[M]*, 2nd ed.; Artech House, Boston, 2006.
17. Pardhasaradhi, B.; Cenkeramaddi, L.R. GPS Spoofing Detection and Mitigation for Drones using Distributed Radar Tracking and Fusion. *IEEE Sens. J.* **2022**, *22*, 11122–11134.
18. Christophersen, H.B.; Pickell, R.W.; Neidhoefer, J.C.; Koller, A.A.; Kannan, S.K.; Johnson, E.N. A Compact Guidance, Navigation, and Control System for Unmanned Aerial Vehicles. *J. Aerosp. Comput. Inf. Commun.* **2006**, *3*, 187–213.
19. Sabatini, R.; Bartel, C.; Kaharkar, A.; Shaid, T.; Ramasamy, S. Navigation and Guidance System Architectures for Small Unmanned Aircraft Applications. *Waset Org.* **2014**, *8*, 733–752.
20. Qi, Z.; Li, H.; Qian, L. GPS spoofing attack on time synchronization in wireless networks and detection scheme design. In Proceedings of the MILCOM 2012—2012 IEEE Military Communications Conference, Orlando, FL, USA, 1 November 2012.
21. Mao, H.; Dewei, W.U.; Hu, L.U. Analysis of Band-limited Gaussian Noise Blanket Jamming Bandwidth Choosing to GPS Receiver. *J. Proj. Rockets Missiles Guid* **2015**. doi:10.15892/j.cnki.djzdxb.2015.01.030.

22. Florence, M.G.; Petovello, M.G.; Gerard, L. Combined acquisition and tracking methods for GPS L1 C/A and L1C signals. *Int. J. Navig. Obs.* **2010**, *2010*, 190465.
23. Zhang.; Li.; Schwieger.; Volker. Improving the Quality of Low-Cost GPS Receiver Data for Monitoring Using Spatial Correlations. *J. Appl. Geod.* **2016**, *10*, 119–129.
24. Srinivasan, S.; Bricka, S. *Methodology for Converting GPS Navigational Streams to the Travel-Diary Data Format*; University of Florida: Gainesville, FL, USA, 2009.
25. Namie, H.; Nishikawa, K.; Sasano, K.; Fan, C.; Yasuda, A. Development of Network-Based RTK-GPS Positioning System Using FKP Via a TV Broadcast in Japan. *IEEE Trans. Broadcast.* **2008**, *54*, 106–111.
26. Sun, M.T.; Feng, W.C.; Lai, T.H.; Yamada, K.; Fujimura, K. GPS-based message broadcast for adaptive inter-vehiclecommunications. In Proceedings of the Vehicular Technology Conference Fall 2000—IEEE VTS Fall VTC2000—52nd Vehicular Technology Conference (Cat. No.00CH37152), Boston, MA, USA, 24–28 September 2000.
27. Langley, R.B.; Jannasch, H.; Peeters, B.; Bisnath, S. The GPS Broadcast Orbits: An Accuracy Analysis. In Proceedings of the 33rd COSPAR Scientific Assembly, Warsaw, Poland, 16–23 July 2000.
28. Psiaki, M.L.; O'Hanlon, B.W.; Powell, S.P.; Bhatti, J.A.; Humphreys, T.E.; Schofield, A. GNSS lies, GNSS truth: Spoofing detection with two-antenna differential carrier phase. *GPS World* **2014**, *25*, 36–44.
29. Cuntz, M.; Konovaltsev, A.; Dreher, A.; Meurer, M. *Jamming and Spoofing in GPS/GNSS Based Applications and Services-Threats and Countermeasures*; Springer: Berlin/Heidelberg, Germany, 2012.
30. Khanafseh, S.; Roshan, N.; Langel, S.; Chan, F.C.; Pervan, B. GPS spoofing detection using RAIM with INS coupling. In Proceedings of the Position, Location and Navigation Symposium-Plans, IEEE/ION, Monterey, CA, USA, 5–8 May 2014.
31. Huang, L.; Gong, H.; Zhu, X.; Wang, F. Research of re-radiating spoofing technique to GNSS timing receiver. *J. Natl. Univ. Defense Technol.* **2013**, *35*, 93–96.
32. Engel, F.; Mumford, P.; Parkinson, K.; Rizos, C.; Heiser, G. An open GNSS receiver platform architecture. *J. Glob. Position. Syst.* **2004**, *3*, 63–69.
