IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

Spoofing and Anti-spoofing Technologies of Global Navigation Satellite System: A Survey

Zhijun Wu, Yun Zhang, Yiming Yang, Cheng Liang and Rusen Liu
School of the Electronic Information and Automation, Civil Aviation University of China, Tianjin, 300300 China

Corresponding author: Zhijun Wu (e-mail: zjwu@cauc.edu.cn).

This work was supported in part by the Joint Foundation of National Natural Science Committee of China and Civil Aviation Administration of China under Grant U1933108, and in part by the Scientific Research Project of Tianjin Municipal Education Commission under Grant 2019KJ117.

ABSTRACT A large number of facts prove that Global Navigation Satellite System (GNSS) has certain security risks and is threatened by attacks. In particular, GNSS civilian signal receivers have some vulnerability in responding to spoofing attack and jamming attack, because the format and modulation of GNSS civilian signals are public. Based on the concerns of existing GNSS spoofing scenarios, this paper reviews the research on GNSS anti-spoofing technologies from two aspects. In this paper, the strategies of spoofing attacks discovered at this stage are classified in detail, the protection effect and scheme implementation complexity of various anti-spoofing techniques against spoofing attacks are analyzed from the perspective of signal-level and data-level. More specifically, we comprehensively analyze the ability for the combined anti-spoofing methods at the signal-level and the data-level to protect from combinations of different spoofing attack. Finally, the future development trend and potential research direction of GNSS anti-spoofing technology are summarized and predicted.

INDEX TERMS GNSS civilian signal**,** spoofing**,** Anti- spoofing**,** jamming attack**,** signal-level**,** data-level**,** attack**.**

I. INTRODUCTION

In recent years, global satellite navigation systems have been applied to all aspects of our lives. Real-time location, accurate time information and speed information are obtained through the navigation signals transmitted by artificial satellites [1][2]. These information are widely used in electric systems, finance systems, communication systems, transportation systems (as shown in Figure 1) and other fields to provide our lives for great convenience [3]-[5]. Once the information security of the satellite navigation system is destroyed, the receiver receiving the wrong satellite data would mislead the user to generate the wrong positioning information [6][7], which may have an impact on our daily life and even potentially dangerous [8][9]. In addition, the band resources are limited. As the construction of modern communication will cause the frequency band to become crowded and there will be mutual interference between them, this will also cause the positioning of the GNSS receiver to deviate [10]. Since most of the current civil satellite navigation systems are characterized by information transparency and signal openness [11]-[13], these systems are likely to suffer from information tampering and entity camouflage attacks.

After intercepting the real navigation signal sent by the satellite, the attacker deliberately tampers with the navigation information carried by the satellite signal to achieve the purpose of information tampering. Due to the lack of security protection measures such as authentication, the receiver cannot guarantee whether it has been subjected to tampering attacks. If the spoofed information is received as authentic navigation message, the spoofed information could lead receivers to incorrect positioning or timing [14].

Entity camouflage attacks are mainly aimed at the current BeiDou satellite navigation system. At present, most receiving user terminals of the current global satellite navigation system can only receive navigation message and cannot contact the GNSS control center. Most receivers of the BeiDou satellite navigation system have short message function that can be used to communicate with some ground facilities. However, the short message lacks effective information authentication means and is easily forged by the third parties [15]. This situation causes the receiver to receive an erroneous command that misleads normal operation.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

Considering the security of future civil satellite navigation technology, countries have introduced information authentication technology for their own navigation systems, such as the GPS system of the United States [1], the BeiDou navigation system of China [15], the Galileo system of the European Union [16] and so on. From the perspective of the receiver, how the receiver guarantees the integrity of the information from the information authentication center is also one of the issues to be considered. In other words, the receiver needs to be designed to meet the requirements for information authentication.

A. BACKGROUND OF THIS SURVEY

Since the satellite works far away from the earth, the signal received by the receiver is very weak and is easily affected by deliberate interference and accidental interference. The accuracy and integrity of satellite navigation signals cannot be guaranteed [17]. The Interface Control Document (ICD) of civil GNSS have detailed descriptions and accounts of relevant parameters such as carrier frequency, modulation mode, navigation message, etc. for civil satellite navigation signals [18][19]. The spoofer can easily forge the real satellite navigation signal through technical means and then send spoofing signals to the receiver through a certain spoofing strategy. This kind of spoofing has a strong disguise, making it difficult for the target receiver to find out that it has been deceived in time. The receiver could get the wrong pseudorange, location and timing according to the spoofers' prior assumptions.

On the military side, Iran interfered with the Global Positioning System (GPS) equipment of the US RQ-170 "Sentinel" drone by using spoofing attack to control the drone landing in December 2011 [20] [21]. At that time, the unmanned reconnaissance aircraft was carrying out the task of collecting information on the construction of nuclear facilities on the Iranian side. After being discovered by the Iranian military's monitoring device, the Iranian military adopted deceptive attacks to make the unmanned reconnaissance aircraft receive wrong instructions. The Iranian military successfully tampered with the message information transmitted by the control section to the receiver, causing the U.S. unmanned reconnaissance aircraft to deviate from its original operating route. After the "Sentinel" unmanned surveillance aircraft was successfully seized, the United States had to admit it. In December 2012, Iran announced that the US Scanning Eagle drone has been captured by using the same technology [22]. In January 2016, two small patrol boats of the US Navy deviated from the original navigation route into Iranian waters. The incident is likely to be caused by Iran's spoofing to make the corresponding vessel lose its connection with the US military. The Iranian side used spoofing techniques to guide the vessel into the wrong waters and make the vessel be detained [24]. In June 2017, the US Oceanic Administration found that at least 20 ships near the Russian New Rossik port had incorrect GPS positioning, and believed that the Russian side was likely to be testing new technologies for GPS spoofing [25] [26].

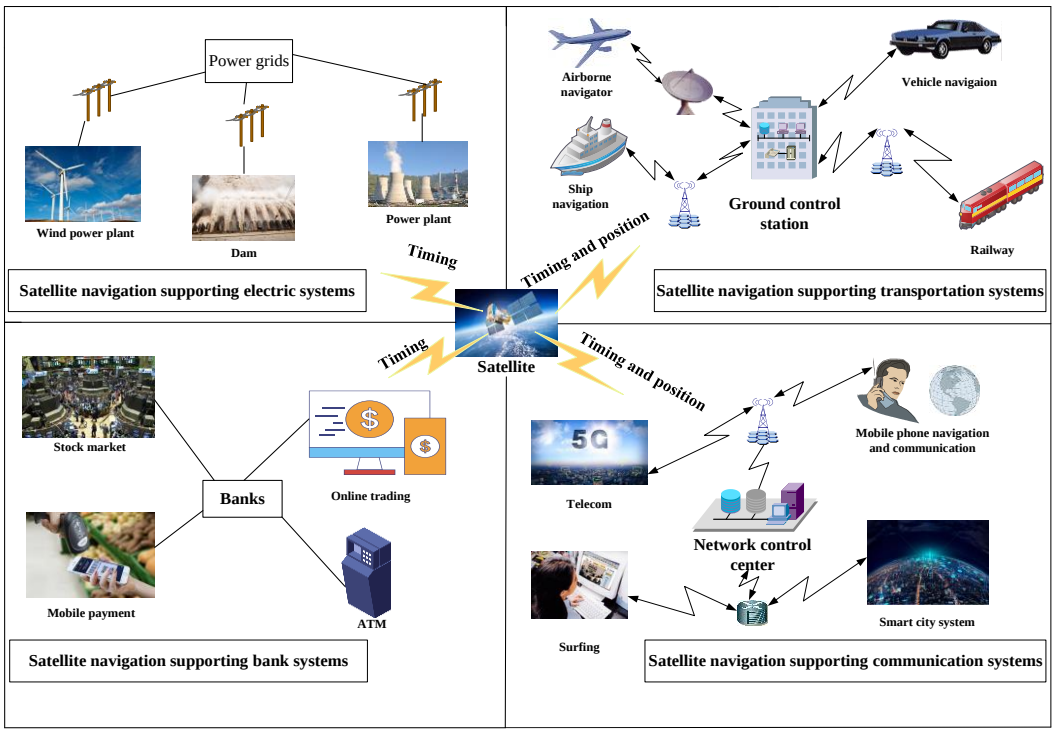

FIGURE 1. The Application of Satellite Systems in People's Daily Life.

On the academic side, the research team led by Professor Todd Humphreys from the University of Texas successfully controlled a super yacht's navigation system using only one laptop, a small antenna, and a cheap GPS spoofing jammer in

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

2013 [23]. In 2017, research units such as Stanford University, the University of Texas at Austin, and Cornell University have also shown through experiments that GNSS receivers are highly vulnerable to spoofing and it is difficult for users to detect the presence of spoofing attacks [6]. At the hacker security conference held in Amsterdam, the Netherlands in April 2013, Hugo Teso, an engineer from a German cyber security company who was also a commercial pilot, announced that after many years of hard work he developed a set of PlaneSploit applications that can bypass aircraft Security check system and take over computer systems on the aircraft. In this simulation, Hugo Teso "PlaneSploit" fully controlled the aircraft, successfully changing the flight route, changing the air-conditioning settings, and even crashing the aircraft [21].

On the civilian or national security side, In March 2014, the flight MH370 from Kuala Lumpur International Airport, Malaysia to Beijing Capital International Airport was lost. No wreckage has been found so far. Some experts speculated that MH370 was likely to be attacked by deceptive interference, causing it to deviate from the route and crash after exhausted fuel. From a technical perspective, spoofing attack technology has this potential attack power, and this possibility is not ruled out at the moment when there is no conclusion on the incident [21]. Spoofers, such as, terrorists use civil navigation signals with open, unencrypted, unauthenticated defects to tamper with civil aviation command information. In other words, the act of "hijacking" has become easier than imagined, and this possible behavior has directly threatened the lives of the people. The security of civil satellite navigation signals requires more means to implement. The issue of signal authentication is also imminent. As the world attaches more and more importance to the safety of certification of civil satellite navigation signals, the US Congress issued certain requirements in the "Federal Aviation Administration's Modernization and Reform Act of 2012" issued in February 2012. The FAA needs to include all drone systems, including commercial drones, under the management of national airspace by September 2015, and develop corresponding safety plans. In 2016, More than 50 GPS interference incidents occurred in Manila Airport in just three months.[27]

These four applications are power system, transportation system, financial system and communication system. Among them, the application of the GNSS system in the power and financial systems is mainly in terms of timing, and the application in the transportation and communication systems is in terms of timing and positioning. The solid line of the border in Figure 1 is mainly used to isolate the four application aspects. The solid lines with arrows in the figure indicate the transmission of information, and the solid lines without arrows indicate the classification of applications.

The above examples have proved that civil navigation systems have obvious security risks in the face of spoofing attacks. For example, at some unknown time in the future, attackers use this security flaw to deceive our daily lives and infrastructure, such as transportation systems, communication systems, power grids and other basic system facilities. The effects of deception can disrupt people's normal lives and cause unpredictable property and security consequences. Therefore, in order to highlight our background, we will detail the background in the form of civil or national security, military and academic classification.

The application of the GNSS system in the power and financial systems is mainly in terms of timing, and the application in the transportation and communication systems is in terms of timing and positioning. The solid line of the border in Figure 1 is mainly used to isolate the four application aspects. The solid lines with arrows in the figure indicate the transmission of information, and the solid lines without arrows indicate the classification of applications.

B. TYPES OF CIVIL GNSS THREATS

In order to highlight the background of the upcoming satellite spoofing technology, we mainly divide the jamming systems to satellite navigation receivers into two categories: jamming attack [28][29] and spoofing attack [30]-[34], and spoofing attack is divided into forwarding spoofing attack and generating spoofing attack according to the generation of deceptive signals. The specific attack classification (taking GPS as an example is shown in Table I) and the schematic diagram are shown in Figure 2.

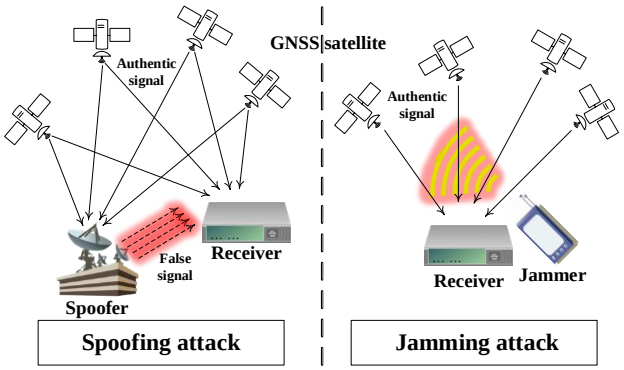

FIGURE 2. Spoofing schematic diagram of jamming attack (left) and spoofing schematic diagram of spoofing attack (right).

The solid lines with arrows in Figure 2 represent satellite signals. In the case of spoofing attack, both the deceiver and the receiver can receive real satellite signals. The red dotted arrow indicates the spoofing signal sent by the deceiver to the target receiver. In the case of jamming attack, the yellow curve represents the interference signal sent by the jammer.

The spoofing attack mainly includes generating spoofing attack and forwarding spoofing attack. The spoofer who want to implement spoofing attack should not only have a comprehensive understanding for the information format of navigation satellite, but also understand the satellite signal structure. The spoofer autonomously generates satellite signals and transmits them to the receiver, accordingly guiding the receiver to capture and track the spoofing signal

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

unconsciously [35]. This kind of jamming gradually guides the receiver away from the correct navigation and positioning results, so that the receiver will generate wrong speed, position and other information [36]. The above-mentioned spoofing attack is known as the spoofing process of the generating spoofing attack, while the forwarding spoofing attack is simpler than the interference in the implementation of the spoofing process. In the forwarding spoofing attack, the spoofer intercepts the authentic signal transmitted by the satellite to the receiver, and then delays the intercepted satellite signal before forwarding it to the target receiver. Therefore, the interference signal after being forwarded by the spoofer is exactly the same as the authentic navigation signal, except that the delay and amplitude of the signal are different. After receiving the signal forwarded by the spoofing device, the receiver calculates the erroneous signal propagation delay and pseudorange information, thereby affecting the positioning result of the receiver [37]. The forwarding spoofing attack spoofers must match some interference strategies that are compatible with the forwarding spoofing attacks in order to improve the success rate of the forwarding spoofing attacks [1].

The jamming attack mainly uses the transmitter to transmit high-power interference signals and suppresses the satellite signals at the front of receiver, thereby shielding or suppressing the spectrum of the GNSS satellite signals to be received by the GNSS receiver. In addition, the jamming attack significantly diminishes the signal-to-noise ratio of the received signals and makes the GNSS receiver reduce or completely lose its normal working ability. The GNSS receiver that suffered from jamming attack is unable to receive the satellite signals being tracked routinely [28]. The receiver can adjust the relevant receiving antennas to remove the blocking signal in the received signal to improve the signal to interference ratio [29]. Therefore, the jamming attack is effortlessly detected by the receivers.

Both jamming attack and spoofing attack have an impact on military signals or civilian signals of GNSS. The overall impact of two jamming methods for military signals and civilian signals is shown in Table I

In summary, the jamming attack is the most effective method for spoofing in the case of low technical conditions, but this kind of jamming is also the most easily detected by the receiver with certain anti-spoofing performance. From the scope of application, forwarding spoofing attack can interfere with both military signals and civilian signals. Because of the easily detectable nature of jamming attack, the spoofer must design a spoofing strategy to ensure the reliability of the spoofing effect. From the perspective of jamming effects, although generating spoofing attack is less threatening to the military signal, it has a superior impact on the security of the civilian signal. Since the jamming attack is easily recognized by the receiver, this jamming mode can be resisted by the relevant measures taken by the receiver in time. If the satellite signal is suppressed, the probability of successful spoofing attacks is very high. Under this assumption, the receiver cannot detect it in time, thereby obtaining incorrect positioning or timing results. Based on this, this paper analyzes different anti-spoofing methods and studies application of these methods to spoofing.

Table I

IMPACT OF SATELLITE NAVIGATION JAMMING ON GNSS SIGNAL

Type of GNSS signal	Jamming attack	Spoofing attack	
		Forwarding spoofing attack	Generating spoofing attack
Military signals	Jamming attack is less difficult to implement and has a strong interference effect on existing satellite signals. However, the jamming method is easily detected by the receiver and resisted by corresponding measures [28] [29].	The implementation of the jamming mode is less difficult, and the spoofer can carefully design a spoofing scheme to achieve a better deception effect. If the spoofer does not combine some spoofing strategies, the receiver may perform spoofing detection based on some characteristic information of the navigation message. For a receiver based on navigation message ranging, the forwarding spoofing cannot arbitrarily control the position information output by the receiver, so that the spoofing effect of the spoofer has some defects.	Since military signal is not disclosed, the spoofer cannot perform the generating spoofing attack on the military signal.
Civilian signals			Since the navigation message content, frame structure and signal characteristics of the civilian signal have been introduced in the relevant documents, the spoofer can generate a spoofing signal through this information, so that the receiver outputs the time and position information designed by the spoofer.

C. THE WORK AND ORGANIZATION OF THIS PAPER

The work of this paper are as follows. First of all, the progress of this survey beyond the state-of-the-art is that we have discussed and analyzed the anti-spoofing performance of countermeasures combining data-level and signal-level from five levels (e.g., Table XLVI). Then based on the theory that satellite signals carry significant satellite information, as long as the signal or information is deceived, it may affect the satellite application terminal. This paper divides the existing anti-spoofing strategy into signal-level anti-spoofing technology and data-level anti-spoofing technology. Based on the classification, this paper further discusses the performance of different anti-spoofing technologies against deception. Finally, this paper combines signal-level and data-level anti-spoofing techniques and then analyzes the performance of the combined anti-spoofing strategy.

This paper is a survey that introduces non-professionals to the various spoofing techniques of GNSS and the current

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

anti-spoofing techniques. The structure of this paper is arranged as follows: Section I introduces most of the existing user receivers are very vulnerable to the security threat of spoofing attacks. Section II presents the research status of spoofing attack classification, spoofing strategy, and spoofing attack performance. Advanced spoofing techniques can even influence complex structure receivers. Section III and section IV show a detailed analysis for the resistance effect of the anti-spoofing methods at the signal processing level and information level respectively to the spoofing strategy that will propose in section II. The spoofing resistance performances for many anti-spoofing methods have been verified in software simulation, laboratory hardware testing or field actual testing. Section V introduces the anti-spoofing performance of some practical anti-spoofing methods applied to the combined spoofing scenarios. Comprehensive consideration and appropriate combination of the anti-spoofing techniques summarized in this paper provides a certain reference value for receiver designers and can be directly applied to receiver design. Section VI introduces challenges and future research of GNSS anti-spoofing. Section VII summarizes the development trend of anti-spoofing interference technology of GNSS system. Section VIII concludes this paper with summary.

II. STRATEGY FOR SATELLITE NAVIGATION SIGNAL SPOOFING ATTACK

A. ABBREVIATIONS AND ACRONYMS EXPLANATION OF BASIC TECHNIQUES AND THE CLASSIFICATION OF THE GENERAL ARCHITECTURE

In order to facilitate the reader's understanding of this survey, some important abbreviations and their meanings are shown in Table II. The abbreviations are only applicable to this survey. The specific explanations are given in the form of a table. In the process of basic technology explanation, we give three basic technology classifications, which are the explanations of the proper nouns involved in this paper, the explanations of the spoofing attack strategies terms involved in this paper, and the explanations of the anti-spoofing attack method terms involved in this paper.

TABLE II
ABBREVIATIONS TABLE

Abbreviation	Meaning
Abbreviations related to proper nouns	
GNSS	Global Navigation Satellite System
PVT	Position Velocity and Time
RAIM	Receiver Autonomous Integrity Monitoring
GPS	Global Positioning System
ICD	Interface Control Document
Abbreviations related to spoofing attack strategies	
RSA	Replay Spoofing Attack
FSA	Forgery Spoofing Attack
ESA	Estimation Spoofing Attack
ASA	Advanced Spoofing Attack
FEA	Forward Estimation Attack
SCER	Security Code Estimation and Replay
Abbreviations related to anti-spoofing attacks	
NMA	Navigation Message Authentication
NMET	Navigation Message Encryption Technology
NON-NMET	Non-Navigation Message Encryption Technology
PA	Protocol Authentication
NMA&PA	Navigation Message Authentication and Protocol Authentication combination
SCA	Spreading Code Authentication
SCE	Spreading Code Encryption
WT	Watermark Techniques
CA	Combined Authentication

B. SPOOFING PRINCIPLES AND CLASSIFICATION OF SPOOFING STRATEGIES

For most receivers, the received signal power is small and weak, and the acquisition and tracking of satellite signals is typically determined by spreading code correlation. However, in a realistic living environment, multipath effects and high-power electromagnetic waves can affect the normal reception of the receiver. Since the power of the multipath signal is less than the power of the authentic signal, the receiving opportunity mistakenly believes that the signal of the lower power is noise, thereby tracking the signal with higher power to resist the multipath effect. The spoofer utilizes the receiver mechanism to adjust the power of the spoofing signal to be slightly larger than the authentic signal power, thereby achieving the purpose of spoofing the receiver. In Pasiaki's paper [6], the four types deception process diagram of the spoofing signal is introduced.

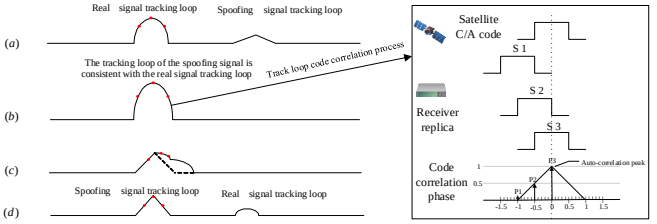

FIGURE 3. Spoofing process of spoofing signal (adapted from [6] and [38]).

In the spoofing process shown in Figure 3, there are mainly four relative power modes of the authentic signal and the spoofing signal. Curve (*a*) represents the process by which the spoofing signal is searching for the tracking loop of the real signal, and the power of the spoofing signal is less than the power of the real signal. Curve (*b*) indicates that the tracking loop of the spoofing signal is consistent with the tracking loop of the real signal. Curve (*c*) shows the transition of the receiver from capturing the state of the real signal to capturing the state of the spoofing signal. Curve (*d*) denotes that the spoofing signal power of the spoofer is greater than the authentic signal power, and there is a certain offset between the phases of the two types signal. In this way, the receiving opportunity mistakenly believes that the real signal with low power is a by-product under noise. Under this condition, the receiver continuously captures the spoofing signal. Due to the phase offset, it is difficult for the receiver to find that the received signal is a spoofing signal.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

The overall deception process is generally shown in curve (a) to curve (d). The right part of Figure 3 is the process of how the satellite C / A code is related to the receiver's replica code. S1 to S3 are the three code phase states of the receiver's replica code [38]. In order to further improve the success rate of spoofing attacks, the spoofing party must also combine certain spoofing strategies to conduct spoofing attacks. Existing spoofing strategies are mainly divided into four categories, replay spoofing attack (hereinafter referred to as replay spoofing attack strategies, these strategies are abbreviated to RSA) [6], [39]-[44] and [54], forgery spoofing attack (hereinafter referred to as forgery spoofing attack strategies, these strategies are abbreviated to FSA) [14], [45]-[49], estimation spoofing attack (hereinafter referred to as estimation spoofing attack strategies, these strategies are abbreviated to ESA) [36], [54]-[55] and advanced spoofing attack (hereinafter referred to as advanced spoofing attack strategies, these strategies are abbreviated to ASA) [6], [56] as shown in Figure 4.

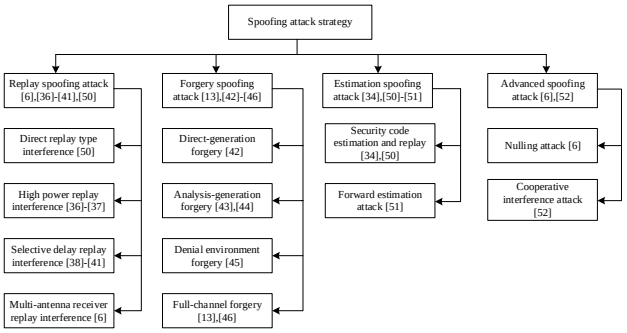

FIGURE 4. Taxonomy of spoofing attack strategy.

In Figure 4, this classification depends on different strategies for spoofing attacks, and each spoofing attack strategy has many variations. For example, RSA can be divided into direct replay type interference, high power replay interference, selective delay replay interference and multi-antenna receiver replay interference according to different spoofing strategies. The mainly spoofing strategies' characteristics (including difficulty of implementation and attack effect) are shown in Table III.

The "attack effect" defined in Table III is divided into four levels of "poor" "moderate-good" "good" and "good". The four levels are relative, that is, the ability of the spoofer to successfully spoofing the target receiver. The attack effect "poor" means that the spoofer cannot deceive the target receiver. The attack effect "Moderate" means that the attack method of the deceiver may be recognized by the target receiver. The attack effect "Moderate-good" and "Good" means that the deceiver can quietly cause the target receiver to be deceived. From the above four types of spoofing strategies, the spoofer usually uses RSA and FSA for general receivers. For receivers that have applied anti-spoofing strategies, the spoofer will have better spoofing effects by using ESA and ASA. The difficulty of implementation is mainly determined by the hardware cost and technical cost of the spoofing strategy. In general, the higher the technical cost of hardware, the more difficult it is to achieve. However, for those deceptive designs with lower hardware costs but high technical costs, the implementation difficulty is mainly based on technology cost. The evaluation of the attack effect of a spoofing strategy is mainly based on the related papers of the spoofing strategy. Through the relevant experimental information in the paper, the spoofing performance of some spoofing strategies for simple receivers is evaluated.

1) REPLAY SPOOFING ATTACK

For RSA, the spoofer generally uses different interference methods to assist the spoofing process. The auxiliary interference methods of spoofing strategy are mainly divided into direct replay type interference [54], high power replay interference [39][40], selective delay replay interference [41]-[44] and multi-antenna receiver replay interference [6]. The specific classification criteria are based on the following analysis. RSA scenario as illustrated in Figure 5.

TABLE III
CLASSIFICATION OF SPOOFING ATTACKS

Deception type	Difficulty of implementation	Attack effect	Characteristics
Replay spoofing attack (RSA) [6], [39]-[44] and [54]	Low	Moderate	The spoofing party delays the transmission of the received signal to the receiver, thereby spoofing the receiver. The implementation of this spoofing type is relatively simple. However, if the spoofer wants to improve the spoofing success rate by this method, the spoofer should adjust the spoofing signal parameters reasonably and assist the appropriate spoofing environment to ensure a better spoofing effect.
Forgery spoofing attack (FSA) [14], [45]-[49]	Medium	Moderate-good	This spoofing method adjusts the relevant parameters of the signal by generating a spoofing signal, so that the spoofer controls the positioning result of the receiver.
Estimation spoofing attack (ESA) [36], [54]-[55]	Medium-high	Good	This method can not only affect ordinary civil signals, but also cheat some civil satellite signals with unknown security codes. This method estimates satellite information by means of signal estimation and generates satellite signals through the result of signal estimation to control satellite signal receiver.
Advanced spoofing attack (ASA) [6], [56]	High	Good	For receivers that are more complex and use anti-spoofing methods, the receiver not only adopts multiple spoofing strategies, but also combines signal characteristics to design a more effective spoofing signal format, thereby more directly and effectively spoofing the receiver.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

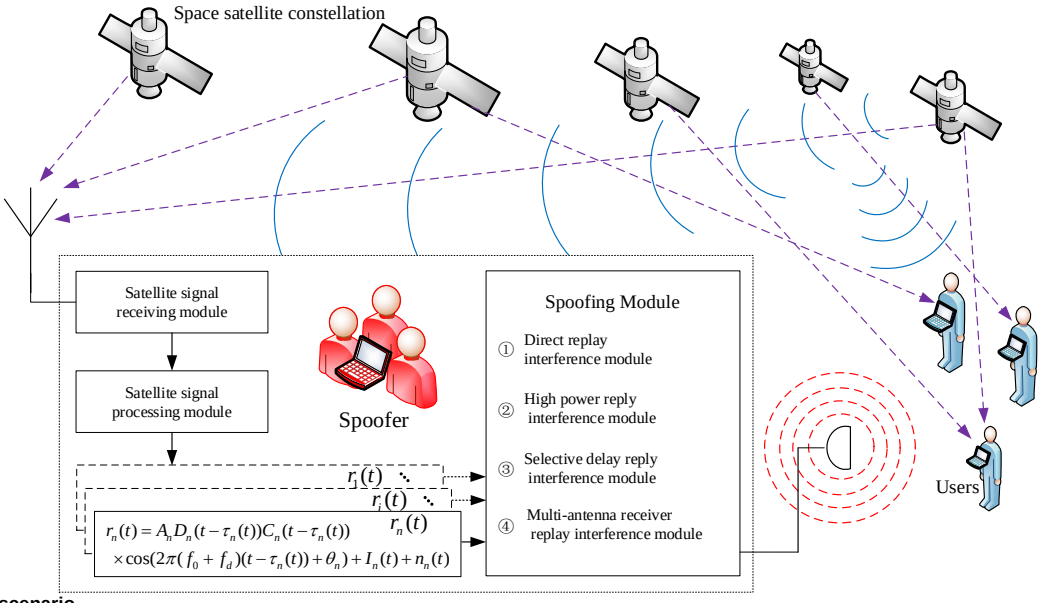

FIGURE 5. RSA scenario.

There is a propagation delay for the satellite signal arriving at the receiver. RSA is based on the inherent signal propagation delay, artificially replaying, or adding a certain delay to implement the spoofing attack. We assume that the receiver receives a normal satellite signal expression in Figure 5. Here A denotes the amplitude of the n_{th} satellite signal, $D_n(t)$ denotes the navigation message of the satellite signal, $C_n(t)$ denotes the ranging code of the satellite signal, $\tau_n(t)$ is the propagation delay of the signal, f_0 and f_d are the standard carrier frequency of the satellite signal and doppler frequency, θ_n is the beat carrier phase, $I_n(t)$ denotes the possible interference of the received satellite signal, and $n_n(t)$ denotes noise.

When the spoofer initiates a RSA, it can artificially send the real satellite signal directly to the receiver, which is said direct replay spoofing interference. The spoofer artificially increases the amplitude of the satellite signal, which is called high-power replay interference. The Selective delay replay interference adds a certain delay to the satellite signal propagation delay. Multi-antenna receiver replay interference is an auxiliary interference means for a spoofer to implement RSA using multiple antennas. Since the signals of the spoofing attack are from one direction (as shown in Figure 2), the spoofer can use the multi-antenna receiver to replay the spoofing signal to prevent the receiver from detecting the spoofing attack by using the method of "signal arrival detection is consistent". The characteristics of these four interference modes are shown in Table IV.

TABLE IV
CLASSIFICATION OF RSA

Auxiliary interference methods	Difficulty of implementation	Attack effect	Characteristics
Direct replay type interference [54]	Low	Poor	The spoofing device of the interference method is similar to the signal repeater, which directly forwards the received signal and affects the positioning result of the receiver. This type of deception is generally not used because of its poor deception effect.
High power replay interference [39]-[40]	Medium-low	Moderate	The interference method artificially increases the power of the spoofing signal to trick the receiver into thinking that the spoofing signal is a real signal, and the weak satellite signal is a product of the multipath effect, thereby tricking the receiver into receiving the spoofing signal. This method is generally used in combination with other strategies to improve the success rate of fraud.
Selective delay replay interference [41]-[44]	Medium-low	Moderate	The interference method artificially adds a certain delay to the satellite signal, accordingly, affecting the phase of the spreading code and the normal capture of the receiver. This method is generally used in combination with other strategies to improve the success rate of fraud.
Multi-antenna receiver replay interference [6]	High	Moderate-good	For a multi-antenna receiver, the direction of arrival angle can be detected by the antenna. Since the spoofing signal is transmitted through the transmitter of the surface, the direction angles measured by the antennas are substantially the same, so that the spoofing signal is easily detected. Therefore, a multi-antenna receiver requires multiple spoofing sources for combined spoofing and combines the above spoofing strategies to enhance the effect of spoofing.

Huang et al. used signal sources to simulate RSA [37]. By studying High power replay interference, the team found that in their prescribed experimental environment, when the power of the replayed spoofing signal is higher than the power of the real signal by 4 dB, it can destroy the target receiver's reception of the authentic signal within 50 minutes and then track the spoofing signal instead. Gao et al. further found through experiments that if the interference-to-signal ratio of the forwarded signal is greater than 14 dB, signal spoofing can be completed within 4 seconds [39]. Huang' team also studied the selective delay replay interference [40]. Through simulation, they found that this interference has a great attack effect on the timing receiver, and this interference is more difficult to be detected by the receiver. Shi's team used genetic algorithms to optimize the signal delay duration at various points in the deception process [42]. In this way, not only the concealment of the signal is improved, but also the complexity of the method is lower than that of the point-by-point approach. If the receiver uses the carrier ranging method instead of the navigation message ranging method for positioning, Bian et al. verified that the deception can even affect the measurement of the receiver's PVT (Position, Velocity and Time) [43].

Complex satellite navigation receivers not only have multiple antennas to receive and measure signals, but also perform data fusion analysis with other navigation systems to resist spoofing signals. For such a receiver, if the attacker only uses the RSA, it needs to combine the delay adjustment and the power adjustment scheme to implement the spoofing attack by multiple spoofing sources [1]. In addition, the deceptive effect designed by the attacker is also selective. Wang et al. believes that if the deceiver slowly adjusts the deception signal positioning effect for a long time, the deception effect will not only deceive the satellite navigation system, but also affect some parameters of the inertial navigation system, and affect the normal calibration process system of the inertial navigation system, thereby further deceiving the entire inertial navigation system [41].

In summary, although the implementation process of the RSA is relatively simple, if the attack wants to achieve a good spoofing effect, the relevant parameters of the spoofing signal also need to be appropriately adjusted to improve the spoof success rate. However, some of the auxiliary interference methods in the process of RSA are also applied to other spoofing processes at the same time, thereby facilitating the implementation of the spoofing process.

2) *FORGERY SPOOFING ATTACK*

FSA is more complicated than RSA. This spoofing attack has a large impact on most receivers. For FSA, it is mainly divided into direct-generation forgery [45], analysis-generation forgery [46][47], denial environment forgery [48] and full-channel forgery [49]. Figure 6 is a schematic diagram of FSA. The specific classification criteria are based on the following analysis.

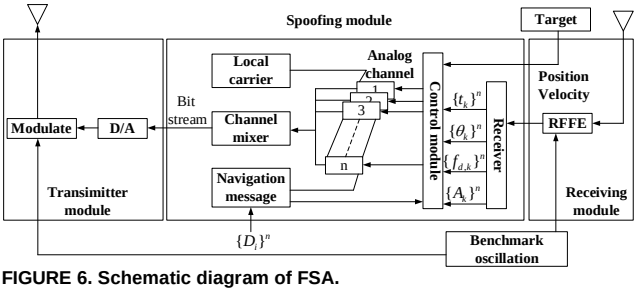

FIGURE 6. Schematic diagram of FSA.

The simple signal generation model of the FSA consists of three parts: the satellite signal receiving module, the spoofing signal generating module, and the spoofing signal transmitting module. The following three modules are introduced separately to illustrate the above criteria for classification of FSA.

In the satellite signal receiving module, the spoofing receiver receives the real satellite signal through the antenna and then transmits the signal to the receiver of the spoofing signal generating module via the radio frequency front end (RFFE). In addition, the spoofing receiver monitors the spoofed target in real time to obtain the location and speed of the spoofed target.

In the spoofing signal generation module, there are two cases. In the first case, the receiver directly generates satellite signals. This is the direct-generation forgery mentioned above, but the satellite signals generated in this case tend to deviate from the real signals. In the second case, in order to generate a signal similar to the real signal, the spoofer needs to frequency-convert the received signal. The spoofer will obtain the baseband signal after demodulation, so as to obtain the relevant parameters of the real satellite signal for analysis and generate a fraud signal. The spoofing process in the second case is the above-mentioned analysis-generation forgery. As shown in Figure 6, the receiver obtains four parameters by processing and calculating the baseband signal, where $\{t_k\}^n$ is the estimation initial moment of the k_{th} C/A code period of receiving channel $1 \sim n$, $\{\theta_k\}^n$ is the estimated carrier phase of receiving channel $1 \sim n$ at $\{t_k\}^n$, $\{f_{d,k}\}^n$ is the estimated doppler frequency shift of receiving channel $1 \sim n$ at $\{t_k\}^n$, and $\{A_k\}^n$ is the signal amplitude of receiving channel $1 \sim n$ at $\{t_k\}^n$. In order to increase the success rate of fraud, the spoofer often increases the amplitude $\{A_k\}^n$ of the spoofing signal, which is the above-mentioned denial environment forgery. The parameters calculated by the spoofing receiver are input to the control module, and the specific spoofing process of the control module is as shown in Figure 3. The spoofing signal after the control module can be completely synchronized with the entire capture and tracking loop of the spoofing target receiver. The signals generated in each of the N spoofed channels are identical to the channel parameters corresponding to the signals tracked by the receiver module, so that Full-channel forgery can be implemented.

The specific characteristics of the above-mentioned four-forgery spoofing attacks (FSA) are shown in Table V. In

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

TABLE V
CLASSIFICATION OF FSA

Spoofing attack type	Difficulty of implementation	Attack effect	Characteristics
Direct-generation forgery [45]	Medium	Moderate	The spoofer directly generates satellite signals using Field Programmable Gate Array (FPGA), Digital Signal Processor (DSP), and Software-defined Radio (SDR) through various satellite navigation interface files [50]. However, the directly generated satellite signal does not match the phase difference and related parameters of the existing propagating satellite signal, and thus is not easily received by the receiver.
Analysis-generation forgery [46],[47]	Medium-high	Moderate-good	The fraud signal transmitter includes a receiver and a transmitter. The receiver analyzes the received authentic satellite signal and then applies the obtained signal parameters to the spoofing signal, which is transmitted immediately, accordingly improving the spoof success rate.
Denial environment forgery [48]	Medium	Moderate	In order to improve the success rate of signal spoofing, the spoofer will send large-scale interference to the target receiver, forcing the receiver to jam and losing the current tracking accuracy. In this case, the spoofer sends the spoofing signal to be more easily received by the receiver, thereby achieving the purpose of spoofing.
Full-channel forgery [14],[49]	High	Good	Full channel forgery is a full-scale spoofing of all known channels (or channels that the target receiver can receive). This means that the spoofer must simultaneously deceive multiple satellite signals. In this case, the spoofer can control the receiver positioning result more accurately. Due to the complexity of full-channel satellite signal spoofing attacks, some simple anti-spoofing strategies will fail.

addition, the high-power replay interference, and selective delay replay interference mentioned in Section A can also be applied in FSA. The specific application process will be explained later.

For the direct-generation FSA, it can be traced back to Scotta's experiment [44]. In his experiment, he used GSS8000 GNSS simulator from Spirent Company to configure the corresponding power amplifier and transmitting antenna to make a proper signal spoofing device. However, the signal generated by such a generating device lacks relevant parameters of the authentic signal. Even if the signal sent by the spoofer forces the receiver to lose lock and recapture, the receiver will be alert to this spoofing signal. The receiver can also directly detect such an error signal and discard it based on the error of the phase information of the signal which is generated by signal generating device. For analysis-generation FSA, the most representative is the GNSS spoofing source developed by Professor Humphreys' team, which can generate high-concealed spoofing signals in combination with the received satellite signals [45]. This kind of signal has been experimentally proven to cause real-time spoofing of drones. Professor Dai proved that this kind of spoofing technology is effective for both static and dynamic positions, and the performance is relatively stable [46].

In the FSA, the spoofing method based on analysis generation is the common spoofing method. However, in order to spoof the target receiver as fast as possible, the three methods mentioned above, namely, adjusting signal power, adjusting signal delay and denial environment, are generally adopted. Professor He found that when the spoofing signal correlation peak is aligned with the real signal correlation peak, if the signal power is increased, the spoofing signal can control the receiver [47]. However, in order to avoid the detection of anomalies by the receiver, the signal power should not increase too much, and the signal power should not increase too fast. In addition, denial environment is a common spoofing strategy. The main working process of the spoofing strategy is to add high-power signals to the receiver during the normal receiving process, causing the receiver to be jamming, which is called the denial environment. In this case, the spoofing success rate of adding spoofing signals to the receiver will be greatly improved. Professor Shi used broadband white Gaussian noise as a jamming signal to create a denial environment [48]. By establishing a simulation environment, he found that the denial environment not only improved the success rate of spoof, but also reduced the receiver's capture rate of normal signals. However, this method still needs further study for considering the relevant engineering parameters of the environment. Wang et al. simulated the spoofing process through the GPS signal source [51]. They found that the spoofer in the denial environment can better cover up the real signal, highlight the deceptive signal, and realize the spoofing process. One speaks of full-channel FSA, which is a process in which a signal source performs multi-channel spoofing processing. Since there are many satellite signals that a receiver can receive, the receiver needs to implement a full-channel spoofing attack in order to better implement the satellite signal spoofing process. In the process of full channel forgery, the receiver cannot increase the power of the spoofing signal indefinitely, which requires adjustment the satellite signal power of each channel. Professor Yang developed a power control algorithm using genetic factor algorithm [49]. Simulation experiments show that the relative capture rate of multi-channel spoofing signals is increased by

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

50% when the noise rise is less than 10dB, and the concealment of spoofing signals is also enhanced. Xie et al. also proposed some key techniques for full-channel FSA [14]. First, since the time precision of the spreading code is high, if the spoofer wants to complete the signal spoofing, the synchronization phase of the spoofing signal must be accurately controlled. Secondly, since the navigation message contains various parameters such as signal integrity and ionospheric correction, the spoofer must generate a reasonable spoofing signal to avoid the alarm of the receiver. Since the broadcasting time interval of navigation messages is short, the spoofing signal is also broadcasted in real time and in accordance with the interface control document (ICD) requirements for the spoofing signal, thereby continuously spoofing the receiver. Finally, Professor Lu implemented real-time simulation control of the navigation process. He believes that for the deceptive effect of deceptive signals, the spoofer must also monitor and generate appropriate navigation messages in real time to achieve the intended goal. In addition, Ma et al. believe that the spoofer should also pay attention to avoid the Receiver Autonomous Integrity Monitoring (RAIM) alarm mechanism to complete the deception process in the process of spoofing [52].

In a word, the spoofing effect of FSA is good and relatively easy to operate. However, during the spoofing process, the spoofer should also pay attention to the spoofing signal power and phase size in real time to avoid being detected by the receiver. Meanwhile, FSA in the denial environment should not send high-power jamming signals multiple times in the same time period, so as to prevent the receiver from thinking it is compression interference.

3) *ESTIMATION SPOOFING ATTACK*

For some navigation messages that contain anti-spoofing means, for example, an unknown security code is inserted into the navigation message to improve the security of the navigation message. The spoofer alone relies on generating spoofing attack, which does not work because the spoofer cannot predict the security code in the navigation message and thus cannot read and generate a navigation message that can be recognized by the receiver. Therefore, the spoofer must estimate the received navigation signal in order to perform the deception process and judge the content of the navigation message by the estimated result. Nowadays, there are two types of ESA, namely security code estimation and replay (SCER) [36][54] and forward estimation attack (FEA) [55].The navigation message containing the security code is generated by the sender through an encryption algorithm. The spoofer needs to calibrate the satellite signal propagation delay to estimate the code offset of range code and estimate the carrier phase. The spoofer will use real satellite signal parameters to generate spoofing signals after successfully estimating security codes, and update spread codes and carrier replicas at the same time.

The SCER attack was first proposed by Professor Humphreys to achieve a more difficult spoofing attack [36][54]. If the spoofer wants to launch such an attack, it must study various aspects such as navigation messages, navigation signals, and signal estimation methods. For this spoofing attack, the most important is the accurate estimation of the security code and the precise control of artificially adding delay. When the security code inserted in the navigation message is too long, the above two key points are more important. For the existing SCER anti-spoofing method, the receiver mainly constructs the probability decision function from the perspective of signal probability analysis, and the receiver also judges the spoofing attack by combining signal power, delay, and information integrity. However, this method of deception is difficult, and it is generally not used in actual projects.

The FEA attack is a method of pre-estimation proposed in recent years [55]. Since most receivers do not check the navigation message before decoding, the spoofer can generate a navigation message in combination with the prior information to deceive the receiver. The navigation message in the FEA attack is generally a navigation message with an authentication function. By the intrinsic relevance of the navigation message, the more the navigation message information is obtained by the spoofer, the more accurate the false navigation message estimated by the spoofer. In FEA, the spoofer can send fake information even before the authentic information is sent to implement the spoofing process. In contrast, the SCER must first obtain the authentic signal and then estimate the signal parameters before it can implement the spoofing process. Curran et al. performed a simulated attack on the FEA spoofing attack, in which the attack object was a Galileo signal with navigation message authentication (NMA)[55]. The experimental results show that under the FEA attack, the NMA cannot achieve the authentication function. However, if the sender adds anti-replay information to the navigation message, this means that parts of each navigation message are different, making it difficult to estimate the sender's future navigation messages. The above process can resist FEA attack to some extent.

Both two types of attacks are based on signal estimation. Since the implementation of the two attacks is difficult, the spoofer generally does not adopt it. However, if the sender adopts some cryptography anti-spoofing methods in the future, the deception effect of these two attacks will also have some influence. Therefore, when designing cryptographic-based anti-spoofing methods (especially the NMA method), the receiver needs to consider the resistance of these two attacks.

4) ADVANCED SPOOFING ATTACK

In addition to the above types of spoofing attacks, some scholars have proposed other spoofing attacks in recent years, including nulling attack [6] and cooperative interference attacks [56]. As shown in Figure 7, the signal schematic diagram of nulling-spoofing attack is generated.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

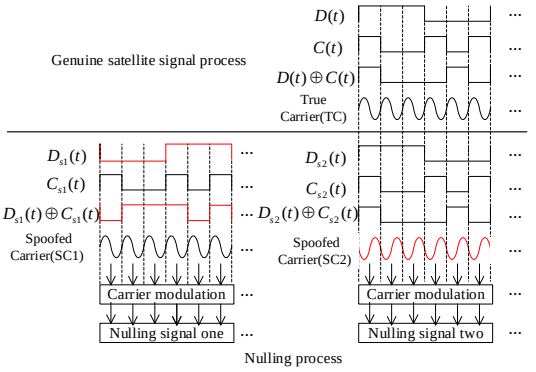

FIGURE 7 . Nulling attack signal diagram.

The signal of the nulling attack consists of two parts, a nulling signal one and a nulling signal two. The nulling signal one is a spoofing signal, which tampers with the received genuine satellite information, thereby changing the positioning and time of the target receiver to achieve the purpose of fraud. It can be seen from Figure 7 that the spoofing satellite information $D_{s1}(t)$ is different from the genuine information $D(t)$, but the ranging code and the carrier are the same ($C(t) = C_{s1}(t)$ and true carrier (TC) = spoofed carrier (SC1)). The information of the nulling signal two $D_{s2}(t)$ and the ranging code $C_{s2}(t)$ are the same as those of the genuine signal, but the carrier phase has a deviation of π . The function of the signal two is to eliminate the genuine signal received by the receiver. Nulling signal two makes the receiver not capture the genuine signal, only captures the nulling signal one, and finally achieves the purpose of deception. The expression of the GNSS signal received by the receiver can be as follows.

$$R(t) = \mathrm{Re}\{\sum_{i=1}^{N} A_i D_i[t-\tau_i(t)]C_i[t-\tau_i(t)]e^{j[w_c t-\phi_i(t)]}\}$$

where N is the number of constituent spreading-code specific signals, A_i is the amplitude of the signal, D_i is the data of the signal, C_i is the PN code of the signal, $\tau_i(t)$ is the code phase of the signal, $\phi_i(t)$ is the beat carrier phase of the signal. In nulling process, signal one and signal two must satisfy the following relationship. $C_{i+N}(t) = C_i(t)$ and $D_{i+N}(t) = D_i(t)$ for *i*=1, ….,N. The function of the signal two is to eliminate the genuine signal received by the receiver. Therefore, the nulling signal must obey $A_{s[i+N]} = A_i$, $\tau_{s[i+N]}(t) = \tau_i(t)$ and $\phi_{s[i+N]}(t) = \phi_i(t) + \pi$.

Spread spectrum communication has the characteristic of low probability of interception. The object of this paper is to analyze the anti-spoofing and spoofing technology of civil GNSS navigation system. The spread spectrum technology used in most civil systems is the direct sequence spread spectrum method (DSSS). The low intercept probability of DSSS signals is due to the fact that any enemy receiver, even if the bandwidth is sufficient to receive direct sequence spread spectrum signals, it will also receive a lot of noise power, resulting in a very low signal-to-noise ratio of the intercepted signal. Compared with direct spread spectrum, frequency hopping communication is widely used in military navigation signals. The reason why the frequency-hopping signal is used as the LPI signal is that the time it takes up a frequency is very short, making it difficult for the enemy to detect the presence of the signal. In other words, the frequency-hopping signal stays at each frequency for a short time, so that the power that the signal is received at the instant is significantly reduced.

The main characteristics of nulling attack and cooperative interference attacks are shown in Table VI.

TABLE VI
CLASSIFICATION OF ASA

Attack name	Difficulty of implementation	Attack effect	Characteristics
Nulling attack [6]	High	Moderate-good	The spoofer sends the same power delay as the real signal, but the carrier phase is opposite. After receiving this signal, the receiver will cancel with the real signal, making the receiver lose the signal parameters of the real signal and reducing the anti-spoofing performance of the receiver.
Cooperative interference attacks [56]	Extremely High	Good	The attack mode is coordinated by multiple spoofers using the spoofing strategy mentioned above. Even if some receivers adopt sophisticated anti-spoofing methods, the integrity and reliability of information may not be guaranteed.

Nulling attack [6] is a spoofing method proposed in recent years to improve the receiver's spoofing success rate. However, the implementation of nulling attack is very difficult. Until now, this attack method is only a theoretical means of interference and has not been put into practice. Cooperative interference attacks are designed to affect the normal operation of anti-spoofing receivers, such as RAIM receivers. Ledvina et al. [56] have implemented a cooperative interference attack and has achieved the accuracy of deception to a three-dimensional sub-centimeter. The cooperative interference attacks he designed can counter complex anti-spoofing methods, such as anti-spoofing based on estimated angle of arrival. However, this anti-spoofing method is difficult to implement and requires more consideration of the surrounding environment.

For advanced signal spoofing, most of them remain in the theoretical stage. However, with the continuous development of hardware and computer technology, the theoretical spoofing mode may also be turned into reality in the future. Therefore, these spoofing methods need to be considered when designing anti-spoofing methods.

C. THE APPLICATION OF SPOOFING TECHNIQUES AND ANTI-SPOOFING TECHNIQUES

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

The first is the application of spoofing techniques. In 2016, drones have been widely used in U.S. military, police, and border patrols. However, due to limited budgets, other U.S. departments use drones smaller than the military. According to reports from the US Department of Homeland Security (DHS) and the US Customs and Border Protection (CBP), drug traffickers on the US-Mexico border are using deceptive GPS jamming techniques to attack U.S. border patrol drones for the purpose of secret crossing. In 2017, when a 37,000-ton tanker Atria was about to dock at the port of Novosibirsk in the Black Sea port, an alarm sounded suddenly, and the positioning system showed that the tanker was located 20-30 miles from the port. The captain found that the tanker's GPS showed that the tanker was located at Gelendzhik Airport, more than 32 kilometers off the coast. It was later proved that more than 20 ships nearby had suffered the same deceptive attack. In June 2019, the latest research by Israeli cybersecurity company Regulus Cyber showed that the navigation systems of Tesla Model S and Model 3 electric vehicles are vulnerable to deception. Regulus Cyber recently tested the car using Tesla's "navigate on autopilot" feature. It turned out that an attack on the "navigation on autopilot" function could cause the car to slow down suddenly and deviate from the main road.