33. He, T. Improvernent of the method of GNSS retransmission deception interference mode. *Bull. Surv. Mapp.* **2019**, *25*, 71.
34. Wuxing Su, Shusheng Yan, Y.L. Efficiency Analysis of Repeater Deception Jamming GPS Repeater. *J. Air Force Radar Acad.* **2004**, *4*, 001.
35. Yi Gao, Yang Chen, G.L. Influence Analysis of Deceptive Jamming Signal on GPS Civil Receiver. In Proceedings of the The 4th China Satellite Navigation Academic Annual Conference, Wuhan, China, 15–17 May 2013.
36. Jianyong Zhai, Wei Wang, H.L. Analysis of receiver deception jamming threat and anti deception measures. In Proceedings of the 4th China Satellite Navigation Academic Annual Conference, Wuhan, China, 15–17 May 2013.
37. Zhicheng Lv, Feixue Wang, L.H. Research on spoofing for satellite navigation receiver. *J. Astronaut.* **2012**, *33*, 884–890.
38. A, D.P.S.; A, T.E.H.; B, A.A.F. Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks-ScienceDirect. *Int. J. Crit. Infrastruct. Prot.* **2012**, *5*, 146–153.
39. Xin, L.; Wang, Y.; Li, C.; Chen, J. Choice of sampling frequency for Gps signal simulator calibration receiver and influence on spread-spectrum ranging. In Proceedings of the IEEE International Conference on Electronic Measurement and Instruments, Harbin, China, 16–19 August 2013.
40. Psiaki, M.L.; Humphreys, T.E. GNSS spoofing and detection. *Proc. IEEE* **2016**, *104*, 1258–1270.
41. Tanil, C.; Khanafseh, S.; Pervan, B. *GNSS Spoofing Attack Detection using Aircraft Autopilot Response to Deceptive Trajectory*; Institute of Navigation: Manassas, VI, USA, 2015.
42. Humphreys, T.E. *Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing*; University of Texas at Austin: Austin, TX, USA, 2012.
43. Kerns, A.J.; Shepard, D.P.; Bhatti, J.A.; Humphreys, T.E. Unmanned Aircraft Capture and Control Via GPS Spoofing. *J. Field Robot.* **2014**, *31*, 617–636.
44. Mosavi, M.R.; Baziar, A.R.; Moazedi, M. De-noising and spoofing extraction from position solution using wavelet transform on stationary single-frequency GPS receiver in immediate detection condition. *J. Appl. Res. Technol.* **2017**, *15*, 402–411.
45. Available online: http://www.yidianzixun.com/article/0Khd4VYr (accessed on 18 November 2018).
46. Psiaki, M.; Humphreys, T. Civilian GNSS Spoofing, Detection, and Recovery. In *Position, navigation, and timing technologies in the 21st century: Integrated satellite navigation, sensor systems, and civil applications*; Wiley Online Library: Hoboken, NJ, USA, 2020.
47. Qiao, Z.; Assad, S.E.; Taralova, I. Design of secure cryptosystem based on chaotic components and AES S-Box. *AEU Int. J. Electron. Commun.* **2020**, *121*, 153205.
48. Kwon.; Shim. Performance Analysis of Direct GPS Spoofing Detection Method with AHRS/Accelerometer. *Sensors* **2020**, *20*, 954.
49. Wu, Z.; Zhang, Y.; Yang, Y.; Liang, C.; Liu, R. Spoofing and anti-spoofing technologies of global navigation satellite system: A survey. *IEEE Access* **2020**, *8*, 165444–165496.
50. Junzhi, L.; Wanqing, L.; Qixiang, F.; Beidian, L. Research progress of GNSS spoofing and spoofing detection technology. In Proceedings of the 2019 IEEE 19th International Conference on Communication Technology (ICCT), Xi'an, China, 16–19 October 2019; pp. 1360–1369.
51. Caparra, G.; Wullems, C.; Ioannides, R.T. An Autonomous GNSS Anti-Spoofing Technique. In Proceedings of the Satellite Navigation Technologies and European Workshop on Gnss Signals and Signal Processing, Noordwijk, Netherlands, 2017.
52. Carroll, J.V. Vulnerability Assessment of the U.S. Transportation Infrastructure that Relies on the Global Positioning System. *J. Navig.* **2003**, *56*, 185–193.