Secondly, the application aspects of anti-spoofing technology are introduced. In February 2017, Israel launched a GPS anti-jamming system at the Indian Air Show. According to information provided by Israel Airlines, this system is only the size of a laptop. The GPS anti-jamming system is based on the design of Israel Airline industry 's multi-channel control receiving antenna technology. The system mainly consists of a GPS antenna array composed of multiple antennas and an advanced digital processing unit. It protects the avionics system from direct electronic attacks such as GPS jammers. In June 2019, wireless security company infiniDome demonstrated GPS interference and deception protection features for autonomous vehicles at the 2019 EcoMotion Main Event. During the live demonstration, the GPS jammer near the BWR self-driving car was activated and the navigation function of the self-driving car was disabled. The experimenter connected the "GPSdome" protection scheme to the same self-driving car with the same GPS system. Experiments have found that cars can not only detect jamming attacks, but also maintain GPS signals and navigation functions when subjected to jamming attacks.

D. SUMMARY

In combination with the twelve spoofing strategies described in this section, in addition to the final cooperative interference attacks, these eleven schemes can also be associated with the forwarding spoofing attack and the generating spoofing attack mentioned in section I. The spoofer selectively selects the spoofing strategy according to the spoofing target and combines some combinable spoofing scheme (such as selective delay, selective power, etc.), so that the spoofer can form the three levels of spoofing techniques shown in Figure 8.

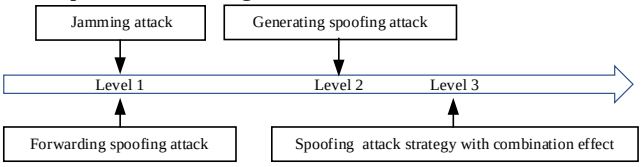

FIGURE 8. Ability level of spoofing techniques.

In Figure 8, Level 1 means that the spoofer only uses jamming attack or forwarding spoofing attack to implement spoofing process. Level 2 means that the spoofing party utilizes the generating spoofing attack to implement the spoofing process. Level 3 refers to the spoofing attack (forwarding spoofing attack or generating spoofing attack) carried out by the spoofer in combination with the spoofing strategy in Figure 4. At the same time, the spoofer also combines combinable spoofing scheme (as shown in Table VII) to perform combination of spoofing process. The combination of spoofing process is shown in Table VII. Since the ESA is based on pre-judging the content of the previous navigation message and generating a new navigation message, the ESA is classified as a generated spoofing attack.

Considering the technical difficulty and cost, this paper divides the implementation difficulty of the spoofing scheme into five levels (low, medium-low, medium-high, high, and extremely high). For the transmitter, the difficulty of internally adjusting the phase is consistent with the difficulty of adjusting the power. However, due to the high price of the high-power amplifier, the difficulty of the selective delay is less than the difficulty of the selective power. The power required to create a denial environment is higher, so the difficulty of achieving selective power is less than the difficulty of creating a denial environment. For nulling attack, its implementation is the most difficult. Therefore, the relationship between the difficulty of the spoofing attack is as follows: selective delay < selective power < create jamming < nulling attack.

From the perspective of the effectiveness of spoofing attacks, this paper is divided into four levels (Moderate, moderate-good, good, extremely good). The implementation effect of spoofing attacks is mainly considered from the combination of signal generation methods and spoofing methods. In general, the attack strength of a directly generated signal is less than the attack strength of the analysis. The reason is that the attack signal generated by the analysis is more suitable for the current spoofing environment and can improve the success rate of spoofing. In addition, the full channel spoofing effect is better than the single channel spoofing effect, so the full channel spoofing effect is the best. For spoofing methods, according to the previous analysis of multiple spoofing methods (title A of section II to title D of section II), the spoofing effect of selective delay and selective power is similar, and they are generally complementary. Both the nulling attack and the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

TABLE VII
SPOOFING COMBINATIONS

Spoofing method	Spoofing signal generation method	Combinable spoofing scheme (code)	Difficulty of implementation	Attack effect
Forwarding spoofing attack	Direct-replay spoofing attack [54]	Selective delay（A11）	Low	Moderate
		Selective power（A12）	Medium-low	Moderate
	Replay spoofing attacks based on multiple antenna receivers [6]	Selective delay（A21）	Medium-low	Moderate-good
		Selective power（A22）	Medium-high	Moderate-good
Generating spoofing attack	Direct-generation spoofing attack [45]	Selective delay（B11）	Medium-low	Moderate
		Selective power（B12）	Medium-high	Moderate
		Denial environment（B13）	Medium-high	Moderate-good
		Nulling attack（B14）	High	Good
	Analyze-generated spoofing attacks [46], [47]	Selective delay（B21）	Medium-low	Moderate-good
		Selective power（B22）	Medium-high	Moderate-good
		Denial environment（B23）	Medium-high	Moderate-good
		Nulling attack（B24）	High	Good
	SCER [36],[54]	Selective power（B31）	Medium-high	Moderate-good
		Denial environment（B32）	Medium-high	Moderate-good
		Nulling attack（B33）	High	Good
	FEA [55]	Selective delay（B41）	Medium-low	Moderate-good
		Selective power（B42）	Medium-high	Moderate-good
		Denial environment（B43）	Medium-high	Moderate-good
		Nulling attack（B44）	High	Good
	Full channel generated spoofing attack [14], [49]	Selective delay（B51）	Medium-high	Good
		Selective power（B52）	High	Good
		Denial environment（B53）	High	Good
		Nulling attack（B54）	Extremely High	Extremely good

cooperative interference attacks can cause the receiver to lose lock, but the nulling attack can also eliminate the information parameters of the authentic signal. Therefore, the effect of different spoofing attacks can be expressed as follows: selective delay ≈ selective power <create jamming <nulling attack.

III. ANALYSIS FOR SATELLITE NAVIGATION ANTI-SPOOFING TECHNOLOGY BASED ON SIGNAL-LEVEL

At present, many researchers have conducted a comprehensive research on the detection and suppression of spoofing attacks. Spoofing attacks can be detected in general terms, if there is no suppression of the satellite signal. The main goal of detecting spoofing is to distinguish the spoofing signal and the real satellite signal from the received signal. The spoofing signal cannot be considered into the navigation and positioning solution process and no suppression or elimination measures are taken for the spoofing signal. Suppression of spoofing refers to suppressing or eliminating spoofing on the basis of detecting the spoofing signal in the received signal, so that the spoofing signal does not affect the normal positioning and solving process of the real satellite signal. Currently there are main two kinds of methods for resisting spoofing attacks. One kind needs to add additional hardware facilities, such as based antenna arrays, based multi-correlator, based on signal arrival angle anti-spoofing interference method, etc.; another kind of spoofing detection or suppression methods are to identify and discover the spoofing signal for the signal parameters such as the signal power and the carrier-to-noise ratio of the received signal. Combined with the research results of researchers from various countries in recent years, the analysis and summary for the existing research techniques in this field are as follows.

As depicted in Figure 9, we categorize anti-spoofing techniques based on whether or not to use additional hardware. The additional hardware facilities independent anti-spoofing methods are subdivided into Doppler shift-based, Consistency check-based, Signal parameter statistics analysis-based, Arrival time and Arrival time difference-based and Residual signal detection-based subcategories. The anti-spoofing methods using additional hardware facilities are subdivided into Antenna array-based, angle of arrival-based, Subspace projection-based, Signal arrival direction-based and Signal quality monitoring-based. We discuss these categories in more details in follows.

A. EQUATIONS SPOOFING DETECTION METHOD BASED ON DOPPLER SHIFT

The relative motion between the navigation satellite that has been doing high-speed motion and the target receiver produces a Doppler shift. The receiver tracking unit tracks all satellite signals and forwards all signal parameters such as satellite signal amplitude, carrier-to-noise ratio, phase and Doppler shift to the spoofing detection unit. If the Doppler shift value of the satellite signal actually received by the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

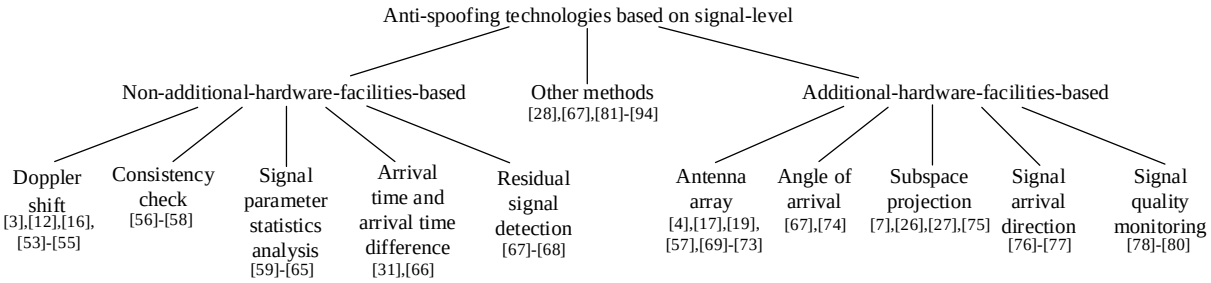

FIGURE 9. The categories of anti-spoofing technologies based on signal-level.

target receiver has a sudden change exceeding a preset threshold, it may indicates that the GNSS receiver is likely to have been subjected to a security threat of spoofing attack. Therefore, monitoring the Doppler shift change provides a good idea for defending against spoofing signals. Spoofing detection scenario based on Doppler shift as illustrated in Figure 10.

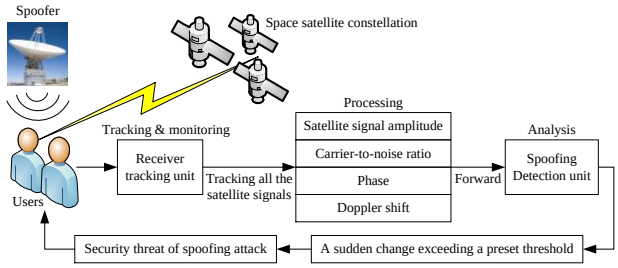

FIGURE 10. Spoofing detection scenario based on Doppler shift.

Jovanovic et al. proposed the concept of adaptive tracking algorithm, using Power Threshold Detector (PTD) and Doppler Offset Detector (DOD) to detect signal power variation and carrier Doppler shift respectively [17]. A statistical value check on both can successfully detect a replay attack. Zhang et al also analyzed anti-spoofing methods from this research perspective [57]. The proposed spoofing detection method uses the satellite signal amplitude and signal frequency difference between superimposed composite signal and the normal signal without spoofing in the tracking loop as spoofing detection evidence. The superimposed composite signal includes the spoofing signal and the real signal. Setting the signal power anomaly detection threshold and Doppler shift detection threshold respectively can detect the spoofing signal in the BeiDou satellite navigation signal. Qi et al. studied the carrier frequency variation process gathered by phase-locked loop of static receiver and phase-locked loop of dynamic receiver in the two scenarios and proposed a GNSS anti-spoofing method based on Doppler shift [58]. The one scenario is receiving only the real signal and the other is receiving the real signal and the spoofing signal.

The above methods are completed during the receiver tracking phase. Capturing satellite signals is a primary and important step in the processing progress for baseband signals. If spoofing can be effectively detected and suppressed during the signal acquisition phase, the receiver can be warned as early as possible to avoid the subsequent ignorance of the erroneous navigation and positioning solution. The following describes several anti-spoofing methods implemented during receivers' capture phase. Yuan et al. calculated the code and carrier Doppler shift of the real signal and the spoofing signal based on the Hough transform in the pre-capture process, and completed the joint consistency check process of the code and carrier Doppler shift [3]. The real signal and the spoofing signal are distinguished from the satellite signal. And then real signal parameters are transmitted to the receiver tracking loop. For detecting spoofing in combination with Doppler offset and satellite signal amplitude indicators, Broumandan et al conducted a worthwhile exploration to compare the amplitude and Doppler correlation characteristics measurements of different visible satellite signals and identified a single point source spoofing signal based on spatial correlation of signal parameters in a multipath interference environment [59]. Reference [13] proposed a novel method to identify and detect spoofing. The method calculated the Doppler frequency shift of each visible satellite carrier and continuously monitored the received satellite signal consistency and Doppler shift. Tu et al. proposed a spoofing detection technique based on frequency-domain bimodal and relative velocity residuals. This technique can not only detect spoofing, but also distinguish spoofing scenarios from multipath scenarios. They used the method of fast Fourier transform to detect the doublet and extract the Doppler difference of the doublet. In addition, they derived the relative velocity residual based on the Doppler difference through the above process, and compared it with the corresponding threshold to determine whether it was spoofed [60]. The analysis and summary for the spoofing detection methods based on Doppler shift is shown in Table VIII.

The Doppler shift is used as a satellite signal parameter due to the relative motion between the navigation satellite and the receiver, and the spoofing detection can be performed during the receiver capture or tracking. Analyzing Table VIII shows that some detection methods have certain application scenarios and are less adaptable to changeable spoofing scenarios. The reliability of anti-spoofing methods proposed in reference [57], [58] and [59] are influenced on spoofing detection in a flexible and variable spoofing environment. The spoofing detection performance for the method proposed in reference [17] is reliable in three different spoofing scenarios with only one spoofer, but it also

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

TABLE VIII
COMPARATIVE ANALYSIS OF ANTI-SPOOFING METHODS BASED ON DOPPLER SHIFT

Method	Characteristics	Defect	Required configuration	Implementation phase	Implementation difficulty	Performance metrics
Multi-test Detection and Protection Algorithm [17]	For spoofing attack of the receiver, the scheme monitors satellite signal characteristics from the perspective of signal physical characteristics and performs multiple statistic tests. Specifically, it estimates variance of the estimated value for Doppler shift and the carrier-to-noise ratio, and performs consistency test by position, velocity, and time to implement the proposed anti-spoofing method.	After the receiver detects the spoofing signal, it needs to switch to the protection mode and use the tracking history data to predict the tracking state. The receiver that completes the above process could recapture and track satellite signals. The accuracy for the prediction of the tracking status in the solution needs to be optimized and improved.	Power threshold detector and Doppler shift detector	Track	High	Total false alarm probability $2.27*10^{-8}$
BeiDou spoofing detection technology for signal power anomaly detection and Doppler shift [57]	The scheme analyzed the tracking stage model of BeiDou navigation signal system and analyzed the relationship between detection probability and false alarm probability for spoofing attack.	The method needs to consider the historical data of the carrier-to-noise ratio and the Doppler frequency shift. The reliability for the historical data is poor in some applications that have been subjected to a spoofing attack for a period of time.	Doppler frequency shift and satellite signal power anomaly detection capability	Track	Medium	Total false alarm probability $2.27*10^{-8}$
Anti-spoofing method based on Doppler shift [58]	The scheme performs spoofing detection from less consideration of extreme value influencing factors and considering all data influencing factors.	In the complex and variable spoofing environment, the reliability of the proposed solution could be affected.	Receiver with Doppler shift analysis capability	Track	Medium	Static receiver and dynamic receiver
Symbol and carrier Doppler joint consistency test [3]	The non-high-dynamic receiver using the anti-spoofing method can detect and suppress one or more spoofing signals while performing satellite signal acquisition normally.	This scheme could increase the computational complexity, and the reliability of spoofing detection and suppression performance for high dynamic mobile receiver reliability is poor.	Receiver capture module needs to be modified.	Capture	Low	Pre-acquisition, doppler calculation performance evaluation is effective.
Spoofing detection based on Doppler offset and satellite signal amplitude indicators [59]	Different satellite navigation signals transmitted by a single spoofing signal transmitter have the same spatial characteristics, while space characteristics of the real satellite signal are different. It is used as the basic principle of spoofing detection.	The method can effectively detect the spoofing signal transmitted by a single spoofing interference source. The spoofing detecting performance for the method is affected when multiple spoofing sources exist simultaneously.	Receiver needs to continuously monitor signal amplitude and Doppler shift value.	Capture and track	Medium	Doppler calculation performance evaluation is not affected by spatial multi path fading.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

Doppler shift detection [13]	The scheme uses Doppler shift to monitor the operation and integrity of satellite signals.	Technology cost and solution complexity could be increased, and the solution reliability could be affected when the sampling rate is low.	Continuously monitoring signal consistency and Doppler shift ability	Capture	High	The method is demonstrated to work accurately provided that the sampling rate is fast enough, typically of the order of 1 Hz.
Frequency domain bimodal and relative velocity residuals [60]	This method is based on fast Fourier transform to detect double peaks in the frequency domain of the signal, then they calculate Doppler differences based on the obtained double peaks, and finally they derive the relative velocity residuals based on the Doppler differences.	This method is not ideal for resisting general deception and advanced deception, and the technical cost of this method is relatively high.	FFT module, relative speed calculation module, decision module	Track	Medium	The spoofing detection probability is the product of dual-peak detection probability and relative velocity solution residual detection probability.

brings certain program complexity and increases implementation cost. The symbol and carrier Doppler joint consistency test method proposed in reference [3] increases the computational complexity, but the method can ensure the authenticity of the received satellite signal by slightly modifying the capture module of the existing receiver while using the lesser cost to capture the satellite signal normally. The resistance effect analysis for anti-spoofing methods based on Doppler shift is shown in Table IX.

TABLE IX
THE RESISTANCE EFFECT ANALYSIS FOR ANTI-SPOOFING METHODS BASED ON DOPPLER SHIFT

Schemes	Selective power spoofing	Selective delay spoofing	Nulling attack	Denial environment
Multi-test Detection and Protection Algorithm [17]	Good	Moderate	Poor	Moderate
BeiDou spoofing detection technology for signal power anomaly detection and Doppler shift [57]	Good	Moderate	Poor	Poor
Anti-spoofing method based on Doppler shift [58]	Moderate	Moderate	Poor	Poor
Symbol and carrier Doppler joint consistency test [3]	Moderate	Moderate	Poor	Moderate
Spoofing detection based on Doppler offset and satellite signal amplitude indicators [59]	Good	Moderate	Poor	Poor
Doppler shift detection [13]	Moderate	Good	Poor	Poor
Frequency domain bimodal and relative velocity residuals [60]	Moderate	Good	Poor	Poor

Table IX shows the anti-spoofing performance for spoofing detection method based on Doppler shift. The term "resistance" is an ability to resist spoofing attacks. The methods continuously monitor for signal parameters such as signal power and Doppler shift. Selective power spoofing and selective delay spoofing respectively perform spoofing attacks on the satellite signals by artificially adding signal delay and artificially increasing the signal power. The method can identify the two kinds of spoofing attacks in a timely manner while continuously monitoring the signal-related parameters, but the detection performance against nulling attack and denial environment is poor.

The methods proposed in reference [17], [57] and [59] can identify selective power spoofing signals and selective delay spoofing signals in the received signal including spoofing signal and the real satellite signal according to variety for the carrier-to-noise ratio, signal amplitude index, and signal power of received signal. For nulling attack and denial environment, the spoofing detection method based on the signal Doppler shift parameter has weak ability to identify and eliminate it. Comparing Table VIII and Table IX, it can be found that the spoofing detection method proposed in reference [13] increases difficulty and cost of implementation, but the adaptability for satellite signal transmission environment with spoofing is better than other methods. The detection methods of spoofing signals proposed in reference [17] and [3] are respectively implemented by statistical test and joint consistency test, and the resistance performance to denial environment is better than other methods.

B. SPOOGING DETECTION METHOD BASED ON CONSISTENCY CHECK

Figure 11 presents the signal parameters of navigation satellite signal and the navigation information carried by the satellite signal are consistent in the clearing scene without spoofing. The signal parameters of the composite signal for the spoofing signal and the real satellite signal may jump or exceed the normal reasonable range. According to the abnormal changes of these signal parameters or indicators and differences between the spoofing scene and the normal

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

transmission environment, the effective detection for the spoofing signal can be realized.

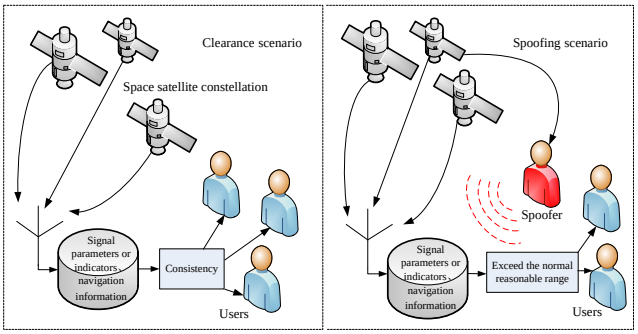

FIGURE 11. Spoofing and spoofing detection scenario based on consistency check.

The single antenna spoofing signal compared with the real satellite signal has the mapping characteristics of region to the single point on coordinate system. Yao et al. used this as the basis of spoofing detection, and proposed anti-spoofing method on information consistency of the received signals at several observation points in the monitoring area [61]. The method improves the spoofing detection performance by multi-node information. The method proposed in the reference [62] uses the receiver mobile antenna to authenticate signal, and detects high correlation of the corresponding amplitude, phase and Doppler changes according to the channel response of the receiver's mobile antenna during the receiver tracking phase. In the positioning navigation phase, spoofing signal can be detected at a position observable for the mobile receiver level. Coupling IMU with GNSS measurements and integrating user motion mode into the detection and classification problem for spoofing can improve the detection performance of spoofing. Network-based or cloud-based satellite signal authenticity verification method assumes that there is a lower rate communication link among receivers, or that the transmitted measurement data can be stored by the cloud [62][8]. And several operating independently receivers operate within this range. The measured values could be shared, and the carrier phase double difference between the real signal and the spoofing signal can be separated to detect a spoofing attack. Compared with the former two methods, Wesson et al. proposed a spoofing detection method for authenticating satellite signals by power and distortion detection technology, which can distinguish interference-free, multipath interference, low-power spoofing with high probability [63]. The analysis and comparison for the characteristics on this type of spoofing detection methods are shown in Table X.As shown in Table X, the methods based on information consistency check and based on power and distortion monitoring technology are suitable for some stable spoofing scenarios. The resistance with many changes or multi-antenna spoofing environment is less effective.

TABLE X
COMPARATIVE ANALYSIS OF SPOOFING DETECTION METHODS BASED ON CONSISTENCY CHECK

Method	Characteristics	Defect	Required configuration	Implementation phase	Implementation difficulty	Performance metrics
Spoofing detection method based on information consistency check [61]	The single-antenna spoofing has a mapping feature for area to a single point of the coordinate system. The receivers consider the character as the basis of spoofing, and perform spoofing detection according to multi-node information.	This method may be less adaptable to multi-antenna spoofing scenarios.	Receiver with multi-node information monitoring capability	Capture and track	Medium	Average position of ublox receiver
Spoofing detection method based on correlation of signal amplitude and phase change [62]	For receiver tracking phase and the positioning solution phase, different spoofing detection methods are adopted to continuously collect spatial features for a period of time.	Modifications to the receiver capture and tracking module are required. The detection performance for this method is affected by antenna motion and oscillator stability.	Single mobile receiver antenna	Track and positioning phase	High	Authentic and spoofing average SNR values
Satellite signal authenticity verification method Based network or cloud [62]	The anti-spoofing method utilizes a zero-slope time variation characteristic on a carrier phase double difference of a spoofing signal to perform spoofing detection.	The extra servers required for this solution could increase the hardware implementation complexity and cost.	High-power processing server that requires data transmission networks and analyzes big data.	Tracking and navigation positioning phase	High	Carrier phase double difference
Power and distortion monitoring technology [63]	This method does not need to rely on external hardware or network connections but is implemented through updating firmware.	Since the satellite signal power itself may change with the environment, it is difficult to apply in the variable spoofing scenario.	PD detector	Tracking phase	Medium	Power-distortion detector

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

In response to this problem, the spoofing detection method based on the correlation of signal amplitude and phase change proposed in the reference [62] and the verification method of satellite signal authenticity based on network or cloud make up for this defect. The above two methods respectively use different working characteristics for different processing stages of the receiver and combine with spatial features to better adapt to different spoofing scenarios. The methods improve the feasibility of identifying and discovering spoofing, and also propose requirement for configuring additional mobile receiver antennas or processing sever to satellite signal receivers, which is relatively difficult. The comparison of the anti-spoofing performance for the spoofing detection methods based on the consistency check is shown in Table XI.

TABLE XI
COMPARISON OF ANTI-SPOOFING METHOD PERFORMANCE BASED ON CONSISTENCY TEST

Schemes	Selective power spoofing	Selective delay spoofing	Nulling attack	Denial environment
Spoofing detection method based on information consistency check [61]	Moderate	Moderate	Poor	Poor
Spoofing detection method based on correlation of signal amplitude and phase change [62]	Good	Moderate	Good	Moderate
Satellite signal authenticity verification method based network or cloud [62]	Moderate	Good	Poor	Moderate
Power and distortion monitoring technology [63]	Moderate	Good	Poor	Poor

As can be seen from the analysis in Table XII, the spoofing detection method based on information consistency check proposed in reference [61] finds the spoofing based on the fact that the spoofing signal transmitted by the single antenna spoofing transmitter has the coordinate system mapping characteristics. The method with a good detection capability for forwarding spoofing attack fails to effectively eliminate the spoofing signal. The detection performance for the selective power spoofing and the selective delay spoofing is moderate. The two methods proposed in reference [62] can continuously monitor the power of the signal and the delay of the signal by collecting the spatial characteristics and time-varying characteristics of received signals, so that the selective power spoofing and selective delay spoofing can be distinguished in a timely manner. The spoofing detection method based on the correlation between signal amplitude and phase change detects the consistency among signal parameters such as the amplitude, phase and Doppler shift of the satellite signal through the receiver antenna in the moving state, and authenticates satellite signals. The method can detect the abnormal situation caused by nulling attack, and the detection performance for spoofing in the environment of denial environment is better than other methods.

C. SPOOGING DETECTION METHOD BASED ON SIGNAL PARAMETER STATISTICSANALYSIS

The variable analysis method used in statistical theory to test data can be applied to the field of GNSS spoofing detection. As it is illustrated in Figure 12, based on the characteristics that the signal parameter statistics are difficult to forge, the scheme uses statistical methods such as sample mean value test, square sum, variance, maximum likelihood estimation test, and adopts methods such as setting decision threshold and decision statistic to complete the effective recognition process of spoofing, combining parameters such as phase space feature and carrier phase measurements.

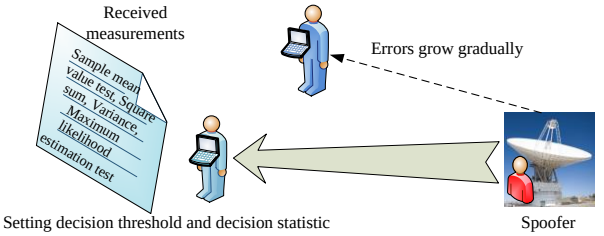

FIGURE 12. Spoofing detection scenario based on signal parameter statistics analysis.

Many scholars at home and abroad have proposed a method of spoofing detection based on statistical analysis. Borio proposed a new phase variance analysis (PANOVA) test method in 2013, under the assumption of known average amplitude and unknown average amplitude [64]. By detecting the difference in sample mean value, phase spatial characteristics of the satellite signal are identified to achieve effective detection for spoofing attacks. Borio and Gioia conducted follow-up research in this research field. In 2016, Sum-of-Squares (SoS)-based angle-of-arrival spoofing detection method was proposed. The generalized likelihood ratio test (GLRT) method was used to realize the square sum detector. The SoS decision statistic is calculated using the carrier phase measurements of two spatially separated GNSS receivers. A carrier phase single difference square sum detector that can be expressed as a correction to the pseudo code and its integer portion is designed. This method simplifies the decision threshold criterion and does not require spoofing location or antenna calibration process. It can be applied to occasions with high real-time requirements [65].

Falletti et al. proposed a practical spoofing detection method based on post-correlation, and proved effectiveness in detecting spoofing signals through a series of static and dynamic field experiments [66]. In the navigation and positioning solution, the navigation satellites subjected to spoofing attacks adopt a strategy for eliminating and reduce the misleading effect on the navigation results of spoofing

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

satellite signals. Hwang et al. proposed a receiver autonomous signal authentication method, which uses the receiver's estimated clock state Allan variance to analyze the clock stability of the receiver in a short time and determined whether there is a dynamic spoofing caused by relative motion between the spoofing source and the GNSS receiver [67]. Yuan et al. from Tsinghua University proposed that the GNSS spoofing detection method based on the sequence probability ratio test does not need to predetermine the required number of observations [68]. Compared with the reliable detection method based on the predetermined number of observations, the number of required observations can be greatly reduced. Maximum Likelihood Estimation (MLE), which utilizes the consistency between different navigation satellites, has been widely used in receiver direct position estimation and can be used to suppress spoofing attacks. Wang et al. solved the problem of finding the optimal MLE solution, and solved the premature convergence problem of the basic particle swarm optimization algorithm by using attractive and repulsive particle swarm optimization (ARPSO) [69]. Gross et al. conducted a more in-depth study on this problem, using the method for fitting the residual of the maximum likelihood estimation based on the single-signal correlation function model instead of the PD detector-based symmetric differential distortion measurement method [70]. The improved technology is called PD-ML detector, which significantly improves the performance of spoofing recognition in multipath interference environments. The prior art technique for detecting spoofing based on signal parameter statistics analysis is as shown in Table XII.

It can be seen from the analysis in Table XII that this type of spoofing detection method usually needs to be combined with other spoofing detection methods to ensure anti-spoofing performance. Some methods are only applicable to specific spoofing scenarios, and the applicability of all spoofing scenarios is poor.

TABLE XII
ANALYSIS AND COMPARISON FOR SPOOFING DETECTION METHODS BASED ON STATISTICAL ANALYSIS OF SIGNAL PARAMETERS

Method	Characteristics	Defect	Required configuration	Implementation phase	Implementation difficulty
Spoofing detection method based on phase variance analysis [64]	The scheme uses the generalized likelihood ratio test method to derive decision statistics and provides approximate criteria for setting decision thresholds.	The spoofing detection performance for the method is poor when the maximum value of the available phase value is small.	Receivers need to add dual antenna system.	Capture	Medium
Spoofing detection method based on square sum [65]	The decision statistic is calculated using spatially separated receiver carrier phase measurements. The scheme derives detector classification method based on generalized likelihood ratio test and models random variables	In some spoofing environments, the spoofing detection performance for the method is poorly reliable.	The receiver needs to configure the antenna array.	Capture and track	Low
Spoofing signal detection method based Post-correlation [66]	The scheme considers static scenarios and dynamic scenarios. After appropriate improvement of the method, multipath interference and deception interference can be distinguished.	The method has a certain complexity, and the spoofing detection is ineffective in the spoofing scene with high real-time requirements.	Receivers need to have post-related inspection capabilities.	Capture	High
Receiver autonomous signal authentication method [67]	The scheme detects whether spoofing exists according to the estimated clock stability of the receiver.	This method needs to combine other detection methods or means to ensure the authenticity of the measured values.	Target receiver is moving.	Capture and track	Low
Spoof detection method based on sequence probability ratio test [68]	The scheme detects spoofing based on the relationship among the average spoofing detection time, the probability of spoofing detection, the false alarm probability, the signal-to-noise ratio, and the ratio of spoofing to the true signal.	The detection performance for the power of spoofing signal similar to the power of the real satellite signal is affected to some extent, and combined detection with other detection methods is also required.	Receivers need to have sequence probability ratio test capability.	Capture	Medium
Anti-spoofing method based on ARPSO-MLE [69]	The scheme uses particle swarm optimization and spatial interaction generalized expectation maximization algorithm (SAGE) for multimodal optimization.	This method is less stable against spoofing attacks at lower signal-to-noise ratios.	Receiver with ARPSO-MLE based position estimation capability.	Capture	Medium
PD-ML detector technology [70]	The scheme can accurately identify spoofing in the environment where satellite signals and interference signals coexist.	This method increases computational complexity and technical cost, lack of sensitivity assessment for applications with narrow front-end bandwidth receivers.	The maximum likelihood multipath interference estimator is required inside the receiver.	Track	High

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

The square-based angle-of-arrival spoofing detection method uses a generalized likelihood ratio test to eliminate the need for accurately locating the spoofing source location or performing antenna calibration. The method can detect selective power spoofing and nulling attack spoofing in the receiver acquisition and tracking phase with lower implementation difficulty. The spoofing detection methods proposed in reference [64], [68] and [69] respectively use statistical analysis such as phase variance and sequence probability ratio test to improve the feasibility in spoofing environment. The above several anti-spoofing methods are applied in the static spoofing environment, while the reference [66] considers both the static spoofing environment and the dynamic spoofing environment, and eliminates the satellite navigation signals that are subject to spoofing attacks. While solving the problem of spoofing detection in the more complex spoofing environment, it also brings the technical difficulty and the realization cost of anti-spoofing method. The anti-spoofing performance based on the signal parameter statistical analysis is summarized in Table XIII.

Analyzing Table XII and Table XIII shows this method continuously monitors signal power or signal delay during spoofing detection process, while the spoofing implementation process of selective power spoofing and selective delay spoofing gradually changes the signal power and the delay to complete the spoofing attack. So, the spoofing detection method based on the signal statistic has better resistance to selective power spoofing and selective delay spoofing. The square-based angle-of-arrival spoofing detection method proposed in reference [65] uses the antenna array to detect direction of the signal arriving at the antenna array, and can detect nulling attack. The difficulty for this kind of method to detect the denial environment signal in spoofing environment where denial environment signal and the real satellite signal coexist through the statistical analysis for the signal parameters is smaller than other methods. The anti-spoofing methods in reference [64] and [65] analyze the phase change and carrier phase of satellite signals, and find selective delay spoofing whose phase gradually approaches towards spoofing more easily and timely in the monitoring process of continuously paying attention to whether the signal phase exceeds the range on reasonable variation. So the two spoofing detection methods are more stable than the other methods of this kind for the detection performance of selective delay spoofing.

TABLE XIII
ANTI-SPOOFING EFFECT INDUCTION BASED ON SIGNAL PARAMETER STATISTICAL ANALYSIS

Schemes	Selective power spoofing	Selective delay spoofing	Nulling attack	Denial environment
Spoofing detection method based on phase variance analysis [64]	Moderate	Good	Moderate	Poor
Spoofing detection method based on square sum [65]	Moderate	Good	Good	Moderate
Spoofing signal detection method based Post-correlation [66]	Good	Moderate	Poor	Poor
Receiver autonomous signal authentication method [67]	Moderate	Moderate	Poor	Poor
Spoofing detection method based on sequence probability ratio test [68]	Good	Moderate	Poor	Poor
Anti-spoofing method based on ARPSO-MLE [69]	Moderate	Moderate	Poor	Poor
PD-ML detector technology [70]	Moderate	Moderate	Poor	Good

D. SPOOGING DETECTION METHOD BASED ON ARRIVAL TIME AND ARRIVAL TIME DIFFERENCE

As it is illustrated in Figure 13, the signal transmission distance (S1) and time (T1) from real satellite that broadcast satellite signals to the forward-type spoofing source plus the signal transmission distance (S2) and time (T2) from forward-type spoofing source to the target receiver is inevitably longer than the transmission distance (S3) and transmission time (T3) of the satellite signal directly transmitted from the real satellite to the target receiver. This is because the forward-style spoofing signal needs to pass a certain delay time to transmit a longer path reaching the receiver. If the time difference among satellite signals reaching the phase center of the receivers' target antenna is outside the reasonable range, then receiving signal is likely to be a composite signal of spoofing signal and real satellite signal. At present, there are many researches on the detection methods of spoofing, and there are a few researches on the spoofing location as important as spoofing detection. In fact, it is very necessary to locate source of spoofing, because accurately locating spoofing source is of benefit to identifying and eliminating spoofer.

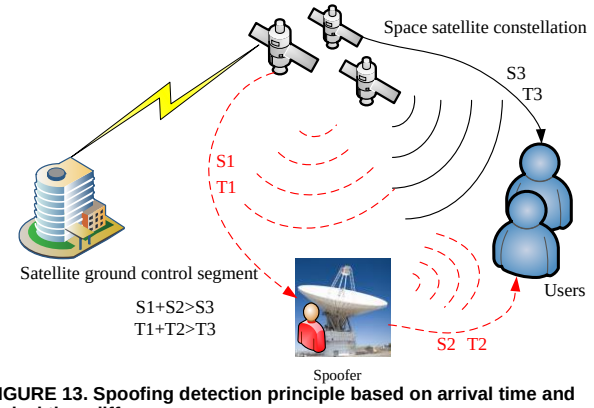

FIGURE 13. Spoofing detection principle based on arrival time and arrival time difference.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

The method of locating the spoofing is mainly based on the estimation for the time difference of arrival, and the time difference of arrival is usually measured based on the signal cross-correlation relationship. Zhang et al proposed a spoofing TDOA estimation method based on differential code phase (DCP), and established a DCP-based TDOA model and its estimation error model [71]. This method has higher precision and better performance than the current methods. Because the power level of the intermediate spoofing is only slightly higher than the power level of the real signal, the anti-spoofing method based on the power detection fails, and it is difficult to perform the real-time intermediate spoofing detection by using other existing anti-spoofing methods. In response to this problem, Li et al. can determine the peak value of tracking signal obtained by the satellite signal acquisition module during the acquisition process, using a multi-modal detection method that exceeds the number of threshold correlation peaks at any signal interval [33]. The scheme utilizes a multimodal detection method that exceeds the number of threshold correlation peaks to determine whether there is a spoofing signal and gives an evaluation criteria definition, a performance evaluation method, and an empirical formula. A comparative analysis for the spoofing detection methods based on arrival time and arrival time difference is shown in Table XIV.

Table XIV shows that spoofing source receives the satellite signals transmitted by the real satellites. After a delay time, the transmission time of the forwarded spoofing signal transmitted to the victim receiver is longer than the satellite signal transmission time from the navigation satellite to the target receiver. According to the difference for the arrival time of the satellite signal arriving at the phase center of the receiver antenna, authenticity of the navigation result can be discriminated. However, the method generally has better detection effect on the receiver in the stationary state. In comparison, detection performance for dynamic spoofing needs to be improved. The anti-spoofing performance based on the arrival time and the arrival time difference is shown in Table XV.

TABLE XIV
COMPARATIVE ANALYSIS OF FRAUD DETECTION METHODS BASED ON ARRIVAL TIME AND ARRIVAL TIME DIFFERENCE

Method	Characteristics	Defect	Required configuration	Implementation phase	Implementation difficulty
Spoofing localization method based on differential code phase [71]	The scheme uses the satellite signal cross-correlation relationship to measure the arrival time difference estimation of spoofing signal, and performs higher-precision spoofing location	The scheme has better performance on the detection of spoofing in static receivers and has poor adaptability to scenes of spoofing in dynamic receivers.	Receiver needs to add dual antenna system	Capture	Medium
Multimodal spoofing detection method [33]	The scheme compares the peak-to-peak value of the captured satellite signal with a preset threshold, and identifies spoofing based on the number of correlation peaks exceeding the threshold.	At present, the spoofing detection performance of this method in atypical cases such as low carrier-to-noise ratio and high spoofing signal ratio is not very stable.	Receivers need to configure multi-correlator	Capture	Low

TABLE XV
COMPARISON OF ANTI-SPOOFING EFFECT BASED ON ARRIVAL TIME AND TIME DIFFERENCE OF ARRIVAL

Schemes	Selective power spoofing	Selective delay spoofing	Nulling attack	Denial environment
Spoofing localization method based on differential code phase [71]	Moderate	Good	Moderate	Poor
Multimodal spoofing detection method [33]	Good	Moderate	Poor	Poor

The spoofing detection method based on signal arrival time essentially uses the signal transmission time difference between spoofing signal and the real satellite signal as the basis for spoofing detection, and usually judges whether there is spoofing by monitoring the signal delay and the signal power change. In the process of performing selective delay spoofing and selective power spoofing on the target receiver, the signal delay and power variation process are slowly controlled to prevent the receiver from being alerted. Therefore, the method continuously monitors the signal power and signal delay simultaneously. It can be confirmed whether the receiver is subject to selective power spoofing or selective delay spoofing. Denial environment sending large-scale interference causes the receiver to lose tracking accuracy to complete the receiver spoofing process. The anti-spoofing method based on the arrival time and the arrival time difference generally performs the spoofing detection in the receiver acquisition phase. Denial environment expands spoofing process after capturing the satellite signal, so the method cannot detect and suppress denial environment.

E. RESIDUAL SIGNAL DETECTION

When receiver receives spoofing signal, it is difficult to completely eliminate the real satellite signal. Under the assumption that the spoofing attack cannot effectively suppress real satellite navigation signal, the residual real

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

TABLE XVI
COMPARISON OF RESIDUAL SIGNAL FRAUD DETECTION METHODS

Method	Characteristics	Defect	Required configuration	Implementation phase	Implementation difficulty
Residual signal detection [72]	The satellite signal received by the receiver subjected to the spoofing attack contains the real signal, and the residual real satellite signal is used for the spoofing detection.	The power of the spoofing signal is usually higher than the power of the real satellite signal, making it difficult to detect the residual real signal and increasing the amount of calculation.	The receiver requires additional satellite signal tracking channels (additional multiple channels).	Capture and track	High
Signal quality monitoring technology and residual signal monitoring joint spoofing detection method [73]	The scheme analyzes the cause of the correlation peak distortion shape and determines whether the distortion is caused by multipath interference or spoofing. The specific method is to evaluate the quality of the correlation function for residual real signal detection.	This method needs to combine two kinds of spoofing detection technologies, and the specific implementation process has certain complexity.	The scheme needs a pair of additional correlators.	Capture and track	Medium
Spoofing profile estimation-based GNSS spoofing identification method [74]	This method uses the characteristics of residual distortion of extended Kalman filter due to spoofing attacks, reconstructs the spoofing profile in reverse and identifys the spoofing. The authors developed an iterative implementation based on the spoofing peofile estimation method to reduce the computational overhead.	The method increases the technical cost and complexity of the solution	Tightly coupled MEMS INS/GNSS integrated navigation system	Track	High

signal component can be utilized to complete the residual signal detection process for the spoofing signal in the received signal. As depicted in Figure 14 [66], the residual signal detection is performed during receiver acquisition phase in order to detect whether there is a spoofing signal of a certain satellite in current received signal at initial startup. Residual signal detection during the tracking phase is to detect spoofing in real time that may be present in the receiver that has tracked the real satellite signal.

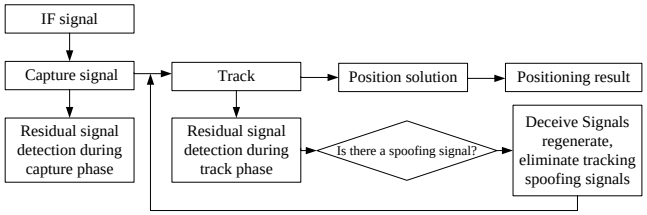

FIGURE 14. Residual signal detection block diagram.

Under the premise that the receiver subjected to spoofing attack can still detect the spoofing signal and the real satellite signal, the residual signal detection method in the capturing phase and the tracking phase can be used to detect spoofing of the current received signal, and extract the signal parameters to complete spoofing signal regeneration and elimination [72]. Ali et al. proposed a spoofing detection algorithm that uses joint signal quality monitoring techniques and residual signal monitoring [73]. The correlation function distortion caused by multipath interference and spoofing is distinguished by two indicators based on the ratio metric and a pair of additional correlators, and the correlation function quality is evaluated to detect the residual signal. Wei et al. proposed a spoofing profile estimation-based GNSS spoofing identification method for tightly coupled MEMS INS/GNSS integrated navigation system. This method uses the characteristics of residual distortion of extended Kalman filter due to spoofing attacks, reconstructs the spoofing profile in reverse and identifies the spoofing [74]. A comparative analysis of residual signal spoofing detection methods is shown in Table XVI.

Analyzing the above table, the signal power of the spoofing signal is usually greater than the signal power of the real satellite signal, making it easier for the receiver tracking loop to track the spoofing signal. Therefore, using a real signal component that is weaker than the spoofing signal to detect the spoofing signal increases the technical difficulty and the amount of calculation, or adds additional tracking channels. Reference [73] provides a certain solution to this problem. Combined with signal quality monitoring technology, the feasibility of this method is improved to some extent.

TABLE XVII
COMPARISON FOR ANTI-SPOOFING EFFECTS OF RESIDUAL SIGNAL SPOOFING DETECTION METHOD

Schemes	Selective power spoofing	Selective delay spoofing	Nulling attack	Denial environment
Residual signal detection [72]	Good	Moderate	Poor	Poor
Signal quality monitoring technology and residual signal monitoring joint spoofing detection method [73]	Good	Moderate	Poor	Moderate
Spoofing profile estimation-based GNSS spoofing identification method [74]	Good	Moderate	Moderate	Moderate

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

It can be seen from Table XVI and Table XVII that the residual signal spoofing detecting method uses received composite signal of the spoofing signal and the real satellite signal to perform residual signal detection for spoofing signal. If spoofer wants to suppress real signals, spoofing needs to synchronize with the real satellite signal in order to achieve certain accuracy. This synchronization process requires that the 3D position for spoofing source and phase center of receiver antenna must be known, which is very difficult in practical operation. Therefore, although the target receiver suffers from a spoofing attack, the real satellite signal can still be detected. The target receiver adopting signal quality monitoring technology can effectively identify selective power spoofing by using monitored power variation of satellite signal received. The method has average performance of selective delay spoofing detection, and the detection performance for denial environment is poor. The method proposed in reference [73] combined with signal quality monitoring technology and residual signal monitoring technology, compared with the method proposed in reference [72], provides more possibilities for effectively detecting denial environment..

F. SPOOFING DETECTION METHOD BASED ON ANTENNA ARRAY

Spoofing detection method based on antenna arrays utilizes spatial filtering techniques to form a received signal beam. This method provides a gain for a specific angle and attenuates a specific spatial sector. It is a practical and effective anti-spoofing method in static and dynamic spoofing scenarios. The method is based on the assumption that the spoofing signals arriving at the antenna array are all from the same direction, but the real satellite signals arriving at the antenna array have spatial characteristics from different directions as it is illustrated in Figure 15. Implementation of this method typically requires additional hardware and even requires correction of the antenna array and some degree of change to the receiver architecture during the capture and tracking phases.

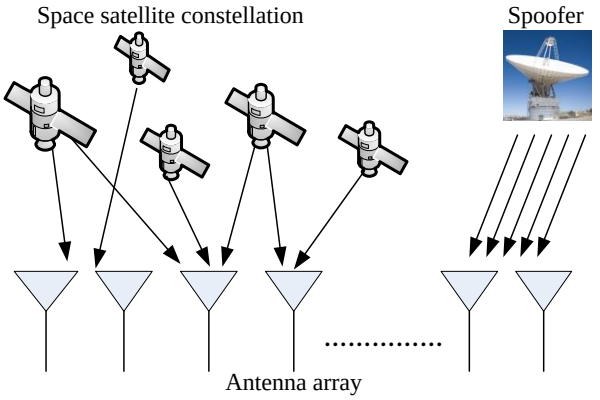

FIGURE 15. The assumption for spoofing detection method based on antenna array

Felski proposed that independent receiving device covered by the antenna beam sector determines navigation parameters, and ignores the information that is inconsistent with parameter information of other navigation monitoring devices in the navigation and positioning solution [75]. The method circumvents the effects of spoofing signals by adding some built-in mechanisms such as special digital hardware and software-controlled multi-element antenna arrays. Hu et al. proposed an array-based blind adaptive array signal processing method [20]. This method not only can adaptively form deep nulls in non-periodic interference, periodic interference and spoofing attack DOA, but also can mitigate in-band spoofing and enhance useful signals. Jiang et al. proposed a method for detecting spoofing based on statistical analysis of baseline data, considering three cases for single fixed baseline, fixed and independent baseline and double independent baseline Max/Min model, and analyzed influence of the baseline values on detection performance [18]. If the dual antennas are out of synchronous, other spoofing detection methods are likely to fail, but the differential power ratio can still be used to spoofing detection. The pseudorange and carrier phase measurement asynchronous models and spoofing detection method proposed by Wang et al. based on dual antenna power measurement can detect spoofing in non-synchronous situations [4]. In different environments of the actual satellite signal transmission process, it may be difficult to use only one anti-spoofing method to cope with the simultaneous existence of various interferences. Chinese Taiwanese scholar Chang proposed a multiplexing scheme that can adaptively respond to various forms of interference, and can perform four internal processing modes according to different environmental conditions, which can detect, identify, mitigate or eliminate spoofing/co-channel interference and continuous wave interference (CWI) [76].Wang et al. calculated the power of spoofing signal by repetitively performing the CLEAN algorithm to estimate the direction and complex amplitude of a spoofing until all spoofing were estimated [77]. This scheme estimates the power of real satellite signal by estimating the direction and complex amplitude of real satellite signal. Each signal source estimated by the CLEAN algorithm can be used to assisting information to detect spoofing.

The above several methods of detecting spoofing are to realize the identification and discovery of spoofing signals in the process of capturing or tracking by the receiver. The following three methods are the spoofing detection process completed in the despreading phase of the receiver. Under the assumption that spoofing signal comes from the same spoofing source, Daneshmand et al. proposed a spoofing suppression method that extracts the steering vector of the spoofing signal and discards the spoofing signal before the receiver despreading [78]. In the whole process of spoofing detection and suppression, the array processing is performed at the pre-despreading phase, and there is no need to track the pseudo-random code of all the spoofing signals and the real signals. The approach extracts the spatial characteristics on

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

the spoofing signal to eliminate the spoofing correlation peak and weaken the noise level caused by spoofing. At the same time, the method extends the antenna output portion to maximize the signal-to-noise ratio of a single real signal. Ge et al. proposed an anti-spoofing method for null-time multi-antenna nulling of the multipath reflection signal of the spoofing signal [79]. The method improves outer-product decomposition algorithm to suppress the spoofing signal and its multipath interference component and proposes a "threshold detection method". The blind pre-despreading technique is an effective and low-complexity spoofing suppression method. The spoofing detection method proposed in the reference [62] does not need to perform array calibration and change the receiver structure in the pre-despreading stage, which reduces the computational complexity. And in the post-despreading phase, the scheme needs to be considered in two cases. This method can effectively detect low-power and high-power spoofing attacks [62]. A simple analysis of anti-spoofing techniques based on antenna arrays is as shown in Table XVIII.

Table XVIII shows that the antenna array-based spoofing detection method analyzes the spatial characteristics of the received navigation signal and identifies the spoofing signal that arrives at the antenna array in the spatial domain. Implementing this method requires configuring the antenna array for the receiver, and the technical cost and hardware implementation complexity can be increased. Different processing measures can be taken at different stages of the receiver to detect spoofing signals. Due to current technology and cost constraints, most spoofing signals of multiple navigation satellites in the spoofing environment are currently transmitted by the same interference source. This kind of method can effectively detect the spoofing signal in such a spoofing environment, but the spoofing detection of the cooperative spoofing scene for multiple interference sources needs further research.