53. Cui, M.; Liu, R.H. Analysis of Countermeasures for GPS Signal Spoofing. *Comput. Secur.* **2010**.
54. Ledvina, B.M.; Bencze, W.J.; Galusha, B.; Miller, I. An In-Line Anti-Spoofing Device for Legacy Civil GPS Receivers. In Proceedings of the 2010 International Technical Meeting of the Institute of Navigation, Portland, Oregon, USA, 21–24 September 2010.
55. Ning, Z. Example analysis of GPS forwarding deceptive jamming applied to UAV. In *Missiles and Other Weapon Systems*; 2015; p. 3.
56. Humphreys, T.E.; Bhatti, J.A.; Shepard, D.P.; Wesson, K.D. The Texas Spoofing Test Battery: Toward a Standard for Evaluating GPS Signal Authentication Techniques. In *Phenomena in Ionized Gases, IEEE, VI International Conference, Volume III*; Nashville Convention Center: Nashville, TN, USA, 2012.
57. Humphreys, T.E.; Bhatti, J.A. The GPS Assimilator: A Method for Upgrading Existing GPS User Equipment to Improve Accuracy, Robustness, and Resistance to Spoofing. In Proceedings of International Technical Meeting of the Satellite Division of the Institute of Navigation, Portland, OR, USA, 21–24 September 2010.
58. Wesson, K.; Shepard, D.; Humphreys, T. Straight talk on anti-spoofing: Securing the future of PNT. *Gps World* **2012**, *23*, 32–34, 59–63.
59. Wesson, K.D.; Shepard, D.P.; Bhatti, J.A.; Humphreys, T.E. An Evaluation of the Vestigial Signal Defense for Civil GPS Anti-Spoofing. In Proceedings of International Technical Meeting of the Satellite Division of the Institute of Navigation, Portland, OR, USA, 20–23 September 2011.
60. Peng, C.; Li, H.; Wen, J.; Lu, M. *Research of Intermediate Spoofing Without Precise Target Information*; Springer: Singapore, 2019.
61. Schmidt, E.; Gatsis, N.; Akopian, D. A GPS spoofing detection and classification correlator-based technique using the LASSO. *IEEE Trans. Aerosp. Electron. Syst.* **2020**, *56*, 4224–4237.
62. Yolleck, S.M.; Walters, D.A. Method and System for Operating Multiple Web Pages with Anti-Spoofing Protection. United States Patent US 8,028,245, 7 September 2011.
63. Psiaki, M.L.; Powell, S.P.; O'Hanlon, B.W. GNSS spoofing detection using high-frequency antenna motion and carrier-phase data. In Proceedings of the 26th International Technical Meeting of the Satellite Division of the Institute of Navigation, Nashville, TN, USA, 16–20 September 2013.
64. Min, L.; Dempster, A.G.; Balaei, A.T.; Rizos, C.; Wang, F. Switchable Beam Steering/Null Steering Algorithm for CW Interference Mitigation in GPS C/A Code Receivers. *IEEE Trans. Aerosp. Electron. Syst.* **2011**, *47*, 1564–1579.
65. Zhang, B.; Yang, C. FFT Acquisition Algorithm for GPS C/A Code Using Frequency-domain Doppler Search. *Telecommun. Eng.* **2010**, *5*, 42–46. .
66. Pirsiavash, A.; Broumandan, A.; Lachapelle, G.; O'Keefe, K. Detection and Classification of GNSS Structural Interference Based on Monitoring the Quality of Signal at the Tracking Level. In Proceedings of the 6th ESA International Colloquium on Scientific and Fundamental Aspects of the Galileo, Valencia, Spain, 25–27 October 2017.
67. Martineau, A.; Macabiau, C.; Mabilleau, M. GNSS RAIM assumptions for vertically guided approaches. In Proceedings of the 22nd International Technical Meeting of the Satellite Division of the Institute of Navigation, Savannah, GA, USA, 22–25 September 2009.
68. Kirkko-Jaakkola, M.; Traugott, J.; Odijk, D.; Collin, J.; Holzapfel, F. A raim approach to GNSS outlier and cycle slip detection using L1 carrier phase time-differences. In Proceedings of the IEEE Workshop on Signal Processing Systems, Tampere, Finland, 7–9 October 2009.
69. Tran, H.T.; Presti, L.L. Demonstration of Multi-GNSS Advanced RAIM Algorithm using GPS and Galileo Signals. *Tech. Rep. Ieice Sane* **2013**, *113*, 191–196.