TABLE XVIII
COMPARATIVE ANALYSIS OF ANTI-SPOOFING TECHNIQUES BASED ON ANTENNA ARRAYS

Method	Characteristics	Defect	Required configuration	Implementation phase	Implementation difficulty
Anti-spoofing interference method for GNSS receivers [75]	Different anti-spoofing interference measures are adopted for different processing stages of the receiver. The method improves the analog-to-digital converter resolution by simulating filtering and automatic gain control in the RF section. Based on the above operations, the scheme reduces the out-of-band interference and suppresses the interference signal by using the mechanism of digital signal processing before the pre-de-spreading process	The scheme needs to add additional digital hardware and multi-element antenna arrays, which increases the cost of certain hardware	Digital hardware, multi-element antenna arrays and antennas with software-defined radio technology or receiver is needed to configure	Capture and track	Low
Blind adaptive array signal processing method [20]	Blind adaptive array signal processing based on array antennas is implemented by a software program integrated into the array antenna. This method does not require adjustment of hardware facilities and is compatible with the receiver.	The adaptive performance for this method applied in multipath interference environment can be affected, and the reliability needs to be optimized.	Array antenna processing capability	Capture	Medium
Baseline data statistical analysis spoofing detection method [18]	According to the number of baselines and different states, the performance for spoofing detection of the method is analyzed in three different situations.	The effectiveness of spoofing detection is not guaranteed for the first two cases when the baseline correlation is not considered.	Receiver needs to have baseline data statistical analysis capabilities	Capture and track	Medium
Spoofing detection method for dual antenna power measurement [4]	The scheme is applicable to the case of dual antenna non-synchronization, using the generalized likelihood ratio test method for research.	The spoofing detection method needs to increase the number of antennas, technical difficulty and cost.	The receiver needs to be configured with dual antennas.	Capture	High
Satellite navigation receiver anti-spoofing scheme [76]	According to different environmental conditions, the method combines with adaptive antenna array technology, frequency removal technology, interference detection technology and decision logic technology and implemented four internal processing modes.	This method belongs to the multiplex anti-spoofing method, and the scheme complexity is high.	Receivers need to have adaptive antenna array technology, frequency removal technology and decision logic technology.	Capture and track	High
Spoofing suppression method using periodic repeat CLEAN [77]	The scheme estimates the direction and number of the spoofing source, using the spoofing space and power characteristics without the receiver feedback information	The method is less adaptable for spoofing scenarios, and reliability is likely to be affected in some spoofing environments.	The antenna array is needed to configure	Capture	Low

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

Anti-spoofing method using antenna array processing technology [78]	In the spatial domain, the spoofing effect is reduced in two stages and the signal-to-noise ratio of the real pseudo-random code is maximized. This method does not require antenna array calibration	Poor adaptability to all spoofing signals from different spoofing sources	Pre-despreading array processing capability	Before despreading	Medium
Anti-spoofing method for space-time multi-antenna nulling [79]	The space-time processing method is used to estimate the channel parameters of the spoofing source and its multipath reflection component. The method can implement the spoofing signal detection and its reflected signal nulling without reducing the true signal power.	Due to the need to configure multiple antennas, the hardware cost is increased; when the power level of the spoofing signal and the real satellite signal are similar, the effectiveness of the scheme is likely to be affected.	The scheme needs to configure an uncalibrated antenna array, and the receiver needs to have array processing technology	Before despreading	Medium
Spoofing detection method based on antenna array processing [62]	The method extracts the spatial characteristics on the higher power spoofing signal and the corresponding steering vector in the pre-despreading stage, and considers the situation that the antenna is not calibrated and the antenna is calibrated in the post-despreading phase.	The scheme increases hardware implementation costs and has a certain power loss	The receiver needs to configure the antenna array	Despreading	High

TABLE XIX
COMPARATIVE ANALYSIS FOR ANTI-SPOOFING PERFORMANCE BASED ON ANTI-SPOOFING METHODS OF ANTENNA ARRAY

Schemes	Selective power spoofing	Selective delay spoofing	Nulling attack	Denial environment
Anti-spoofing method for GNSS receivers [75]	Moderate	Moderate	Good	Poor
Blind adaptive array signal processing method [20]	Good	Moderate	Moderate	Good
Spoofing detection method Baseline data statistical analysis [18]	Moderate	Moderate	Good	Poor
Spoofing detection method for dual antenna power measurement [4]	Good	Moderate	Good	Moderate
Anti-interference scheme for Satellite navigation receiver [76]	Good	Moderate	Good	Moderate
Spoofing suppression method using periodic repeat CLEAN [77]	Good	Moderate	Moderate	Poor
Anti-jamming method using antenna array processing technology [78]	Moderate	Poor	Good	Poor
Anti-spoofing method for space-time multi-antenna nulling [79]	Moderate	Moderate	Good	Poor
Spoofing detection method based on antenna array processing [62]	Good	Moderate	Good	Good

The anti-spoofing methods proposed in [75], [20], [77], [78] and [79], combined with the processing technology of spatial domain are limited in scope. The detection performance of spoofing in some spoofing scenarios could be affected. While the reference [62], [4] and [76] use the adaptive antenna array technology, decision logic technology and other spoofing detection methods, although the difficulty of scheme is increased, the adaptability of the spoofing scene has been improved to some extent. A comparative analysis for the anti-spoofing performance of the anti-spoofing methods based on the antenna array is shown in Table XIX.

Analysis of Table XVIII and Table XIX shows that the above several spoofing detection methods combine antenna array technology, some of which are based on satellite signal power for spoofing detection according to the methods proposed in reference [62], [4], [76] and [77]. The Selective power spoofing signal could gradually increase its power range. When the receiver performs signal power detection, it could detect the abnormal changes caused by the spoofing signal in time, and greatly increase the difficulty for successful implementation of the Selective power spoofing attack. The spoofing suppression method using periodic repeat CLEAN proposed by the reference [77] combined with the linear constrained minimum variance algorithm. According to the estimated spoofing source direction, the scheme designed weighted vectors in multiple spoofing directions and formed antenna nulls. In order to compensate for the shortcoming of estimation accuracy on the forwarding spoofing attack, the first-order differential constraint algorithm is used to broaden the part of the antenna nulling, so that the spoofing source is located in the zero trap. Since the method can suppress multiple spoofing signals without receiving feedback information from the receiver and can be embedded in an ordinary receiver as an independent anti-spoofing module, the resistance to forwarding spoofing attack is also ideal. The spoofing detection method proposed in reference [76] includes a signal detector, a decision logic module and an anti-interference module. The main working process is to accurately identify, detect and characterize spoofing. The method utilizes decision logic to select an appropriate interference mitigation module, effectively protecting the receiver from spoofing signals and avoiding positioning errors. The solution can also be easily and flexibly integrated into existing receivers and controlled by the switching system.

This kind of spoofing detection method is often used to continuously monitor the satellite signal phase parameters. Therefore, the method has a general recognition performance on the selective delay spoofing. The nulling attack can make the receiver lose lock. The spoofing detection methods based

TABLE XX

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

COMPARATIVE ANALYSIS FOR SPOOFING DETECTION METHODS BASED ON ANGLE OF ARRIVAL

Method	Characteristics	Defect	Required configuration	Implementation phase	Implementation difficulty
Receiver autonomous spoofing detection method [80]	Intentional spoofing interference is prevented by any multiple independent receivers or a multi-antenna single oscillator receiver using antenna diversity techniques and single frequency reception techniques.	Due to the lack of physical security protection for static-structured receivers, the anti-spoofing performance could be influenced.	The scheme needs to configure multiple antennas, and increase the number of antennas and cost	Track and capture	Low
Spoofing detection method based on angle of arrival and variance of phase difference [72]	The method uses the spatial characteristics for direction angle reaching the receiver antenna of the spoofing signal and the real satellite signal to perform spoofing detection.	The method uses multiple antennas to monitor the signal arrival angle and needs to increase the number and cost of the antenna.	Receiver needs to configure multiple antennas	Capture	Medium

on the calibrated antenna array can better resist nulling attack, but the method is relatively inferior to the detection performance of denial environment.

G. SPOOFING DETECTION METHOD BASED ON ANGLE OF ARRIVAL

As depicted in Figure 16, the direction angle of the real satellite navigation signal reaching the phase center of the receiver antenna $(\theta_1,\cdots,\theta_i,\cdots,\theta_n)$ is not completely consistent, and the direction angle (θ) of the spoofing signal transmitted by the same transmitter reaching the phase center of the receiver antenna is completely consistent. Therefore, the method is based on the significant arrival angle difference between the spoofing signal and the real satellite signal as the identification feature of spoofing signal and uses the spatial characteristics of the satellite signal to detect the spoofing.

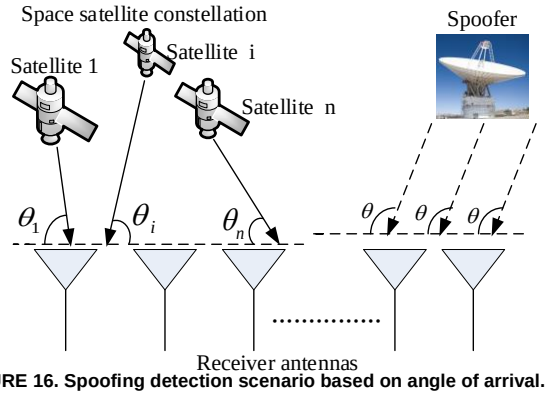

FIGURE 16. Spoofing detection scenario based on angle of arrival.

In general, each additional spoofing transmitter requires an additional antenna to correspond to it. Increasing the number of antennas can improve the technical difficulty for successfully implementing a spoofing attack. Therefore, if the number of antennas can be appropriately increased, the anti-spoofing detection performance can be improved to some extent. For this research, Montgomery et al. proposed an autonomous spoofing detection method based on the receiver angle of the L1 carrier difference for multiple antennas [80]. For receivers in a static state, the receiver antenna can be used to detect the angle of arrival for the received signal or to observe the phase difference changing rate of phase difference variance to achieve effective detection for the spoofing signal [72].Table XX compares and analyzes the spoofing detection method based on angle of arrival.

It can be seen from Table XX that the signal arrival angle spoofing detection method implemented by multiple antennas needs to calibrate the antennas. Although this technology increases the cost and hardware implementation difficulty, the antenna diversity technique using to compare arrival angle differences between the spoofing source and the real signal can effectively deal with spoofing. Because the anti-spoofing method includes a large number of iterative operations, the real-time performance of spoofing detection is poor. Table XXI compares the anti-spoofing performance of the spoofing detection method based on the angle of arrival.

TABLE XXI
COMPARATIVE ANALYSIS OF ANTI-SPOOFING EFFECTS BASED ON ANGLE OF ARRIVAL SPOOFING DETECTION METHOD

Schemes	Selective power spoofing	Selective delay spoofing	Nulling attack	Denial environment
Receiver autonomous spoofing detection method [80]	Moderate	Moderate	Good	Poor
Spoofing detection method based on angle of arrival and variance of phase difference [72]	Moderate	Good	Moderate	Poor

Combining the contents of Table XX and Table XXI, the spoofing detection method based on the angle of arrival and phase difference variance proposed in reference [72] continuously monitors the phase difference variance, and monitors the selective delay spoofing process in time. The detection and suppression of selective delay spoofing is better. The spoofing detection method based on the arrival angle can effectively identify the selective delay spoofing sent by the spoofing party that the power and delay are not much different from the real satellite signal and the phase is opposite by monitoring the direction of the arrival for the received signal. However, this method is less effective in denial environment.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

H. SPOOFING DETECTION METHOD BASED ON SUBSPACE PROJECTION

Subspace projection is a commonly used signal processing method. Choosing the appropriate information needed to construct subspace is a key part of subspace projection technology. By solving the subspace projection of the spatial domain spoofing signal, the spoofing signal with a larger power than the real satellite signal is eliminated. The subspace projection technique is used to analyze the time-frequency domain. The interference subspace estimation method is used to construct the interference subspace and project the input signal data onto the subspace orthogonal to the interference subspace. It is a commonly used anti-spoofing method. We illustrate the spoofing detection scenario based on subspace projection in Figure 17.

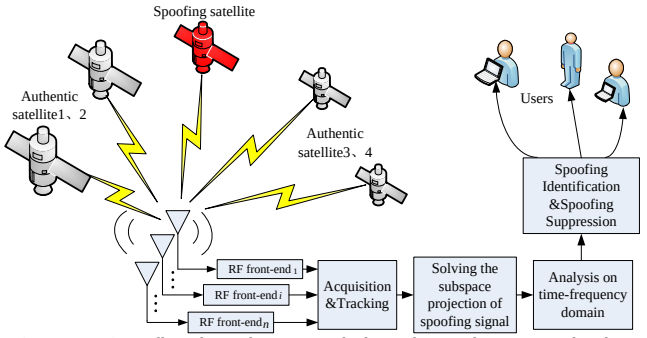

FIGURE 17. Spoofing detection scenario based on subspace projection.

TABLE XXII
COMPARATIVE ANALYSIS OF SPOOFING DETECTION METHODS BASED ON SUBSPACE PROJECTION

Method	Characteristics	Defect	Required configuration	Implementation phase	Implementation difficulty
Pseudo-random noise code domain spoofing detection and cancellation method [7]	The method designs a centralized receiver structure that suppresses cross-correlation interference capability and a distributed receiver structure with low power loss. This method has no additional requirements on the number of antennas and can be implemented in a single antenna receiver.	The spoofing detection performance of this method is greatly affected when the true signal strength is stronger than the spoofing signal strength.	The receiver needs to have a centralized structure or a distributed structure.	Track	Medium
Adaptive block subspace projection technique [81]	The method completes the projection process in a projection block that can adaptively adjust the length of the projection block and is insensitive to estimation errors.	Increasing technical costs and solution complexity	The receiver needs to be configured with a corresponding adaptive projection module.	Capture and track	High
Two-level hybrid spoofing suppression scheme [29]	The first stage uses the second-level feedback results to construct an orthogonal complement space to eliminate potential interference; the second stage uses an asymmetric structure.	The effectiveness of the scenario for specific spoofing is better, and the adaptability of the scene is relatively poor.	Space time adaptive processing (STAP)	Before capturing	Medium
Combined suppression method for jamming attack and spoofing [28]	The subspace technique is used to suppress jamming attack. The despreading and respreading algorithm is used to identify and suppress spoofing, and to form the high gain beam pointing to the real satellite signal again.	The algorithm structure for implementing jamming attack suppression, spoofing signal detection and suppression and multi-beam generation process is complicated.	This method requires to configurate multi-antenna receiver and subspace orthogonal projection technology.	Despreading	Medium

Han et al. from Harbin Institute of Technology found that under the premise of satisfying the signal strength of spoofing signal is greater than that of real signal strength, the carrier frequency and the code delay parameter information are used in the pseudorandom noise code domain to project the received navigation signal on orthogonal zero space of spoofing signal [7]. The process above can detect and eliminate spoofing. The rapid change of the frequency for the spoofing causes the time-frequency domain anti-spoofing method based on the subspace projection technique to be sensitive to the inaccuracy of instantaneous frequency. In response to this problem, Wang et al. used an adaptive projection module to project the received navigation signal onto the orthogonal subspace of spoofing signal [81]. The method optimizes the spoofing algorithm by adaptive block subspace projection technology, which makes the correlator signal-to-noise ratio increase by 11 *dB*.

Dong et al. from the Key Laboratory of Wireless Optical Communication in the Chinese Academy of Sciences proposed a two-stage hybrid interference suppression scheme [29]. In the absence of spoofing, the sigmoid function can be used to adjust the first-level processing to reduce its impact on real satellite navigation signals. The second stage introduces a cross-score algorithm of cross spectrum to generate anti-jamming beams, providing high beam gain for real signals. Most interference detection and suppression methods are only processed for one type interference. Wang et al. [28] proposed a joint suppression method for jamming attack and spoofing based on multi-antenna, and projected the received signal received by the array antenna into the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

orthogonal subspace of jamming attack to remove jamming. The method detects spoofing according to the correlation between weighted vectors obtained by the despreading and re-spreading algorithm. After the scheme completes the above process, the orthogonal subspace of spoofing is suppressed, and finally a high-gain multi-beam directed to the real satellite is formed. A comparative analysis for the spoofing detection method based on subspace projection is shown in

Table XXII.

Table XXII shows that in order to achieve better anti-spoofing performance using subspace projection technology, the subspace projection of the spoofing signal can be constructed by combining the carrier frequency of the satellite signal, the code delay, the Doppler shift, and the signal power. The two-stage structure is used to identify and eliminate the spoofing signal, and the real satellite signal is enhanced while the influence of spoofing on the useful signal is weakened. The method proposed in reference [81] increases the complexity and cost compared with the other three methods, but brings the advantages of adaptively adjusting the projection process and reducing the sensitivity of error estimation. Under the premise that the difficulty of the scheme is acceptable, the method can complement the other three methods to improve the feasibility for the spoofing detection method. A comparative analysis for the anti-spoofing performance of the spoofing detection method based on subspace projection is shown in Table XXIII.

TABLE XXIII
COMPARATIVE ANALYSIS OF ANTI-SPOOFING PERFORMANCE BASED ON SUBSPACE PROJECTION SPOOFING DETECTION METHOD

Schemes	Selective power spoofing	Selective delay spoofing	Nulling attack	Denial environment
Pseudo-random noise code domain spoofing detection and cancellation method [7]	Moderate	Good	Good	Moderate
Adaptive block subspace projection technique [81]	Moderate	Moderate	Good	Moderate
Two-level hybrid spoofing suppression scheme [29]	Moderate	Moderate	Good	Moderate
Combined suppression method for jamming attack and spoofing [28]	Moderate	Moderate	Moderate	Poor

Combined with the analysis in

Table XXII and Table XXIII, the pseudo-random noise code domain anti-spoofing method proposed in reference [7], needs to extract code delay and carrier frequency information in the tracking loop. The method has a good recognition performance on the selective delay spoofing attack that completes spoofing process by adjusting the delay size. The selective delay spoofing attack continuously controls the code delay to complete the spoofing attack process. The method monitors the code delay information, so that the receiver can effectively resist the selective delay spoofing attack. The methods proposed in reference [81] and [29] respectively suppress spoofing by the adaptive block subspace projection module and the two-level structure, which effectively increases the difficulty of successfully achieving nulling attack, and could better suppress nulling attack. The method proposed in reference [28] could suppress the spoofing and achieve the combined suppression of jamming attack simultaneously, which has certain restraining effects on selective power spoofing, selective delay spoofing and nulling attack. In general, this kind of method can effectively detect denial environment to a certain extent, and the reliability of the detection performance of denial environment is general.

I. SPOOFING DETECTION METHOD BASED ON SIGNAL ARRIVAL DIRECTION

The only signal feature that is currently difficult to forge is the direction of the electromagnetic wave. As depicted in Figure 18, there is spatial correlation among the signals emitted by a spoofing signal source. Due to current technical conditions, the spoofing signals of several different satellites are often transmitted by the same spoofing signal transmitter, and the real satellite signals do not have the spatial correlation of the spoofing signals, so spoofing detection could be based on this fact.

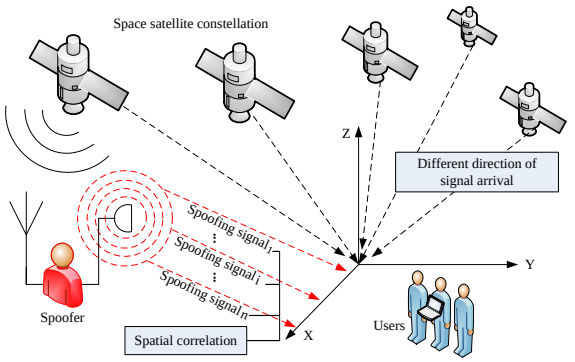

FIGURE 18. Spoofing detection scenario based on signal arrival direction.

Xu et al. proposed a spoofing detection technique based on multiple information sources and parameter estimation predictions [82]. In the first stage, the coordinate source is used to classify the emission source and select a source with a high elevation angle, and the beam space is used instead of the sensor space to provide high gain. In the second stage, each received signal is separated by oblique projection, which can better identify and distinguish spoofing signal and most multipath signals. Shi et al. compared the actual

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

incoming wave direction measured by the attitude measuring instrument and the satellite transmitting signal standard almanac data [83]. The method selects the appropriate decision threshold and eliminates the spoofing signal, so that the spoofing signal does not participate in the subsequent positioning solution process. A comparative analysis for the spoofing detection method based on the arrival direction for the signal is shown in Table XXIV.

TABLE XXIV
COMPARATIVE ANALYSIS OF SPOOFING DETECTION METHODS BASED ON SIGNAL ARRIVAL DIRECTION

Method	Characteristics	Defect	Required configuration	Implementation phase	Implementation difficulty
Signal arrival direction estimation, cross-correlation peak detection, power calculation and comparison spoofing detection method [82]	The estimated beam space arrival direction mitigates multipath interference and possible spoofing effects through multiple information sources and parameter estimation; this method performs power comparison and cross-correlation operation on the four strongest signals.	The spoofing detection method has high operation complexity and increases certain technical cost; and the two-stage anti-spoofing process has poor real-time performance.	The receiver needs to have spatial spectrum estimation and time domain correlation spoofing detection capability.	Track	High
Spoofing detection method based on inertial navigation and attitude measurement [83]	The method compares the direction for the arrival of the actual satellite signal with the direction for the reference signal and detects the spoofing signal.	This approach requires an increase in antenna arrays and hardware implementation costs. The direction for the reference signal is derived from the inertial output parameters and satellite ephemeris data, and its estimation accuracy affects the performance of spoofing detection.	Attitude measurement meter and inertial navigation system	Capture	High

It can be seen from the above analysis that spoofing detection method for measuring direction of the navigation satellite signal has a certain complexity in terms of technology and hardware implementation and brings additional cost problems. The method needs to be collaboratively detected by means of other navigation systems such as an attitude measurement meter and inertial navigation system. The difficulty is larger than other schemes, but spoofing detection performance is better. The real-time performance of the proposed method in the reference [82] is not very satisfactory in the actual receiver operation. Detection method on navigation deception signals based on INS and GNSS attitude measurement proposed in reference [83] optimizes and improves the above methods in real-time. Table XXV compares the anti-spoofing performance of spoofing detection methods based on the arrival direction of the signal.

The spoofing detection method mentioned in reference [82] monitors the arrival direction for satellite signals, and continuously monitors related parameters such as signal power, which can better detect selective power spoofing. Themethod proposed in reference [83] compares the direction of the incoming wave calculated by combined ephemeris and so on with the direction of the incoming wave of the actual received signal. The spoofing detection method can better suppress nulling attack. Analyzing Table XXIV and Table XXV, it can be seen that although the implementation of the spoofing detection method based on the direction for arrival of the signal is more difficult than other methods, the resistance to selective delay spoofing affecting the normal acquisition of the receiver is still not obvious. The method is less effective in resisting denial environment.

TABLE XXV
COMPARATIVE ANALYSIS OF ANTI-SPOOFING PERFORMANCE FOR SPOOFING DETECTION METHODS BASED ON SIGNAL ARRIVAL DIRECTION

Schemes	Selective power spoofing	Selective delay spoofing	Nulling attack	Denial environment
Signal arrival direction estimation, cross-correlation peak detection, power calculation and comparison spoofing detection method [82]	Good	Moderate	Moderate	Poor
Detection on Navigation Deception Signals Based on INS and GNSS Attitude Measurement [83]	Moderate	Moderate	Good	Poor

J. SPOOFING DETECTION METHOD BASED ON SIGNAL QUALITY MONITORING

There is a certain delay between the time when the forwarded spoofing signal arrives at the receiver and the time when the real signal arrives at the receiver. For the receiver configured with the multi-correlator, the difference between the arrival time of the spoofing signal and the real satellite signal arriving at the receiver causes an abnormality in the correlation peak. The spoofing signal affects the receiver correlator output. Therefore, it is possible to judge whether there is a spoofing signal by the distortion of the correlation

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

peak. Figure 19 presents the block diagram for spoofing detection method based on signal quality monitoring.

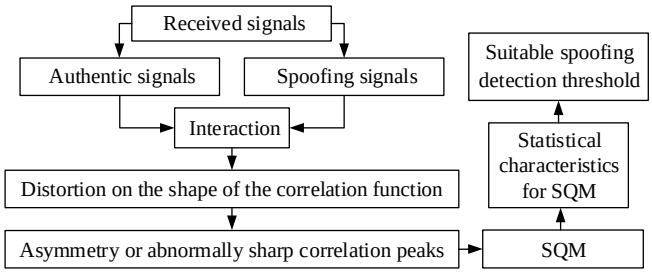

FIGURE 19. Block diagram for spoofing detection method based on SQM [85].

Manfredini et al. proposed a signal processing algorithm using signal quality monitoring technology (SQMT) [84]. The method measures the peak quality of the correlation function and uses a pair of additional correlators to detect the residual signal. It could identify the distortion of related shapes and residual signals under static and dynamic conditions and verify its anti-spoofing performance with lower complexity. Jahromi et al. analyzed the effects of tracking-level spoofing on receiver correlator output and designed signal quality monitoring (SQM) metrics [85]. The method detects a distortion anomaly shape, or an asymmetric correlation peak caused by an interaction between a real signal correlation peak and a forged signal correlation peak in the receiver tracking phase. This method combines the statistical characteristics for multiple signal quality monitoring (SQM) indicators with the mean and variance of each SQM metric to calculate a suitable spoofing detection threshold. Broumandan et al. proposed using pre-despreading metrics and post-despreading metrics to jointly detect spoofing in multipath interference environments where spoofing signals and multipath signals coexist [86]. The

TABLE XXVI
COMPARATIVE ANALYSIS FOR SPOOFING DETECTION METHODS BASED ON SIGNAL QUALITY MONITORING

Method	Characteristics	Defect	Required configuration	Implementation phase	Implementation difficulty
Spoofing detection method based on signal quality monitoring technology (SQMT) [84]	Using the target receiver input power control algorithm, the calibration phase and detection window are defined according to the specific application requirements.	This method is not ideal for the detection rate of TEXBAT spoofing scenario 2 and spoofing scenario 5. Spoofing detection performance is poor, and it needs to cooperate with other methods.	The receiver needs to configure an additional correlator	Track	Low
Signal authenticity test using signal quality monitoring indicators [85]	Joint detection for pseudo-correlation peaks through various signal quality monitoring indicators achieves spoofing signal detection	The method can affect the effective recognition performance of spoofing signals in the case for coexistence of multipath interference and spoofing signals.	Receiver equipment needs to have correlation peak detection capability and additional multi-correlator	Track	High
Pre-despreading index and post-despreading metric joint detection method [86]	By combining the improved pre-despreading indicators and post-despreading metrics, the spoofing can be identified from the multipath interference environment, and the false alarm probability can be reduced.	It is necessary to synthesize the comparison results of the four metrics and the detection threshold for spoofing judgment. This method spends more time and is limited in applications where real-time requirements are high.	The receiver needs to be configured with multiple correlators and has four indicators for monitoring and analysis.	Track	Medium

signal quality detection indicator is initially used to monitor the correlation peak quality affected by multipath interference. The improved SQM technique can detect spoofing as a post-despreading metric during the tracking phase. If only the signal quality detection index and the carrier-to-noise ratio indicator exceed the threshold, it indicates that multipath interference exists; if variance, SPCA, SQM, and carrier-to-noise ratio all exceed the threshold, it indicates that spoofing is detected. Table XXVI compares and analyzes various spoofing detection methods based on signal quality monitoring.