70. Wang, Q.; Hong, L.I.; Ming-Quan, L.U. Position Vector Analysis Method (PVAM) for Evaluating Performance of GNSS Replay Attacks. *Comput. Simul.* **2014**, DOI:10.1109/ChinaSIP.2013.6625403.
71. Maier, D.; Frankl, K.; Blum, R.; Eissfeller, B.; Pany, T. Preliminary Assessment on the Vulnerability of NMA-based Galileo Signals for a special class of Record and Replay Spoofing Attacks. In Proceedings of the 2018 IEEE/ION Position, Location and Navigation Symposium (PLANS), Monterey, CA, USA, 23–26 April 2018; pp. 63–71.
72. Liu, X.; Li, J.; Xu, T. Research on GNSS Anti-spoofing Interference Algorithm Based on Muti-receiver. In Proceedings of the 2019 IEEE International Conference on Signal, Information and Data Processing (ICSIDP), Chongqing, China, 11–13 December 2019.
73. YangGao.; HongLi.; MingquanLu.; ZhenmingFeng. Intermediate Spoofing Strategies and Countermeasures. *Tsinghua Sci. Technol.* **2013**, *18*, 599–605.
74. Shokhmzan, Z.; Mousavi, M. Defense Against Spoofing in GPS Receiver using Correlation and Least Mean Squares Method Based on Sign-Data Algorithm. *J. Electron. Cyber Def.* **2016**, *3*, 11–22.
75. Baziar, A.; Moazedi, M.; Mosavi, M.R. Analysis of single frequency GPS receiver under delay and combining spoofing algorithm. *Wirel. Pers. Commun.* **2015**, *83*, 1955–1970.
76. So, H. Implementation of GPS Spoofing Test Environment using Multiple GPS Simulators. *J. Position. Navig. Timing* **2016**, *5*, 165–172.
77. Meng, Z.; Hong, L.; Peng, L.; Lu, M. Modeling and Simulation of Receiver-Spoofer Attacking Process in Tracking Stage. In *China Satellite Navigation Conference*; Springer: Singapore, 2017.
78. Zeng, K.C.; Liu, S.; Shu, Y.; Wang, D.; Li, H.; Dou, Y.; Wang, G.; Yang, Y. All Your GPS Are Belong to Us: Towards Stealthy Manipulation of Road Navigation Systems. In Proceedings of the 27th USENIX Conference on Security Symposium, Baltimore, MD, USA, 15–17 August 2018; pp. 1527-1544.

79. Khan, A.M.; Iqbal, N.; Khan, M.F. Synthetic GNSS spoofing data generation using field recorded signals. *MethodsX* **2018**, *5*, 1272–1280. https://doi.org/10.1016/j.mex.2018.10.004.
80. Liu;, M.L.K.X. Design and Field Test of a GPS Spoofer for UAV Trajectory Manipulation. In Proceedings of the China Satellite Navigation Annual Conference, Harbin, China, 23–25 May 2018.
81. Yangjun, G.; Zhiwei, L.; Pengjin, Z.; Zhengyang, J. Design and Implementation of Portable GPS Generated Spoofing Device. In Proceedings of the China Satellite Navigation Annual Conference, Beijing, China, 22–25 May 2019.
82. Guo, Y.; Wu, M.; Tang, K.; Tie, J.; Li, X. Covert Spoofing Algorithm of UAV Based on GPS/INS-Integrated Navigation. *IEEE Trans. Veh. Technol.* **2019**, *68*, 6557–6564.
83. Gao, Y.; Lv, Z.; Zhang, L. Two-step Trajectory Spoofing Algorithm for Loosely Coupled GNSS/IMU and NIS Sequence Detection. *IEEE Access* **2019**, *7*, 96359–96371.
84. Rothmaier, F.; Chen, Y.H.; Lo, S.; Walter, T. GNSS Spoofing Mitigation in the Position Domain. In Proceedings of the 2021 International Technical Meeting of The Institute of Navigation, Online, 25–28 January, 2021.
85. Jetto, J.; Gandhiraj, R.; Sundaram, G.; Soman, K.P. Software Defined Radio-Based GPS Spoofing Attack Model on Road Navigation System. In *Soft Computing and Signal Processing*; Springer: Singapore, 2022.
86. Huang, L. Anti-spoofing Techniques for GNSS Receiver. *Geomat. Inf. Sci. Wuhan Univ.* **2011**, *36*, 1344–1347.
87. Xiao, L.; Ma, P.C.; Tang, X.M.; Sun, G.F. GNSS receiver anti-spoofing techniques: a review and future prospects. In *Electronics, Communications and Networks V, Springer*; 2016; pp. 59–68. Available online: https://link.springer.com/chapter/10.1007/978-981-10-0740-8_8 (accessed on 11 August 2022).
88. Dehghanian, V.; Nielsen, J.; Lachapelle, G. GNSS Spoofing Detection Based on Signal Power Measurements: Statistical Analysis. *Int. J. Navig. Obs.* **2012**, *2012*, 313527.1–313527.8.
89. Chu, F.; Li, H.; Wen, J.; Lu, M. Statistical Model and Performance Evaluation of a GNSS Spoofing Detection Method based on the Consistency of Doppler and Pseudorange Positioning Results. *J. Navig.* **2019**, *72*, 447–466.
90. Li, J.; Zhu, X.; Ouyang, M.; Shen, D.; Chen, Z.; Dai, Z. GNSS Spoofing Detection Technology Based on Doppler Frequency Shift Difference Correlation. *Meas. Sci. Technol.* **2022**, *33*, 095109.
91. Akos, D.M. Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC). *Navigation* **2012**, *59*, 281–290.
92. Wesson, K.D.; Rothlisberger, M.P.; Humphreys, T.E. A Proposed Navigation Message Authentication Implementation for Civil GPS Anti-Spoofing. In Proceedings of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation, Portland, OR, USA, 20–23 September 2011.
93. Humphreys, T. Practical Cryptographic Civil GPS Signal Authentication. *J. Inst. Navig.* **2012**, *59*, 177–193.
94. Jahromi, A.J.; Broumandan, A.; Nielsen, J.; Lachapelle, G. GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements. *Int. J. Satell. Commun. Netw.* **2012**, *30*, 181–191.
95. Lee, D.K.; Miralles, D.; Akos, D.; Konovaltsev, A.; Nedelkov, F. Detection of GNSS Spoofing using NMEA Messages. In Proceedings of the 2020 European Navigation Conference (ENC), Dresden, Germany, 23–24 November 2020.
96. Kalantari, A.; Larsson, E.G. Statistical test for GNSS spoofing attack detection by using multiple receivers on a rigid body. *EURASIP J. Adv. Signal Process.* **2020**, *2020*, 8.
97. Dobryakova, L. Antiterrorism-design and analysis of GNSS antispoofing algorithms. *Sci. J. Maritime Univ. Satell. Szczec. Zesz. Nauk. Akad. Morska Szczec.* **2012**, *30*, 93–101.
98. Miralles, D.; Bornot, A.; Rouquette, P.; Levigne, N.; Walter, T. Assessment of GPS Spoofing Detection via Radio Power and Signal Quality Monitoring for Aviation Safety Operations. *IEEE Intell. Transp. Syst. Mag.* **2020**, *12*, 136–146.
99. Kuusniemi, H.; Blanch, J.; Chen, Y.H.; Lo, S.; Enge, P. Feasibility of Fault Exclusion Related to Advanced RAIM for GNSS Spoofing Detection. In Proceedings of the 30th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2017), Portland, OR, USA, 25–29 September 2017.
100. Radin, D.S.; Swaszek, P.F.; Seals, K.C.; Hartnett, R.J. GNSS Spoof Detection Based on Pseudoranges from Multiple Receivers. In Proceedings of the International Technical Meeting of the Institute of Navigation, Dana Point, CA, USA, 26–28 January 2015.
101. Xiao, L.; Tang, X.; Li, B.; Sun, G. A GNSS anti-spoofing technique based on dual-receiver. *J. Natl. Univ. Def. Technol.* **2016**, DOI:10.11887/j.cn.201603008.
102. Zalewski, P. Simple GNSS Spoofing Detection in Two Antennas' or Multi Receiver Maritime Systems. *Eur. J. Navig.* **2014**, *12*, 19.
103. Xu, G.; Feng, S.; Amin, M.; Wang, C. DOA classification and CCPM-PC based GNSS spoofing detection technique. In Proceedings of the 2018 IEEE/ION Position, Location and Navigation Symposium (PLANS), Monterey, CA, USA, 23–26 April 2018.
104. Yang, L.; Fu, Q.; Liu, Z.; Li, S. GNSS Spoofing Detection Ability of a Loosely Coupled INS/GNSS Integrated Navigation System for two Integrity Monitoring Methods. In Proceedings of the 2017 International Technical Meeting of The Institute of Navigation, Monterey, CA, USA, 30 January 2017.