It can be seen from the analysis of Table XXVI that the detection method for monitoring signal quality is generally based on whether the correlation peak of the multi-correlator output for the target receiver is distorted during the tracking phase. In reference [86], the specific implementation method for joint detection of spoofing signals combined with pre-despreading index and post-despreading index in multipath interference environment is given. The above method increases the detection probability and reduces the probability of false alarms. For the problem of long processing time, the reference [84] significantly reduces the processing time of the actual operation process, and the implementation difficulty of the overall scheme is reduced. The following table compares the anti-spoofing performance of the spoofing detection method based on signal quality monitoring.

For the receiver, real satellite signals and spoofing signals are received. It is difficult to keep the correlation peak of the receiver multi-correlator output always normal without distortion. This provides an opportunity to detect selective power spoofing. It can be seen from Table XXVII that the detection performance for this kind of method on selective delay spoofing is general; the signal quality monitoring

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

technology has a poor detection performance on nulling attack spoofing. Even if the spoofing has not begun to influence the tracking process of the target receiver, the joint detection of various SQM indicators can also detect the existence of pseudo-correlation peaks by using the scheme proposed in reference [84]. So, the detection performance for the method of selective delay spoofing is better. Among the three spoofing detection methods shown in Table XXVII, the spoofing detection method proposed in reference [85] combines four detection indicators and detection thresholds respectively, and spoofing detection performance is better than other methods.

TABLE XXVII
COMPARATIVE ANALYSIS OF ANTI-SPOOFING EFFECTS BASED ON SIGNAL QUALITY MONITORING

Schemes	Selective power spoofing	Selective delay spoofing	Nulling attack	Denial environment
Spoofing detection method based on signal quality monitoring technology (SQMT) [84]	Good	Moderate	Poor	Poor
Signal authenticity test using signal quality monitoring indicators [85]	Good	Good	Poor	Moderate
Pre-despreading index and post-despreading metric joint detection method [86]	Good	Moderate	Poor	Poor

K. OTHER ANTI-SPOOFING METHODS

The anti-spoofing method described above implements the resistance of spoofing from the level of spoofing detection or spoofing suppression. The above methods are divided into ten categories from the technical details. Some implementation means and technical details of the anti-spoofing methods are not consistent with the above ten categories. The summary analysis of these methods is as follows:

A spoofing attack that significantly changes the phasor measurement unit (PMU) measurements could seriously influence the normal operation of the network. In response to this problem, Risbud et al. used the spoofing attack metric model to transform the network state estimation and attack reconstruction problem into a non-convex constrained least squares problem [30]. Since the most vulnerable phasor measurement unit in the identification network is to be optimized, the joint state estimation and attack reconstruction interaction minimization algorithm is used to solve the problem responding to spoofing attack. Signal processing technology can mitigate the effects of spoofing. Kim et al. proposed a method for eliminating spoofed channels by signal processing [87]. The research team also proposed a spoofing suppression method for spoofing signal elimination by radio frequency phase control. These two methods cause the navigation positioning result to be converted into a normal state from the abnormal state caused by the spoofing signal. Berardo et al. proposed a time hopping (TJ) anti-spoofing signal processing algorithm combined with signal processing technology [88]. The scheme is based on the idea of using multiple correlators to observe the correlation function between the input signal and the local copy to detect multipath. Estimating the relative delay between real signals and spoofing signals causes the receiver to lose lock and relock to the real signal. Due to the influence of the residual signal, the positional accuracy obtained by navigation signal suppressing spoofing is slightly lower than that of the navigation positioning position obtained by the real signal.

According to the basic principle that the spectral characteristics of the phase detector output signal in the tracking loop is closely related to whether there is a spoofing signal in the tracking loop. Zhao et al. perform spectrum analysis on the output signal of the phase detector and establish a spoofing detection model [89]. This scheme describes a tracking segment regenerative deception signal detection method based on carrier phase tracking spectrum analysis under medium and low dynamics. The forward-style spoofing signal has a certain delay compared to the real signal. When the receiver initially captures the signal, the convolution search process can be completed in the frequency domain. And the frequency phase two-dimensional search in the capture phase can better detect more powerful spoofing signals [72]. Bhamidipati et al. proposed a time-authentication algorithm based on a widely distributed static receiver and its known location network [90]. Firstly, a pairwise cross-correlation operation is performed on the conditionally constrained four-phase carrier erasure input signal, and the auxiliary position information is used to estimate the expected time offset of the P(Y) code received by different receiving ends. On the basis of the above operations, each receiver is verified by analyzing the weighted sum of the paired cross-correlation peak offset and amplitude of each receiver and its common satellite. Wang et al. proposed a new method for judging whether there is a spoofing signal based on the number of correlation peaks found above the threshold in the receiver capture phase [91]. If two correlation peaks are found, it indicates that there is a spoofing signal; If a peak is found, only when the coarse signal to noise ratio is less than the power threshold and the correlation function width is less than the width threshold, it indicates that there is no spoofing signal. The method can solve the problem that the real signal and the spoofing signal overlap. The theoretical calculation method of the above power threshold and its quantitative reference value are given, the influencing factors and performance are analyzed.

The traditional slope spoofing detection method can effectively detect the spoofing interference in the line-of-sight environment, and the spoofing detection performance in the multipath interference environment could be affected to some extent. The spoofing detection method to be introduced

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

next makes up for this deficiency. Cai et al. used the huge difference for correlation value between the deception signal and the multipath signal as the basic detection basis of the spoofing signal [92]. A slope detection algorithm based on multi-correlator structure is proposed. And the traction spoofing detection method with reasonable detection threshold in multi-path interference environment is determined by Naiman-Pearson criterion. The ratio of spoofed satellite signals associated with different satellites and propagating through the same wireless channel is highly correlated, while the true signal ratios transmitted over independent wireless channels are independent of each other. Therefore, spoofing attacks can be identified by the correlation of these ratios. According to the above basic principles, Li et al. propose a new method for spoofing detection using the delay and gain ratio among multipaths in wireless channels [93]. Khalajmehrabadi et al. proposed the time synchronization attack rejection and mitigation (TSARM) technique for static GPS receivers and its evaluation method [94]. The method uses the evaluation platform of the real satellite signal spoofing mechanism available in TEXBAT to study the practicality for reducing the effect of spoofing. The technique utilizes the pseudorange ratio measured at the victim target receiver and evaluates its anomalous behavior. It corrects the measured value taking into account the actual constraints of the real spoofer party. Carson et al. proposed a GPS spoofing detection and removal algorithm [95]. Han et al. proposed a particle filter (PF)-based maximum particle weight spoofing detection scheme, which uses the relationship between spoofing and particle weights [96]. The method detects and suppresses spoofing by using an improved robust estimation method and capturing the anomalous maximum particle weight. Table XXVIII compares and analyzes other kinds of anti-spoofing methods. Shang et

TABLE XXVIII
COMPARATIVE ANALYSIS OF OTHER ANTI-SPOOFING METHODS

Method	Characteristics	Defect	Required configuration	Implementation phase	Implementation difficulty
Spoofing detection method based on spoofing attack metric model [30]	The method uses joint state estimation to solve the phase angle measurement unit optimization problem while extracting attack and dynamic estimation without continuous time measurement.	The spoofing detection method considers less to nonlinear delay dynamic monitoring system in the actual environment.	Receiver needs joint state estimation capability.	Capture and track	Low
Two methods for spoofing suppression [87]	The method combines signal processing technology and RF phase control technology to perform spoofing signal elimination.	The performance reliability of applying this method to the front end of the receiver for spoofing suppression needs to be improved.	Receiver needs RF phase control and analysis capabilities	Capture and track	Medium
Time hopping (TJ) anti-spoofing method [88]	The scheme analyzes time hopping through linear regression algorithm, combined with signal processing techniques	Currently, the amount of calculation is large, and optimization is needed in the selection of the empirical threshold.	Receiver needs signal delay detection capability	Track	High
Regenerative spoofing signal detection method [89]	The method performs spectral analysis on the output signal of the phase detector and establishes a spoofing detection model.	Multipath interference can cause an increase in false alarm probability. This method lacks consideration of the impact for multipath interference in the process of considering the overall plan.	Phase detector output signal spectrum analysis capability	Track	Medium
Frequency phase two-dimensional search spoofing detection method [72]	The method performs spoofing detection according to the characteristics that the spoofing signal energy is usually larger than that of the real satellite signal.	This method has great limitations, and it could cause misjudgment when the signal strength of the spoofing signal is close to or weaker than that of the real satellite signal.	The receiver needs to have frequency phase two-dimensional search capability	Capture	Medium
Time authentication spoofing detection method [90]	The method combines cross-checking and cross-correlation operations to perform time authentication for static receivers and known location networks.	The method has high computational complexity and has certain difficulty in implementation.	Cross-checking and cross-correlation capability	Capture and track	High
A new method of spoofing detection in the capture phase [91]	The scheme monitors the number of correlation peaks above the power threshold based on the signal power level and the preset power threshold comparison result	Spoofing detection performance is unstable when satellite signal sampling rate is low, or signal interval is small.	The receiver has the ability to detect the number of related peaks	Capture	Medium
Slope detection method for multi-correlator structure [92]	The method performs spoofing detection based on the difference of correlation value between the spoofing signal and the multipath	The implementation process requires a certain technical difficulty and hardware cost.	Receiver needs to configure multi-correlator.	Capture and track	High

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

	signal.				
GPS spoofing signal detection method [93]	Spoofing detection based on the difference in correlation between the ratio of spoofing signals and the ratio of real satellite signals	The spoofing detection process for monitoring the delay and gain ratio between multipaths takes a long time, and the applicability in real-time operation applications is poor.	Correlation peak detection capability	Capture and track	High
Real-time time synchronization attack suppression and mitigation techniques [94]	The program monitors satellite clock variation or drift bias, and models spoofing attacks.	This method is less effective in real-time detection.	Receiver needs satellite clock difference and drift deviation monitoring capability	Capture and track	Medium
GPS spoofing detection and removal algorithm [95]	The scheme combines collaborative adaptive cruise control (CACC) system and situational awareness technology.	Spoofing signal detection performance is not very stable in multipath interference environment	Various sensors	Despreading	High
Maximum particle weight spoofing detection scheme [96]	The premise of this method is that only one satellite in the visible satellite participating in satellite navigation and positioning is subjected to spoofing attacks.	The detection scheme has poor reliability in spoofing detection performance in which multiple satellites are subject to spoofing.	Particle filter processing capability	Capture and track	Medium
Method for positioning spoofer based on a space-time double-difference observation model [97]	This method only needs a GNSS receiver and observes the spoofing signal to locate the spoofing party. In addition, the receiver in this method does not receive the influence of position factors, that is, the receiver may be fixed or mobile.	The deviation of the method used by the deceiver in positioning may be affected by environmental factors and lead to excessive positioning deviation.	GNSS receiver	Track	Medium

TABLE XXIX
ANALYSIS OF ANTI-SPOOFING EFFECT OF OTHER ANTI-SPOOFING METHODS

Schemes	Selective power spoofing	Selective delay spoofing	Nulling attack	Denial environment
Spoofing detection method based on spoofing attack metric model [30]	Moderate	Good	Poor	Moderate
Two methods for spoofing suppression [87]	Moderate	Good	Poor	Poor
Time hopping (TJ) anti-spoofing method [88]	Moderate	Good	Poor	Moderate
Regenerative spoofing signal detection method [89]	Moderate	Good	Poor	Poor
Frequency phase two-dimensional search spoofing detection method [72]	Moderate	Good	Poor	Poor
Time authentication spoofing detection method [90]	Good	Moderate	Poor	Good
A new method of spoofing detection in the capture phase [91]	Good	Moderate	Poor	Poor
Slope detection method for multi-correlator structure [92]	Good	Good	Poor	Good
GPS spoofing signal detection method [93]	Good	Good	Poor	Good
Real-time time synchronization attack suppression and mitigation techniques [94]	Moderate	Moderate	Moderate	Good
GPS spoofing detection and removal algorithm [95]	Moderate	Moderate	Moderate	Good
Maximum particle weight spoofing detection scheme [96]	Moderate	Moderate	Poor	Poor
Method for positioning spoofer based on a space-time double-difference observation model [97]	Moderate	Moderate	Moderate	Good

al. proposed a method to use the receiver to track the position of the spoofer. The method uses the time and ephemeris parameters of the spoofed satellite signal received by the receiver to replay the spoofed signal, thereby achieving the effect of tracking the spoofer [97].

The difficulty and implementation phases for the twelve types of spoofing detection or suppression methods introduced in this section and the concerns are different. Satellite navigation systems are vulnerable to spoofing attacks, and certain anti-spoofing measures are necessary and urgent for the growing application of satellite navigation systems. In addition to the above methods, from the perspective of reducing the false alarm probability, the following three methods of spoofing identification are briefly introduced. Wesson et al. proposed spoofing detection method combining symmetric differential autocorrelation distortion monitoring and in-band power monitoring with a low false alarm probability [98]. Gao et al. proposed an anti-spoofing method based on the detection of carrier phase and code phase consistency to identify the weaknesses of spoofing attacks using intermediate spoofing attackers [99]. There is a pseudorange double difference between spoofing signal and the real signal arriving at the receiver two times before and after. Liu et al. constructed the pseudorange

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

double difference detection quantity one by one for the received signals and proposed a spoofing signal recognition algorithm based on the time before and after. This method can identify the spoofing signal of a single channel receiver [100]. The analysis of the above 12 anti-spoofing methods for selective power spoofing, selective delay spoofing, nulling attack and denial environment is shown in Table XXIX.

Combined with the analysis in Tables XXIX and XXX, the spoofing detection method or the spoofing suppression method proposed in reference [72], [30], [87], [88] and [89] mainly completes the anti-spoofing process by monitoring the phase shift of the signal and other techniques. The resistance performance of these methods to selective power spoofing is not as good as the selective delay spoofing, and their resistance performance to nulling attack and denial environment is not very significant. References [90] and [91] are mainly for the continuous monitoring of the possible changes in the received signal power during the process of spoofing. Therefore, the two methods are more ideal for the anti-spoofing performance of selective power spoofing. Among them, the method proposed in [90] detects cross-correlation operations on the collected military GPS signals to detect spoofing attacks by cross-checking whether there is a cryptographic code in each receiver without knowing the exact encryption. This method increases the reliability of the detection performance while increasing the difficulty of certain implementation. Reference [93] proposed to select the correlation peaks with the same satellite delay and the closest to the strongest peak, and calculate the ratio of the peak to the strongest peak, which provides a new idea for the detection of spoofing. This method needs to estimate the delay between the strongest correlation peak associated with each satellite and other correlation peaks. Although the implementation difficulty and processing time are increased, the feasibility of selective power spoofing detection and selective delay spoofing detection is feasible. Moreover, the method has a better resistance performance to the formation of denial environment than other methods. The reference [94] analyzes the deviation for the clock and drift of the receiver under normal conditions and spoofing conditions, and directly models the spoofing attack which can be easily integrated with off-the-shelf GPS equipment. The performance for resisting denial environment is considerable. Reference [95] uses the distance between users and the situational awareness provided by various sensors to detect spoofing, while the spoofing suppression system removes spoofing attacks from incoming data streams. The method has the average performance on the selective power spoofing detection and the selective delay spoofing detection. However, this method has superior detection performance compared to other methods for nulling attack and denial environment.

TABLE XXX
ANTI-SPOOFING EFFECT OF ANTI-SPOOFING METHODS IN TEN TYPES OF SIGNAL PROCESSING

Schemes	Selective power spoofing	Selective delay spoofing	Nulling attack	Denial environment
Spoofing detection based on Doppler shift	Good	Good	Poor	Poor
Spoofing detection method based on consistency check	Good	Moderate	Poor	Moderate
Spoofing detection based on signal parameter statistics analysis	Moderate	Good	Poor	Poor
Spoofing detection based on arrival time and arrival time difference	Moderate	Good	Moderate	Poor
Residual signal detection	Good	Moderate	Poor	Poor
Spoofing detection method based on Antenna array	Good	Moderate	Good	Good
Spoofing detection method based on angle of arrival	Moderate	Moderate	Moderate	Poor
Spoofing detection based on subspace projection	Moderate	Moderate	Good	Good
Spoofing detection method based on signal arrival direction	Moderate	Moderate	Moderate	Moderate
Spoofing detection method based on signal quality monitoring	Good	Moderate	Poor	Poor

L. SUMMARY

The anti-spoofing attack method for user receiver can be considered separately from the signal processing level and the information processing level. This section mainly analyzes the anti-spoofing performance from the receiving satellite signal level. The anti-spoofing method for data processing level will be introduced in detail in the next section. The anti-spoofing performance of other anti-spoofing methods in the previous section has been analyzed and summarized in detail above and will not be described here. The anti-spoofing performance for the anti-spoofing methods of the ten kinds of signal processing levels is shown in Table XXX.

The resistance performance for various implementation methods of each type anti-spoofing method to different spoofing attacks has been elaborated and summarized in the previous sections and is beyond the scope of this section. In the following, according to the anti-spoofing methods, the anti-spoofing performance is compared and analyzed.

Spoofing detection methods that monitor signal parameters or satellite signal indicators usually do not require additional

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

hardware. Because this method continuously monitors and compares parameters such as signal power and signal amplitude, it has better detection performance for selective power spoofing and selective delay spoofing. However, its resistance to nulling attack is not particularly ideal. In comparison, the spoofing detection or suppression method of adding a hardware configuration such as an antenna array or multiple antennas is more reliable for the detection performance of the nulling attack. Denial environment could cause undesirable consequences such as receiver blockage and tracking loop loss and cause the receiver to complete the capture and tracking process again. It is a relatively complicated way of spoofing. The anti-spoofing method described above generally has a general detection performance in a denial environment. However, the hybrid anti-spoofing method for the signal-level anti-spoofing method described in this section and the information-level anti-spoofing method described in the next section are expected to be effective in detecting and suppressing denial environment.

The performance for each kind of anti-spoofing method is not completely consistent in the detection or suppression of spoofing. The advantages and disadvantages of the anti-spoofing performance are closely related to the technical details of each anti-spoofing method. The evaluation of anti-spoofing performance is an objective evaluation of spoofing detection or suppression performance and promotes the development or progress for anti-spoofing technology. At present, there is no accurate representation for the definition of signal integrity and its evaluation methods. In response to this problem, Chen et al. proposed a trust framework based on subjective logic to evaluate the integrity of received civil satellite signal [101]. This paper first formalizes the signal integrity in the framework and is used to accurately characterize the detection performance for different spoofing detection methods. The framework quantifies the uncertainty in the signal integrity inference process and accurately characterizes the spoofing detection method. By extracting the causal relationship between measurement effectiveness and signal integrity, the method provides a series of operators that correspond to logical operations and uncertainties, as well as a general understanding of spoofing detection performance.

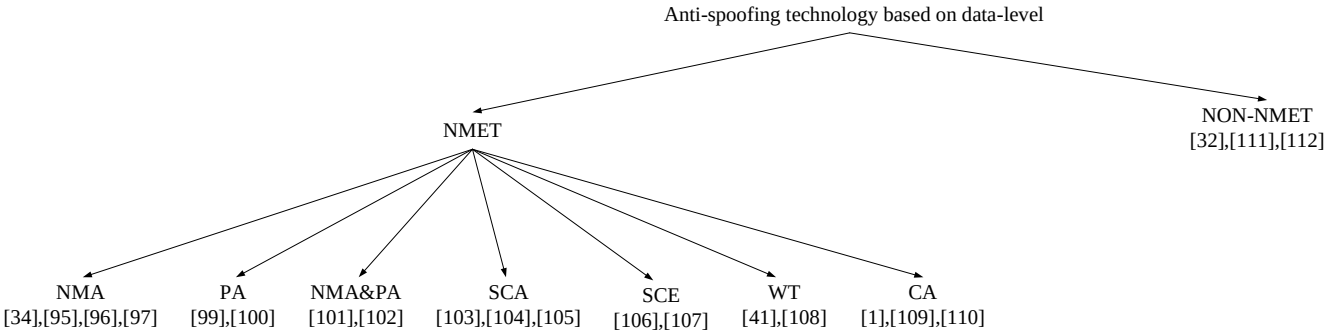

FIGURE 20. Taxonomy of anti-spoofing technology based on data-level.

IV. ANALYSIS OF SATELLITE NAVIGATION ANTI-SPOOFING TECHNOLOGY BASED ON DATA-LEVEL

Since the signal parameters and information format of GNSS civil signals are public, more and more civil GNSS signals are affected by spoofing attacks. Therefore, it has become increasingly important to study a scheme that can effectively prevent GNSS civil signals from being spoofing. At present, GNSS anti-spoofing technology can be divided into non-navigation message encryption technology (NON-NMET) and navigation message encryption technology (NMET). Non-navigation message encryption technology is a traditional anti-spoofing technology proposed at the receiver-level. However, with the improvement of spoofing technology in recent years, these traditional anti-spoofing technologies begin to show deficiencies. Based on this, many scholars use navigation message encryption technology to achieve the purpose of resisting fraud.

We divide navigation message encryption technology into seven categories, navigation message authentication (NMA), protocol authentication (PA), navigation message authentication and protocol authentication combination (NMA&PA), spreading code authentication (SCA), spreading code encryption (SCE), watermark techniques (WT), and combined authentication (CA), as shown in Figure 20.

In the following subsections, we discuss these subcategories of NEMT and the whole category of NON-NEMT in detail.

A. NAVIGATION MESSAGE AUTHENTICATION

For civilian GNSS navigation messages, some scholars have proposed a navigation message authentication method (NMA). The specific implementation principle of this method is shown in Figure 21. The sender generates authentication information through an encryption algorithm (e.g., DES, RSA, DSA, ECDSA, etc.). The receiver decrypts the authentication information using the key. By analyzing the decrypted results, the receiver can confirm the integrity of the navigation message. When the navigation information cannot be successfully authenticated, the receiver can treat the information as spoofing information and delete it, accordingly, achieving the purpose of resisting spoofing attacks. At present, the main methods mentioned in the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

relevant references are symmetric encryption algorithm and asymmetric encryption algorithm to implement NMA.

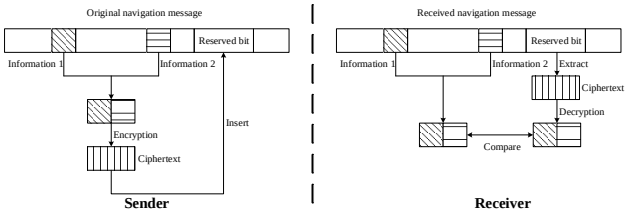

FIGURE 21. The specific implementation principle of NMA.

Figure 21 gives a brief overview of NMA method. In Figure 21, information 1 and information 2 represent two types of navigation message parameters. The sender can choose different navigation message parameters or all navigation message parameters to encrypt according to security requirements. After the encryption process, the sender inserts the ciphertext information into the reserved bits in the navigation message. The receiver extracts the ciphertext in the received navigation message and then decrypts it.

Maier et al. have built an estimated spoofing attack scenario software platform based on navigation message authentication technology [102]. Based on this platform, they evaluated the anti-spoofing performance of the Galileo E1B INAV signal that passed the navigation message authentication technology. The evaluation results show that the navigation message authentication technology under this platform cannot resist the estimated spoofing attacks in certain environments, but it can resist most of the generated spoofing attacks. In addition, they also analyze the impact of character errors in the transmission of navigation signals on the success rate of NMA authentication. CHINO et al. built an experimental platform for power spoofing attacks [103]. The sender encrypts the QZSS L1C/A part of the navigation message by using the RSA encryption algorithm to generate ciphertext information and inserts the ciphertext into the navigation message for transmission. The receiver decrypts the ciphertext to determine whether the received navigation message is spoofed information. However, the scheme does not consider other security factors, such as signal transmission protocol, key management and so on. Therefore, this scheme cannot effectively guarantee the overall security of the system. Wesson et al. used the elliptic curve digital signature algorithm to generate the signature of the navigation message [36]. The sender inserts the signature into the GPS Civil Navigation Message (CNAV) and transmits the CNAV. The receiver verifies the integrity of the CNAV by authenticating the signature information. In addition, this scheme can detect replay spoofing attack (RSA) with a detection probability greater than 0.97 and a false alarm probability of 0.001. However, this scheme lacks detection in a real environment to judge its actual performance. Wu et al. proposed a scheme to protect BeiDou-II navigation information based on ECDSA algorithm [104]. They not only analyzed the authentication rate of different navigation messages in the Gaussian noise environment, but also designed the complete key exchange process of the BeiDou-II navigation system. The experimental simulation shows that the BeiDou navigation system based on ECDSA encryption algorithm has better anti-spoofing ability. Wu et al. Also proposed a Beidou civil anti-spoofing scheme combining navigation message authentication and spreading code authentication. This scheme analyzes the Beidou system theoretically and involves the mutual authentication of the satellite segment, the user segment, and the ground segment. From the experimental results, this scheme has a small false alarm rate [105].

TABLE XXXI
RESISTANCE OF VARIOUS NAVIGATION MESSAGE AUTHENTICATION METHODS TO DIFFERENT SPOOFING ATTACKS

Schemes	Maier et al.'s scheme [102]	CHINO et al.'s scheme [103]	Wesson et al.'s scheme [36]	Wu et al.'s scheme [104]	Wu et al.'s scheme [105]
Direct-replay spoofing attack	Moderate	Good	Good	Good	Good
Replay spoofing attacks based on multiple antenna receivers	Poor	Moderate	Moderate	Poor	Poor
Direct-generation spoofing attack	Good	Good	Good	Good	Good
Analyze-generated spoofing attacks	Moderate	Moderate	Moderate	Moderate	Moderate
SCER and FEA spoofing attacks	Poor	Poor	Moderate	Poor	Moderate
Full channel generated spoofing attack	Poor	Poor	Poor	Poor	Poor

CHINO et al.'s scheme [103] is difficult to implement, mainly due to its high hardware configuration and complete design of the overall design. Based on the analysis of the above various navigation message authentication schemes, the resistance of various schemes to different spoofing attacks is shown in Table XXXI.