105. Jullian, O.; Otero, B.; Stojilovi, M.; Costa, J.J.; Verdu, J.; Pajuelo, M.A. Deep Learning Detection ofGPS Spoofing. In Proceedings of the International Conference on Machine Learning, Optimization, and Data Science, Grasmere, UK, 4–8 October 2021.
106. Zhang, L.; Sun, C.; Zhao, H.; Feng, W.; Liu, H. The Derivation and Evaluation of Algorithm of Anti-spoofing Attack on Loosely/Tightly Coupled GNSS/INS Integration System. In Proceedings of the China Satellite Navigation Conference (CSNC) 2020 Proceedings, Chengdu, Sichuan, China, 22–25 November 2020; Volume III.
107. Hu, K.; Huang, Y. A Composite Detection Method for Direct GPS Deception Attack. *IOP Conf. Ser.* **2020**, *790*, 012028

108. Nguyen, L.; Jang, W.M. *Self-Encoded Spread Spectrum Modulation for Robust Anti-Jamming Communication*; Nebraska Univ at Omaha Peter Kiewit Inst.: Omaha, NE, USA, 2009.
109. Gao, Y.; Zhiwei, L.; University, I.E. Impact Analysis of GPS Time Spoofing Based on TEXBAT Scenes. *J. Geomat. Sci. Technol.* **2019**, DOI:10.3969/j.issn.1673-6338.2019.02.004.
110. Chu, F.; Hong, L.; Lu, M. A GNSS Spoofing Detection Method Based on the Consistency of Measured and Calculated Carrier Dopplers. In Proceedings of the ION 2017 Pacific PNT Meeting, Honolulu, HI, USA, 1–4 May 2017.
111. Wei, X.; Aman, M.N.; Sikdar, B. Light-Weight GPS Spoofing Detection in Synchrophasors. In Proceedings of the 2020 IEEE International Conference on Power Electronics, Drives and Energy Systems (PEDES), Jaipur, India, 16–19 December 2020.
112. Wang, H.; Chang, Q.; Xu, Y. Deception Jamming Detection Based on Beam Scanning for Satellite Navigation Systems. *IEEE Commun. Lett.* **2021**, *25*, 2703–2707.
113. Shuai, H.; Yu, Z.; Meng, W.; Cheng, L. GPS anti-spoofing technology based on RELAX algorithm in smart grid. In Proceedings of the 2015 10th International Conference on Communications and Networking in China (ChinaCom), Shanghai, China, 15–17 August 2015.
114. Magiera, J.; Katulski, R. Accuracy of differential phase delay estimation for GPS spoofing detection. 2013 36th International Conference on Telecommunications and Signal Processing (TSP), Rome, Italy, 2–4 July 2013.
115. Oh, T.; Chung, M.J.; Myung, H. *Accurate Localization in Urban Environments Using Fault Detection of GPS and Multi-Sensor Fusion*; Springer International Publishing: Berlin/Heidelberg Germany, 2017.
116. Dasgupta, S.; Rahman, M.; Islam, M.; Chowdhury, M. A Sensor Fusion-based GNSS Spoofing Attack Detection Framework for Autonomous Vehicles. *arXiv* **2021**, arXiv:2108.08635.
117. Meng, L.; Ren, S.; Tang, G.; Yang, C.; Yang, W. UAV Sensor Spoofing Detection Algorithm Based on GPS and Optical Flow Fusion. In Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy, Nanjing, China, 10–12 January 2020; pp. 146–151. https://doi.org/10.1145/3377644.3377670.
118. Tanil, C. *Detecting GNSS Spoofing Attacks Using INS Coupling*; Illinois Institute of Technology: Chicago, IL, USA,2016.
119. Ceccato, M.; Formaggio, F.; Laurenti, N.; Tomasin, S. Generalized likelihood ratio test for GNSS spoofing detection in devices with IMU. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 3496–3509.
120. Bose, S.C. GPS Spoofing Detection by Neural Network Machine Learning. *IEEE Aerosp. Electron. Syst. Mag.* **2021**, *37*, 18–31.
121. Xue, N.; Niu, L.; Hong, X.; Li, Z.; Hoffaeller, L.; Pöpper, C. Deepsim: Gps spoofing detection on uavs using satellite imagery matching. In Proceedings of the ACSAC ’20: Annual Computer Security Applications Conference, Austin, TX, USA, 7–11 December 2020; pp. 304–319.