In view of the characteristics of the various spoofing methods in the section II and the characteristics of the navigation message authentication method, Table XXXI is only a theoretical analysis of the possibility that various design schemes can resist different spoofing attacks. Since the process of generating a signature for a navigation message is one-way and irreversible, the navigation message authentication method can resist most direct-generation spoofing attacks. Compared with the analysis generation spoofing attack, since this attack can analyze and generate the corresponding navigation signal with authentication function, the user can resist the spoofing attack generally. Maier et al.'s scheme [102] has lower requirements on receiver hardware, so their scheme is less effective against RSA based on multi-antenna receiver. For SCER and FEA spoofing attacks, since the navigation message authentication

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

only encrypts the navigation message and does not protect the spreading code of the satellite signal, the navigation message authentication technology has a poor resistance to this ESA. Wesson et al.'s scheme [36] designed SCER and FEA detection to resist ESA, so their scheme has a better defense effect. The implementation of full-channel spoofing attacks is difficult and the spoofing effect of this type of spoofing attacks is better. For this reason, most anti-spoofing schemes have less resistance to full-channel spoofing attacks, except for some combination-type authentication schemes. For RSA, navigation message authentication technology can determine whether the time information in the navigation message is spoofing information or not, so this scheme has good anti-spoofing effect for most RSA. However, for replay spoofing attacks based on multiple antenna receivers, some schemes do not involve multi-star spoofing (such as Maier et al.'s scheme [102] and Wu et al.'s scheme [104]), so their scheme has a poor defense effect against replay spoofing attacks based on multiple antenna receivers.

B. PROTOCOL AUTHENTICATION

The method of navigation message authentication uses encryption algorithm to generate a signature or ciphertext that requires authentication information. The receiver uses the asymmetric key to implement the authentication function or decrypts the ciphertext through the symmetrical key. However, the authentication method using asymmetric encryption will cause a large authentication overhead [106] and symmetric encryption algorithm has low security, so some scholars have proposed using a protocol scheme to improve the speed of navigation message authentication and the security of satellite communications.

Timed Efficient Steam Loss-tolerant Authentication (TESLA) is a protocol type authentication scheme that uses a symmetric encryption algorithm and uses key release delay technology to implement asymmetric encryption. The purpose of this protocol is to meet both the above performance and security requirements. In essence, TESLA is one of the navigation message encryption technologies as well as the navigation message authentication. TESLA uses the key delay release technology to achieve asymmetric encryption, which is the key attribute (asymmetric encryption) of NMA. Since TESLA was proposed, many scholars have mixed it with other encryption algorithms to achieve navigation message authentication, accordingly, improving the speed of navigation message authentication and the security of satellite communications. The sender who utilizes the TESLA generates a message authentication code (MAC) corresponding to a partial or all navigation message through an intermediate key (symmetrical key), and delays transmission of an intermediate key used to calculate the MAC. The symmetrical key belongs to a one-way function chain. Figure 22 is the model diagram of TESLA protocol.

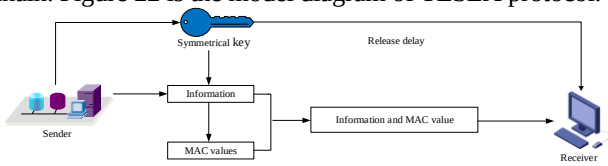

FIGURE 22. TESLA model.

As shown in Figure 22, the sender encrypts the information within a certain period of time using a key that is only known by itself and then generates a MAC value corresponding to the information in the time period. The sender sends the MAC value along with the information to the recipient. Since the receiver does not have a corresponding decryption key, it can only buffer the information and cannot authenticate the information. After a

TABLE XXXII
COMPARATIVE ANALYSIS OF VARIOUS PROTOCOL SCHEMES

Schemes	Caparra et al.'s scheme [107]	Fernandez -Hernandez et al.'s scheme [108]
Basic characteristics	This scheme is a navigation message authentication scheme based on the TESLA protocol, and each user using the scheme has a one-way key chain (SHA-256) function.	This scheme is a navigation message authentication scheme based on TESLA protocol. Each user using the scheme has a one-way keychain function and can cross-authenticate between different users.
Type of information protection	Navigation message information for GNSS	Navigation message information for Galileo open service signal
The integrity of scheme (Key management, massive users, etc.)	An effective spoofing attack is introduced to determine the optimal parameters of key generation required by navigation message authentication scheme by establishing a key design model. However, this scheme is only theoretical analysis, and whether this scheme can really protect all global satellite navigation signals remains to be considered.	The scheme manages and protects the key used in the authentication process. In addition, the scheme reduces authentication cost, communication cost and so on, and improves the robustness of the system, thereby improving the robustness of the system. However, there is not only a need to improve the key negotiation between the user and the satellite system, but also the delay of the TESLA key transmission.
Scheme implementation difficulty	High	Medium
Hardware Configuration	The keychain generation model designed by this scheme needs to be filled in multiple iterations. The key generation process is computationally complex and hardware implementation is difficult.	This scheme utilizes the improved TESLA protocol to use the same keychain function for all satellites to achieve cross-certification between different satellites, accordingly, enhancing satellite system stability. In addition, this scheme sets a variety of parameter indicators to evaluate its anti-spoofing performance.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

period of time, the sender releases the key, and the receiver obtains the key in some way to authenticate the buffered information.

Caparra et al.'s scheme proposed the one-way key chains generation algorithm model for the TESLA protocol [107]. This model provides an estimated collision probability and an upper bound to the entropy of keys generated. The experimental results show that this scheme can improve the robustness of the system. However, this scheme is only for theoretical analysis and lacks simulation under real spoofing environment. Fernandez-Hernandez et al. also designed a more complete navigation message authentication scheme based on the TESLA protocol, which is applied to the Galileo open service signal to shorten the navigation message authentication time and enhance the robustness of the system [108]. In addition, they also mentioned to the navigation message authentication scheme of cross certification. Their scheme can provide navigation message authentication with double assurance (i.e. when the satellite malfunction or restricted, the user can use the other satellite for message authentication, in order to guarantee system normal operation and safety). However, only when the transmitted navigation data (messages that need to be authenticated) is unpredictable, the cross-certification method can provide navigation message authentication for all satellites and resist RSA. Based on this, Fernandez-Hernandez et al. compared different types of TESLA protocols and finally got a more complete navigation message authentication scheme.

Based on the above research status, the analysis of the above various protocol schemes is shown in Table XXXII.

As shown in Table XXXII, Caparra et al.'s scheme is difficult to implement [107]. The main reason is that the hardware requirements of the scheme are high, the overall design of the scheme is relatively complete, and the receiver needs to produce a large computational overhead. Based on the analysis of the above various protocol schemes, the resistance of various schemes to different spoofing attacks is shown in Table XXXIII.

TABLE XXXIII
RESISTANCE OF VARIOUS PROTOCOL METHODS FOR DIFFERENT SPOOFING ATTACKS

Schemes	Caparra et al.'s scheme [107]	Fernandez -Hernandez et al.'s scheme [108]
Direct-replay spoofing attack	Moderate	Good
Replay spoofing attacks based on multiple antenna receivers	Poor	Moderate
Direct-generation spoofing attack	Good	Good
Analyze-generated spoofing attacks	Moderate	Moderate
SCER and FEA spoofing attacks	Poor	Poor
Full channel generated spoofing attack	Poor	Poor

Since Fernandez -Hernandez et al.'s scheme implements cross-certification between users, this scheme can resist replay spoofing attacks based on multiple antenna receivers [108]. In contrast, Caparra et al.'s method does not utilize cross-certification, so their scheme has lower anti-spoofing performance for replay spoofing attacks based on multiple antenna receivers [107]. Because the analyze-generated spoofing attack is to analyze the parameters of the received satellite signal, this spoofing attack has better spoofing effect than the direct generation spoofing attack. Therefore, Caparra et al.'s scheme [107] and Fernandez -Hernandez et al.'s scheme [108] have a general effect against analyze-generated spoofing attacks. The reason why Caparra et al. 's scheme [107] and Fernandez -Hernandez et al.' s scheme [108] have poor resistance to SCER and FER spoofing attacks is that their schemes have not been designed to resist SCER and FER spoofing attacks, and the present research has poor resistance to such spoofing attacks.

TABLE XXXIV
COMPARATIVE ANALYSIS OF VARIOUS NAVIGATION MESSAGE AUTHENTICATION AND PROTOCOL COMBINATION SCHEMES

Schemes	Yuan et al.'s scheme [109]	Kerns et al.'s scheme [110]
Basic characteristics	The scheme is based on a combination of ECDSA and TESLA. ECDSA is used to generate signatures for navigation message information and key information. The receiver receives the above information for super-frame authentication. TESLA is used for main-frame authentication.	The scheme is based on a combination of ECDSA and TESLA.
Type of information protection	BeiDou navigation message information	GPS civil navigation message information
The integrity of scheme (Key management, massive users, etc.)	In this scheme, the ECDSA algorithm generates a signature of both navigation information and key information and inserts them into the navigation information for transmission to protect the security of the key. From the perspective of the efficiency of the authentication process that can be completed every 2 minutes, more receivers can work simultaneously.	This scheme compares the advantages and disadvantages of ECDSA algorithm and TESLA protocol, and designs a navigation message authentication scheme based on EDSSA and TESLA. The scheme greatly reduces the authentication overhead while ensuring security, and the scheme involves protecting the key and managing the key.
Scheme implementation difficulty	Low	Medium
Hardware Configuration	The design of the scheme requires a key management center to perform key distribution, and the implementation of this scheme has lower hardware requirements for the receiver.	The scheme implements a lower playload on the civilian GPS signal and has lower communication overhead. There are lower hardware requirements for the receiver. However, the key distribution and protection of this scheme is more complicated.

C. NAVIGATION MESSAGE AUTHENTICATION AND PROTOCOL AUTHENTICATION COMBINATION

The protocol authentication scheme requires strict time synchronization between the sender and the receiver. In addition, considering that an anti-spoofing scheme using only one encryption authentication method cannot resist multiple spoofing attacks. Therefore, some scholars have proposed a scheme that combines a protocol authentication scheme with other encryption algorithms. Yuan et al. utilized the combination of ECDSA and TESLA to protect BeiDou civil navigation information [109]. On the one hand, this scheme used ECDSA algorithm to ensure the reliability of BeiDou civil information in the transmission process. On the other hand, the TESLA protocol is used to improve the authentication efficiency of the receiver. Although this scheme has high authentication efficiency, the resistance performance against multi-star spoofing attacks remains to be analyzed. Kerns et al. compared ECDSA and TESLA to propose a hybrid scheme based on the ECDSA-TESLA method [110]. They gave a modern civil navigation message authentication scheme from the aspects of certification overhead and implementation feasibility. This scheme greatly reduced the overhead of the user terminal while encrypting and protecting the navigation message.

Based on the above research status, the analysis of the above various navigation message authentication and protocol combination schemes is shown in Table XXXIV.

As shown in Table XXXIV, the main reason for the difficulty of the implementation of Yuan et al. is that the scheme has less analysis of spoofing attacks [109]. This scheme is only a theoretical analysis of the impact of noise on certification and involves less consideration of external factors. Based on the analysis of the above various navigation message authentication and protocol combination schemes, the resistance of various schemes to different spoofing attacks is shown in Table XXXV.

TABLE XXXV
RESISTANCE OF VARIOUS NAVIGATION MESSAGE AUTHENTICATION AND PROTOCOL COMBINATION SCHEMES FOR DIFFERENT SPOOFING ATTACKS

Schemes	Yuan et al.'s scheme [109]	Kerns et al.'s scheme [110]
Direct-replay spoofing attack	Moderate	Moderate
Replay spoofing attacks based on multiple antenna receivers	Poor	Poor
Direct-generation spoofing attack	Good	Good
Analyze-generated spoofing attacks	Moderate	Moderate
SCER and FEA spoofing attacks	Moderate	Moderate
Full channel generated spoofing attack	Poor	Poor

Yuan et al. [109] and Kerns et al. [110] established models and algorithms for resisting SCER and FEA spoofing attacks based on NMA, and verified the anti-spoofing performance of their schemes by simulation, so their schemes for SCER and FEA spoofing attacks have a general anti-spoofing effect. Since Yuan et al.'s scheme utilizes the TESLA protocol for authentication of each group of time, this scheme has a general deception effect on the direct replay type spoofing attack. The reason why Yuan et al.'s scheme [109] and Kerns et al.'s scheme [110] have poor resistance to replay spoofing attacks based on multiple antenna receivers and full-channel generated spoofing attacks is that neither of them involve multi-star spoofing attacks. Combined with the characteristics of the navigation message authentication scheme, most of the navigation message authentication schemes can better resist the direct-generation spoofing attack and analyze-generated spoofing attacks.

After comprehensively comparing the different types of navigation message authentication schemes, it is found that although the cryptographic algorithm-based navigation message authentication scheme has high security, it has poor detection performance for RSA in certain environments [110]. Although the protocol authentication scheme has the characteristics of low computation and strong robustness, the implementation of this scheme must ensure strict time synchronization between the sender and the receiver. The navigation message authentication scheme combined with the cryptographic algorithm and the protocol can improve the above deficiencies. However, how the sender combines the cryptographic algorithm with the protocol to make the anti-spoofing effect optimal still needs further consideration.

D. SPREADING CODE AUTHENTICATION

Spreading code authentication (SCA) is one of the message encryption technologies, and it is generally aimed at public civil spreading codes. The method achieves protection of unencrypted and public spreading code information by inserting some unpredictable chips (e.g., encrypted chips or watermark sequences) into the spreading code.

Since the GNSS signal transmission power of the spread spectrum modulation is lower than the power of the noise, the GNSS signal is buried in the noise signal. Therefore, it is difficult for the spoofer to accurately predict the spreading chips of SCA in this case unless the spoofer has certain information (such as encrypted information or authentication information) to generate unpredictable chips. In summary, the spreading code authentication technology inherently has the characteristics of good confidentiality of spread spectrum communication. Since the spreading code authentication process is a posterior process, there is a delay between the ground control segment transmitting unpredictable chips and the receiver receiving unpredictable chips. In combination with the above characteristics of the spreading code authentication, the spoofer will utilize this delay to implement a replay attack on the GNSS signal.

Pozzobon proposed a concept of signal authentication sequence (SAS) [111]. The SAS schematic is shown as

Figure 23. The SAS code generation is related to both the length of the SAS code and the first chip observation time of the stream cipher. On the ground segment, the sender encrypts the spreading code and uploads it to the satellite. On the space segment, signal authentication sequences are transmitted in the open-signal data messages. On the user segment, the receiver uses the received SAS to generate the spreading code which correlates with the decrypted spreading code. Through these processes, the receiver compares the calculated correlation peak with the saved correlation threshold to detect the spoofing signals. Pozzobon further studied the SCA scheme to propose a novel scheme for authentication of open GNSS signals using supersonic codes [112]. In this scheme, he multiplexed the supersonic code with the block cipher encryption of the spreading code. He also used code shift keying modulation to demodulate the encrypted spreading code at the receiver. Through the above process, the speed of GNSS signal authentication is accelerated, and the ability to resist reply attacks is enhanced. Furthermore, he further analyzed the designed scheme based on known spoofing attacks. From the analysis results, the open GNSS signals using supersonic codes have better anti-spoofing performance and lower authentication delay. Kuhn proposed a concept of hidden markers to implement the secret transmission of spreading codes [113]. The hidden marker is a rectangular pulse of the duration δ . It broadcasts with direct spread spectrum (DSSS) modulation by using a previously unpublished spreading sequence. The receiver can detect complex spoofing attacks by recording the arrival time of the hidden makers.

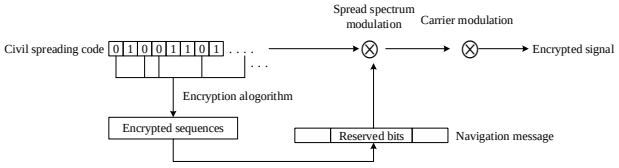

FIGURE 23. SAS schematic.

The three schemes based on the spreading code authentication are more difficult to implement because the robustness of the system based on the spreading code authentication is strong. In addition, the SCA system requires an independent time synchronization source and an additional buffer for the receiver to ensure high precision implementation of the spreading code authentication. Based on the analysis of the above various schemes of spreading code authentication, the resistance of various schemes to different spoofing attacks is shown in Table XXXVI.

TABLE XXXVI
RESISTANCE PERFORMANCE OF VARIOUS SPREADING CODE AUTHENTICATION SCHEMES FOR DIFFERENT SPOOFING ATTACKS

Schemes	Pozzobon et al.'s first scheme [111]	Pozzobon et al.'s second scheme [112]	Kuhn's scheme [113]
Direct-replay spoofing attack	Moderate	Moderate	Good
Replay spoofing attacks based on multiple antenna receivers	Poor	Poor	Good
Direct-generation spoofing attack	Good	Good	Good
Analyze-generated spoofing attacks	Moderate	Moderate	Moderate
SCER and FEA spoofing attacks	Moderate	Moderate	Moderate
Full channel generated spoofing attack	Poor	Moderate	Poor

From the point of view of spoofing party, it is easier to estimate the chip of navigation message authentication than the chip of spreading code authentication, because the premise of estimating the chip of spreading code authentication is that a high-gain receiving antenna is needed to receive weak signals reaching the ground. Therefore, the spread code authentication technology has better anti-spoofing effect against the SCER and FEA spoofing attacks than the navigation message authentication technology. For replay spoofing attacks based on multiple antenna receivers, the spreading code authentication technique also has a poor resistance to deception. Kuhn's scheme evaluated the detection performance of the scheme for RSA through experimental simulation, so it has better anti-spoofing effect on direct-replay spoofing attacks [113]. Pozzobon et al.'s second scheme evaluated a variety of channel propagation models and also detected the impact of noise on authentication [112]. Therefore, this scheme has a good anti-spoofing effect on full channel generated spoofing attacks.

E. SPREADING CODE ENCRYPTION

Spreading code encryption (SCE) is a method of encrypting a publicly spread code (i.e., civil spread code) and then transmitting it. In terms of whether the spread spectrum code is completely encrypted, the first category can be divided into the full spread spectrum code encryption scheme, namely spreading code encryption technology. The second category can be divided into partly spreading code encryption, namely watermark technology. In general, both SCE and watermarking techniques are methods of fully or partially encrypting the spreading code for the purpose of protecting it.

For civil satellites, the satellite's spreading code is publicly available. Therefore, both the spreading code encryption and the watermarking technology encryption are only for the spreading code of the civilian satellite signal, not the military satellite. Fernandez-Hernandez et al. encrypted the entire spreading code of the Galileo E6 service commercial signal, and also designed a navigation message authentication scheme based on the TESLA protocol [114]. This scheme theoretically proved the possibility of Galileo civil satellite signal spreading code encryption, but not all civilian satellites

can complete the protection by encrypting their spreading codes. In addition, the scheme not only realized the encryption process of the spreading code through hardware simulation, but also realized the function of high-accuracy authentication in the existing receiver. Rugamer et al.'s scheme designed a method that would allow civilian users to use public regulated service code information to protect their significant information [115]. In addition, their scheme also provided users with a server that can perform cross-authentication function, and all public regulated service code information is not disclosed to the public, but is saved by the receiver itself, which can save the key overhead problem. However, their scheme is only a theoretical study, and theexperimental simulation process in the real environment is not carried out.

Based on the analysis of the above various schemes of spreading code encryption, the resistance of various schemes to different spoofing attacks is shown in Table XXXVII.

TABLE XXXVII
RESISTANCE PERFORMANCE OF VARIOUS SPREADING CODE ENCRYPTION SCHEMES FOR DIFFERENT SPOOFING ATTACKS

Schemes	Fernandez-Hernandez et al.'s scheme [114]	Rugamer et al.'s scheme [115]
Direct-replay spoofing attack	Good	Good
Replay spoofing attacks based on multiple antenna receivers	Poor	Moderate
Direct-generation spoofing attack	Good	Good
Analyze-generated spoofing attacks	Moderate	Moderate
SCER and FEA spoofing attacks	Moderate	Moderate
Full channel generated spoofing attack	Poor	Poor

Like the spread spectrum code authentication technology, spread spectrum code encryption technology also has a good anti-spoofing effect when resisting SCER and FEA spoofing attacks. Rugamer et al.'s scheme can satisfy cross-certification between different users, so their scheme has better resistance in replay spoofing attacks based on multiple antenna receivers [115]. Like the spreading code authentication and the navigation message authentication, the spread code encryption has a poor anti-spoofing effect on the full channel generated spoofing attacks. Spreading code encryption has a good anti-spoofing effect on spoofing attacks on direct-generation spoofing attack and analyze-generated spoofing attacks.

F. WATERMARK TECHNIQUES

The technique of encrypting a part of the spreading code is called a watermarking technique for protecting the information of the spreading code. The watermark-related authentication scheme can be divided into two categories. The first type is the scheme proposed in reference [44]. Scoctt flooded the spread spectrum security code (SSSC) in thermal noise based on some unpredictable spreading code sequences. The receiver completes the authentication by verifying the unpredictable chips. In the above process, the receiver knows in advance the chip selection of the encrypted spreading code. The other type is that not only the chip selection of the encrypted spreading code is part of the encryption scheme, but also the choice of the chip changes over time [116]. In comparison, the latter has better security.

Based on the analysis of the above two watermarking techniques, their resistance to different spoofing attacks is shown in Table XXXVIII.

TABLE XXXVIII
RESISTANCE OF TWO WATERMARKING TECHNIQUES TO DIFFERENT SPOOFING ATTACKS

Schemes	Scoctt's scheme [44]	Anderson et al.'s scheme [116]
Direct-replay spoofing attack	Good	Good
Replay spoofing attacks based on multiple antenna receivers	Poor	Poor
Direct-generation spoofing attack	Good	Good
Analyze-generated spoofing attacks	Moderate	Moderate
SCER and FEA spoofing attacks	Moderate	Moderate
Full channel generated spoofing attack	Moderate	Poor

Like the spreading code authentication, the watermarking technology and the spreading code encryption have better anti-spoofing effects when resisting SCER and FEA spoofing attacks. However, the watermark technique only encrypts part of the spread spectrum codes, which saves the cost of authentication and makes it easier to implement. Scoctt's scheme [44] is designed for computers with strong computing power, so the scheme has a general anti-spoofing effect on the Analyze-generated spoofing attacks and full channel generated spoofing attacks.

G. COMBINED AUTHENTICATION

The above few sections are just some specific anti-spoofing techniques, and there are also some schemes that combine multiple message encryption techniques. For example, Curran et al. proposed a TESLA broadcast authentication encryption scheme based on a combination of NMA and SCE [117]. They proposed to encrypt the spreading code of the Galileo E6 signal pilot channel. The selection and allocation scheme of the encryption key is introduced in detail. Margaria et al. conducted a comparative analysis of the feasibility of existing civil GNSS signal authentication schemes [1]. By combining multiple deceptions, they proposed a more comprehensive encryption and authentication scheme for the next generation of civilian GNSS signals. However, the feasibility of the scheme is highly dependent on the complexity and compatibility of the receiving system. Motella et al. proposed a scheme based on

TABLE XXXIX

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

COMPARATIVE ANALYSIS OF VARIOUS COMBINED AUTHENTICATION SCHEMES

Schemes	Curran et al.'s scheme [117]	Margaria et al.'s scheme [1]	Motella et al.'s scheme [118]
Basic characteristics	The scheme protects navigation message information based on the navigation message authentication of the TESLA protocol and protects the spreading code based on the spreading code encryption technology.	This scheme combines the existing message encryption technology to propose a scheme combining navigation message authentication and spreading code authentication.	The scheme protects navigation message information based on the navigation message authentication scheme of the TESLA protocol and protects the spreading code based on the spreading code encryption technology.
Type of information protection	Galileo civil signal spreading code and navigation message information	Galileo E1 open service spreading code for civil signals	Galileo E1 open service spreading code and navigation message information for civil signals
The integrity of scheme (Key management, massive users, etc.)	This scheme introduces the key selection and distribution method in detail and can meet the needs of a large number of users in performance.	In this scheme, the authentication performance is judged by changing the parameters of relevant key to obtain the corresponding authentication delay, and the key management is not involved. However, this scheme can be used to analyze authentication blocking from the change of signal to noise ratio.	In terms of navigation message authentication, the scheme used a TESLA keychain to encrypt the navigation message by time slot. In terms of spreading code authentication, the scheme used CSK modulation to insert the authentication code into the spreading code by time slots. In addition, this scheme involves key management and allocation issues to ensure the security of the key.
Scheme implementation difficulty	Medium	Low	High
Hardware Configuration	This scheme is designed for the Key Management Center to select and assign keys, and the entire authentication process protects the ground, satellite and user.	This scheme is only a theoretical analysis and does not involve the relevant hardware simulation process.	The scheme uses CSK modulation to have higher requirements on receiving hardware, and the scheme involves time synchronization problem in key distribution, so it is difficult to implement.

spreading code and navigation message authentication (SNAP) [118]. Their scheme protects the navigation message and the spreading code information of the Galileo E1 OS signal. In terms of navigation message authentication, the scheme used a TESLA keychain to encrypt the navigation message by time slots. In terms of spreading code authentication, the scheme used CSK modulation to insert an authentication code into a spreading code by time slots. The experimental results show that the scheme has better resistance to estimated spoofing attacks and can meet different security requirements of users, but this scheme requires strict time synchronization.

Based on the above research status, the analysis of the above various combined authentication schemes is shown in Table XXXIX.

As shown in Table XXXIX, Motella et al.'s scheme is difficult to implement, mainly because of its high hardware configuration and high requirements for receiver synchronization [118]. Margaria et al.'s scheme is relatively difficult to implement, mainly because this scheme is only theoretical analysis and does not involve the relevant hardware simulation process [1]. Curran et al.'s scheme [117] is generally difficult to implement, because this scheme is relatively well designed relative to the Margaria et al.'s [1]. Based on the analysis of the above various combination of authentication schemes, the resistance of various schemes to different spoofing attacks is shown in Table XLTable XL

RESISTANCE OF VARIOUS COMBINED AUTHENTICATION SCHEMES TO DIFFERENT SPOOFING ATTACKS

Schemes	Curran et al.'s scheme [117]	Margaria et al.'s scheme [1]	Motella et al.'s scheme [118]
Direct-replay spoofing attack	Moderate	Moderate	Moderate
Replay spoofing attacks based on multiple antenna receivers	Moderate	Poor	Poor
Direct-generation spoofing attack	Good	Good	Good
Analyze-generated spoofing attacks	Moderate	Moderate	Moderate
SCER and FEA spoofing attacks	Moderate	Moderate	Moderate
Full channel generated spoofing attack	Moderate	Poor	Poor

Curran et al.'s scheme [117] is a combined authentication scheme based on NMA-SCE. NMA has a good spoofing effect on generation spoofing attacks, while SCE has a good spoofing effect on SCER and FEA spoofing attacks and RSA. Since the key selection scheme of Curran et al.'s method [117] changes over time and is part of the encrypted information, their scheme has a good anti-spoofing effect against the full channel generated spoofing attack. In addition,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

this scheme designs multi-user reception problem, so it has good anti-spoofing effect for replay spoofing attacks based on multiple antenna receivers. Margaria et al.'s scheme is a combined authentication scheme based on NMA-SCA [1]. NMA has a good spoofing effect on generation spoofing attacks, while SCA has a good spoofing effect on SCER and FEA spoofing attacks and RSA. Motella et al.'s scheme [118] is a combined authentication scheme based on NMA-SCE. NMA has a good spoofing effect on generation spoofing attacks, while SCE has a good spoofing effect on SCER and FEA spoofing attacks and RSA. Therefore, the schemes in reference [1] and reference [118] have similar resistance to various spoofing attacks.

H. NON-NAVIGATION MESSAGE ENCRPTION TECHNOLOGY

The non-navigation message encryption technology is from the perspective of the receiver, and it does not fall into the category of message encryption technology. This method only relies on the performance of the receiver to analyze the received navigation message and determine whether the received information is spoofed or not.

For some receivers with higher performance, the navigation message information from multiple satellites is combined and analyzed, and the information of a certain satellite can be inferred to be spoofing information through certain algorithms. Han et al. used RAIM technology and particle filtering technology to analyze the received navigation information [34]. The receiver uses the particle filter technology to reduce the dimensionality of the measured position information and speed information and improve the information precision of each dimension. The calculated result is detected by the analysis of the RAIM receiver to detect spoofing information. Zhang et al. utilized the Kalman filter position information parameter to determine whether the receiver received spoofing information [119]. Experiments showed that the method can be applied to highly dynamic receivers to detect fraud signals. However, since this method is computationally intensive, it is not suitable for a simple chip receiver. Anti-spoofing methods based on non-navigation message encryption technology generally make the receiver bear a large computational burden. Curran et al. used information coding to resist spoofing attacks [120]. This method performs better than the general cryptographic anti-spoofing method in resisting the influence of noise. However, this method requires a strong decoding capability at the receiving end, so it is not suitable for general receivers. Sun et al. proposed a new threat for pseudorange-based RAIM. They described the threat for pseudorange-based RAIM as an optimization problem, and then used the Fast Gradient SignMethod (FGSM) algorithm [120] to optimize the problem so as not to trigger the alert function of the target receiver. In other words, they did a spoofing attack, which could achieve the purpose of spoofing without triggering RAIM. However, they did not conduct defense analysis on the proposed attack model, which is worth considering in the future [121]. Liu et al. introduced a Kalman filter innovation based GNSS spoofing detection method and described the two techniques of innovation averaging and measurement averaging and their differences. This method has very promising application prospect for its high detection performance and easy software deployment [122]. Sun Minhong et al. proposed a new method of dimension reduction called axial integrated Wigner bispectrum (AIWB). AIWB is integrated WB along the direction parallel to one of the frequency axises on the bifrequency plane. This method utilize singular values of AIWB as the feature vector of the signal, and use support vector machine (SVM) to realize the identification of spoofing signals [123]. Daniele Borio et al. investigated GNSS receiver fingerprinting identification by the clock-derived metrics and implemented a filter approach for feature selection. Novel experimental results show that the adopted technique is time effective and three intrinsic features are sufficient to identify a receiver. While inter-model identification can be easily achieved with the methodology proposed, experimental results show that a different approach is required for intra-model identification [124].

Anti-spoofing methods based on non-navigation message encryption technology all require certain requirements on receiver hardware or computing power, which is not applicable to simple and portable small receivers or chip receivers. Based on the analysis of the above research status, it can be concluded that the anti-spoofing method of non-navigation message encryption technology is only a method to detect spoofing attacks based on the receiver level, while the anti-spoofing method based on message encryption technology is a relatively safe anti-spoofing method from the whole satellite system level. Therefore, no matter the difficulty of the implementation of the scheme, the anti-spoofing method based on the message encryption technology is relatively difficult to implement, or the anti-spoofing method based on the message encryption technology has better anti-spoofing performance. This paper does not compare the methods of non-navigation message encryption technology and their comparison of anti-spoofing performance for different spoofing methods.

I. SUMMARY

As for the classification of message encryption technology mentioned in this section, it can be divided into navigation message authentication (NMA), protocol authentication(PA), navigation message authentication and protocol authentication combination (NMA&PA), spreading code authentication (SCA), spreading code encryption(SCE), watermark techniques(WT), combined authentication (CA) and the non-navigation message encryption technology(Non-NMET). Combined with the characteristics of various methods, the anti-spoofing performance analysis of various

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

methods for different spoofing schemes is presented as follows. The analysis is shown in Table XLI.

The navigation message authentication method utilizes the scalable characteristics of the GNSS signal navigation message, and the satellite system control segment can perform asymmetric encryption processing on the GNSS signal to implement digital signature. In addition, the NMA only processes the navigation message and does not change the structural form of the signal, so the receiver does not need to change the receiver hardware, and the computational overhead of the receiver is less. Therefore, the NMA has a better anti-spoofing effect on generating spoofing attacks (including direct generation and analysis generation). However, real-time estimation of NMA chips is relatively simple, so NMA is less effective in estimating spoofing attacks. NMA has a low time delay requirement, so it has a poor resistance to RSA (including direct replay and multi-antenna replay). Protocol authentication requires higher time synchronization, so the protocol authentication method has better resistance to direct replay-type spoofing attacks. However, additional discussion is needed for the case of replay spoofing attacks based on multiple antenna receivers. Most protocol authentication schemes are less effective against such spoofing attacks. SCA and SCE inherently have the characteristics of confidentiality of spread spectrum communication. Since the verification process of SCA and SCE is a posteriori process, there will be a delay between transmitting unpredictable code and receiving unpredictable code in the ground control segment, and the spoofer will use this delay to replay the GNSS signal. Therefore, spreading code authentication and spreading code encryption have poor resistance to RSA (including direct replay and multi-antenna replay). Real-time estimation of SCA and SCE chips is difficult to implement, so spreading code authentication and spreading code encryption have better resistance to SCER and FEA spoofing attacks. At the same time, SCA, SCE, and navigation message authentication are better at resisting generation spoofing attacks, including direct generation and analysis generation, because they are all processes for signing and authentication based on certain information. As for the combined authentication method, it can only theoretically analyze the different combination schemes which may have better anti-spoofing effect to various spoofing methods. This paper is only a qualitative description, not representative. The non-navigation message encryption technology has a poor anti-spoofing effect in resisting the general spoofing attacks, but it can have a good anti-spoofing effect on the full channel generated spoofing attacks, because this method can combine the performance of the receiver with multiple receivers to resist spoofing of multi-channel satellite signals. However, other message encryption technologies have poor resistance to the full channel generated spoofing attacks.

TABLE XLI
ANTI-SPOOFING PERFORMANCE ANALYSIS OF VARIOUS METHODS

Scheme		NMA	PA	NMA&PA	SCA	SCE (WT)	CA	Non-NMET
Performance against spoofing attacks	Direct-replay spoofing attack [54]	Poor	Moderate	Good	Poor	Poor	Moderate	Poor
	Replay spoofing attacks based on multiple antenna receivers [6]	Poor	Poor	Moderate	Poor	Poor	Moderate	Poor
	Direct-generation spoofing attack [45]	Good	Good	Good	Good	Good	Good	Poor
	Analyze-generated spoofing attacks [46][47]	Good	Good	Good	Good	Good	Good	Poor
	SCER and FEA spoofing attacks [36] [54] [55]	Poor	Poor	Poor	Moderate	Moderate	Moderate	Poor
	Full channel generated spoofing attack [14] [49]	Poor	Poor	Poor	Poor	Poor	Moderate	Moderate

V. ANTI-SPOOFING TECHNOLOGY ANALYSIS OF COMBINED SPOOFING METHOD

Spoofing attack is one of the biggest security threats to navigation and positioning. Different deception scenarios could result in a wide variety of spoofing attack strategies. Spoofing attacks are versatile. Each type of spoofing detection or spoofing suppression method is usually effective against some specific spoofing scenarios. Not every anti-spoofing method is equally effective and feasible for all spoofing attacks. Moreover, it is also necessary to consider the additional cost of the self-developed or directly purchasing the required hardware facilities, the complexity of the setting operation, the implementation steps or the operation process, and the difficulty of the professional knowledge in the process of actually designing the anti-spoofing interference part of the receiver. Less difficult the cost and expertise difficulty required to implement a spoofing interference scenario is, the more likely it is to successfully implement a spoofing attack. The following is considered from the perspective of the receiver designer on the premise that the anti-spoofing interference performance is similar. If the implementation difficulty or the technical cost of anti-spoofing method is lower and spoofing interference scenes that could be resisted are more, the method is adopted by the receiver designer and applied to the actual receiver design more easily. A variety of practical application scenarios have different requirements for security and cost budget. The

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

appropriate anti-spoofing schemes can be selected according to specific design requirements.

This section analyzes the anti-spoofing methods including ten kinds of signal processing methods and seven kinds of information processing methods, and the resistance performance of these methods to the spoofing attack strategy for the combined spoofing scenario. The above contents provide some possible solutions for the design of anti-spoofing receivers in actual spoofing environments. Each kind of anti-spoofing method has its own characteristics, shortcomings and application scenarios. Combining the similarities and differences of various methods and merging several kinds of anti-spoofing methods, we can achieve better anti-spoofing performance by complementing their advantages and disadvantages as much as possible. Table XLII gives a comparative analysis of resistance performance to combined spoofing attack strategy for anti-spoofing methods based on the signal processing layer and the information processing layer. Table XLIII illustrates the meaning of the symbols in Table XLII.

TABLE XLII

COMPARISON OF RESISTANCE PERFORMANCE FOR ANTI-SPOOFING METHODS TO COMBINED SPOOFING ATTACKS

Attack mode	Anti-spoofing methods																
	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	M1	M2	M3	M4	M5	M6	M7
A11	▲	•	▲	▲	•	•	•	•	•	•	▼	•	✓	▼	▼	✓	▼
A12	▲	✓	•	•	▲	▲	•	•	•	▲	▼	•	✓	▼	▼	✓	▼
A21	▼	▼	•	•	▼	▼	▼	▼	▼	▼	✗	✗	•	✗	✗	✓	✗
A22	▼	•	▼	▼	•	•	▼	▼	▼	•	✗	✗	•	✗	✗	▲	✗
B11	✓	▲	✓	▲	▼	•	•	•	•	•	✓	✓	✓	✓	✓	✓	▼
B12	▲	✓	•	•	▲	▲	•	•	•	▲	▲	▲	▲	▲	▲	✓	▼
B13	✗	✗	▼	▼	▼	•	✗	•	▼	▼	•	•	•	•	•	▲	▼
B14	✗	✗	✗	▼	✗	▼	▼	•	✗	✗	•	•	•	•	•	▲	✗
B21	•	▼	•	•	▼	▼	▼	▼	▼	•	✓	✓	✓	✓	✓	✓	▼
B22	•	•	▼	▼	•	•	▼	▼	▼	•	▲	▲	▲	▲	▲	✓	▼
B23	✗	▼	▼	▼	▼	▲	▼	•	▼	•	•	•	•	•	•	▲	▼
B24	✗	✗	✗	▼	✗	•	▼	▼	✗	✗	•	•	•	•	•	▲	✗
B31	•	•	▼	▼	•	•	▼	▼	▼	•	▼	▼	▼	•	•	✓	▼
B32	▼	▼	▼	✗	▼	•	•	•	▼	▼	▼	▼	▼	•	•	✓	▼
B33	✗	✗	✗	▼	✗	✗	✗	•	✗	✗	✗	✗	✗	▼	▼	▲	✗
B41	•	▼	•	•	▼	▼	▼	▼	▼	▼	▼	▼	▼	•	•	✓	▼
B42	•	•	▼	▼	•	•	▼	▼	▼	•	▼	▼	▼	•	•	✓	▼
B43	✗	▼	▼	▼	▼	•	✗	•	▼	▼	▼	▼	▼	•	•	▲	▼
B44	✗	✗	✗	✗	✗	•	▼	▼	✗	✗	✗	✗	✗	▼	▼	▲	✗
B51	▼	✗	▼	▼	✗	▼	✗	✗	✗	▼	✗	✗	✗	✗	✗	▲	•
B52	▼	▼	▼	✗	▼	▼	✗	✗	✗	▼	✗	✗	✗	✗	✗	▲	▼
B53	▼	✗	▼	✗	▼	•	✗	▼	▼	▼	✗	✗	✗	✗	✗	•	▼
B54	✗	✗	✗	✗	▼	▼	✗	✗	✗	✗	✗	✗	✗	✗	✗	▼	✗

TABLE XLIII

MEANING OF EACH SYMBOL IN THE ABOVE TABLE

Combined spoofing attack strategy	Anti-spoofing method
A11 Selective delay Direct replay attack	S1 Spoofing detection based on Doppler shift
A12 Selective power Direct replay attack	S2 Spoofing detection method based on consistency check
A21 Selective delay Multi-antenna receiver replay attack	S3 Spoofing detection based on signal parameter statistics analysis
A22 Selective power Multi-antenna receiver replay attack	S4 Spoofing detection based on arrival time and arrival time difference
B11 Selective delay Direct-generation attack	S5 Residual signal detection
B12 Selective power Direct-generation attack	S6 Spoofing detection method based on Antenna array
B13 Denial environment Direct-generation attack	S7 Spoofing detection method based on angle of arrival
B14 Nulling Direct-generation attack	S8 Spoofing detection based on subspace projection
B21 Selective delay Analysis-generation attack	S9 Spoofing detection method based on signal arrival direction
B22 Selective power Analysis-generation attack	S10 Spoofing detection method based on signal quality monitoring
B23 Denial environment Analysis-generation attack	M1 Navigation message authentication
B24 Nulling Analysis-generation attack	M2 Protocol authentication
B31 Selective power SCER attack	M3 Navigation message authentication and protocol authentication combination

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

B32 Denial environment SCER attack	M4 Spreading code authentication
B33 Nulling SCER attack	M5 Spreading code encryption (Watermark techniques)
B41 Selective delay FEA attack	M6 Combined authentication
B42 Selective power FEA attack	M7 Non-navigation message encryption technology
B43 Denial environment FEA attack	✓- Good anti-spoofing performance ▲- Good moderately anti-spoofing performance ●- Moderate anti-spoofing performance ▼- Poor moderately anti-spoofing performance ✗-Poor anti-spoofing performance
B44 Nulling FEA attack	
B51 Selective delay Full-channel generation attack	
B52 Selective power Full-channel generation attack	
B53 Denial environment Full-channel generation attack	
B54 Denial environment Full-channel generation attack	

The advantages and disadvantages of the anti-spoofing performance are usually related to the difficulty of implementing spoofing attack, the effect of the spoofing attack, and the characteristics of the anti-spoofing method itself. If the deception strategy is more difficult to implement and the spoofing performance is better, then the spoofing detection or suppression technology may have a greater difficulty in achieving better anti-spoofing performance, and vice versa. The anti-spoofing methods based on the signal processing level and anti-spoofing performance for different combinations of spoofing means (as shown in Table VII) have been described in detail in section III. The characteristics of the anti-spoofing methods based on the information processing level, and anti-spoofing performance analysis of the methods are introduced correspondingly in section IV.

The following uses spoofing detection method based Doppler shift (S1) as an example to illustrate spoofing resistance performance of the anti-spoofing method on signal processing level. It can be seen from Table XXX that the method has better resistance performance to selective power spoofing and selective delay spoofing, and has less resistance performance to nulling attack and denial environment. Combined with the analysis of performance for spoofing attack in section II, the effect of selective delay spoofing attack is close to that of selective power spoofing attack. Both have weaker spoofing effects than denial environment. The spoofing performance of nulling attacks is better than denial environment. As can be seen from Table III, the spoofing effects of RSA, FSA, ESA, and ASA are sequentially enhanced one by one. Relatively speaking, the anti-spoofing method is weakened in response to these kinds of spoofing. Considering the spoofing attack performance comprehensively of the combined spoofing strategy, the difficulty of implementing direct replay spoofing is less than that of multi-antenna receiver replay spoofing. Therefore, the method has better anti-spoofing effect on combination of spoofing means A11 and A12. The resistance consequence to the combination spoofing means of A21 and A22 is generally good. Because the spoofing effects of analysis generation spoofing attack is better than that of direct generation spoofing attack, the B21, B22, B23, and B24 combination of spoofing attacks are more effective than the spoofing attacks corresponding to B11, B12, B13, and B14. Therefore, the method has better resistance performance to the B11, B12, B13 and B14 combination of spoofing means than the B21, B22, B23 and B24 combined spoofing means. Since the implementation difficulty of ESA is weaker than the full channel generation spoofing attack, the anti-spoofing effect of the method for ESA is slightly better than the anti-spoofing effect of the full channel generation spoofing attack.

The navigation message authentication scheme (M1) at the information processing level has poor anti-spoofing effect for most replay type spoofing attacks and has better anti-spoofing effect for most generation spoofing attacks. This type of method has a poor anti-spoofing effect on ESA and full channel generation spoofing attack. In addition, the relationship between the combinable spoofing means and the attack performance can be explained in the section II, i.e. selective delay spoofing ≈ selective power spoofing < denial environment < nulling attack. In summary, the navigation message authentication scheme has a poor anti-spoofing performance for A11 and A12; the multi-antenna receiver replay attack starts the deception process from multiple receivers, so the spoofing performance of the spoofing attack is better, so the anti-spoofing effect of A21 and A22 is extremely poor. The navigation message authentication scheme has better anti-spoofing effect on B11 and B12. Because the B11 spoofing method is less difficult to implement, the navigation message authentication scheme has better anti-spoofing performance on B11 than B12. From the perspective of the combinable spoofing attack effect (selective delay spoofing ≈ selective power spoofing < denial environment < nulling attack), the method has moderate anti-spoofing performance on B13 and B14. The anti-spoofing effect on B14 is even worse in some special cases. Similarly, the anti-spoofing performance of B21, B22, B23, and B24 is similar to B11, B12, B13, and B14 respectively. It can be seen from the analysis for the content of section IV that this method has poor anti-spoofing performance on ESA. Combined with the relationship among spoofing effects on above-mentioned combinable spoofing means, it can be concluded that M1 has a poor anti-spoofing effect on B31 and B41. However, due to the difficulty in implementing the B41 combination spoofing method is low , its anti-spoofing performance may achieve an moderate level in some cases. The implementation for selective power estimation spoofing attack and denial environment estimation spoofing attack is difficult. Therefore, it can be considered that the method has poor anti-spoofing performance on B32 and B43, and the anti-spoofing performance on B33 and B44 is extremely poor.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

The above describes how to qualitatively analyze the anti-spoofing performance of the anti-spoofing method based on the Doppler shift (S1) and the navigation message authentication method (M1) for different combinations of spoofing means (as shown in Table VII). Because the anti-spoofing performance analysis process of other anti-spoofing schemes for different combination spoofing means is similar, the specific analysis process of anti-spoofing interference performance for other anti-spoofing methods is not introduced and detailed one by one.

Among the ten types of anti-spoofing methods at signal processing-level shown in Table XLII, the front five methods (S1, S2, S3, S4, and S5) do not need to add additional hardware components such as antenna arrays and multiple antennas. But the methods only need to perform an internal firmware upgrade or embed for the existing system and are relatively easy to implement. The latter five methods (S6, S7, S8, S9, and S10) require additional antenna arrays or multiple antennas, which increases hardware implementation complexity and cost. The spoofing detection methods (M1-M7) at information level usually need to increase the key management center to supervise and operate the process of storing, distributing, updating, and deregistering keys, and have lower hardware requirements for the receiver. However, the spoofing detection method at information level requires the state to reconstruct the ground station and the space satellite segment separately. From this perspective, it could also increase the certain technical cost and implementation cost. According to the characteristics and advantages or disadvantages of the anti-spoofing method at signal processing level and the anti-spoofing method at information processing level listed in Table XLII, some of the methods can be combined to achieve better combined spoofing attack resistance performance. Table XLIV gives examples of anti-spoofing methods that can be combined.

From the combinations of various spoofing detection or spoofing suppression methods, four representative anti-spoofing methods are selected for comparison analysis as shown in Table XLIV. The following is a detailed description about one combination of anti-spoofing methods. The associated anti-spoofing method combined with residual signal detection technology (S5) and navigation message authentication (M1) firstly performs residual signal detection on the spoofing signal in the received signal during receiver acquisition and tracking phase. The scheme determines whether there is spoofing signal in the received signal and distinguishes spoofing signals. After demodulating the received signal, the content of the navigation message is authenticated by using a cryptographic method. The navigation message authentication technology has a good resistance performance to selective delay direct generation attack (B11). Using the residual signal detection technique only has a poor resistance performance to B11. The anti-spoofing method with the combination of the two technologies complements shortcomings of the single anti-spoofing method. Compared with a single method of spoofing detection, the combination of different anti-spoofing methods has a certain degree of improvement on the resistance performance for B11. If the user can afford

TABLE XLIV
COMPARATIVE ANALYSIS OF COMBINED ANTI-SPOOFING METHODS

Method category	Combined anti-spoofing method	Method characteristics	Required configuration	Implementation difficulty
Anti-spoofing attack method combined with information authentication technology without adding hardware facilities	Combined anti-spoofing method for spoofing detection method based on arrival time and arrival time difference (S4) and spread code authentication method (M4)	The scheme comprehensively analyzes the difference between the characteristics of the real signal and the spoofing and the information authentication result to realize spoofing detection.	This method requires an additional key management center.	The implementation of information authentication methods such as navigation message authentication methods requires not only upgrading and updating the firmware of the receiver, but also modifying the existing system and signal system. The combined anti-spoofing method integrating method at signal processing level and method at information processing level needs further improvement in system compatibility and performance reliability
	Combined anti-spoofing method for Residual signal detection method (S5) and navigation message authentication technology (M1)	The scheme combines spatial domain processing methods and navigation message information authentication means		
Combination of anti-spoofing technology that requires additional hardware implementation facilities with information authentication methods at the receiver end	Combined anti-spoofing method for spoofing detection method based on antenna array (S6) and Non-navigation message encryption technology (M7)	The scheme combines signal processing technology, information authentication and encryption methods	The receiver needs to configure the antenna array, multiple antennas, and key management centers.	This kind of anti-spoofing method requires antenna arrays or multiple antennas to be added. In addition, some of the schemes need to correct the antenna array used. Adding a key management center introduces additional overhead and solution complexity. Combining information authentication methods requires reconstructing the spatial signal system from the national level and increasing the overall budget of the program.
	Combined anti-spoofing method for spoofing detection method based on angle of arrival (S7) and protocol authentication (M2)	The scheme utilizes the spatial characteristics difference between the real signal and the spoofing signal, and the protocol authentication result to implement the spoofing attack detection.		

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3022294, IEEE Access

additional technology costs and hardware implementation costs, there are many effective and feasible combinations of anti-spoofing methods.

This section analyzes the anti-spoofing performance for the combination of different spoofing means in the two spoofing scenarios. In practical applications, the spoofing attacker may combine several spoofing modes to deceive the target receiver. The single anti-spoofing method has a very limited resistance performance to this complex spoofing attack method. And it is necessary to comprehensively consider the spoofing scenarios and implementation difficulties that anti-spoofing method at the signal processing level and the information level is applicable to. From the perspectives of scene adaptability, technical cost and scheme complexity for each type anti-spoofing method, we could choose the appropriate spoofing detection or spoofing suppression method.

VI. CHALLENGES AND FUTURE RESEARCH OF GNSS SYSTEM

A. CHALLENGES OF GNSS SYSTEM

Although the theories and technologies related to GNSS have developed rapidly in the past ten years, they still cannot meet the increasing service requirements of civilian users. GNSS spoofing technology and anti-spoofing technology exist in opposition. Any security loophole in the satellite navigation system may cause great problems and challenges to users. The following summarizes the common problems and urgent challenges that navigation users have today.

1) PVT ACCURACY ISSUES

With the introduction of GNSS into various fine operations, the current PVT accuracy can no longer meet the needs of civilian users. It is urgently hoped that the GNSS system can provide higher precision PVT calculation results. But if the user wants to improve the accuracy blindly, it will bring the influence of measurement error.

2) AVAILABILITY OF GNSS SYSTEM

The availability of GNSS is a percentage of the time the system's services can be used. The availability of GNSS is related to the number of satellites visible and the geometric distribution of satellites at a certain location or at a time. There are two factors affecting the number of visible satellites, one is the shelter angle and the other is the landscape of the user in the application environment. Generally speaking, the number of visible satellites will increase when the shielding angle is reduced, but the atmospheric delay and multipath problems will be more serious at the same time. The number of visible satellites also varies between cities and suburbs. At present, GNSS systems cannot solve this problem well.

The geometric distribution of satellites shows the uniformity of the spatial distribution for availability. Generally, the more uniform the spatial distribution, the more consistent the availability of GNSS in the coverage area. In addition, the failure of a satellite in the system will also affect the uniformity of the spatial distribution, which will lead to the availability of the GNSS system.

3) INTEGRITY OF GNSS SYSTEM

Integrity refers to the ability to warn users in the event of a GNSS failure, so that users can avoid being misled by a failed navigation system. As an auxiliary navigation system for the three flight phases of air routes, terminal areas and non-precision approaches in the US airspace, GPS can be used as the main navigation system in oceanic routes and remote areas. However, in the precision approach flight phase, using GPS alone cannot meet the system's integrity requirements.

4) ANTI-INTERFERENCE ABILITY OF GNSS SYSTEM

The anti-interference performance of GNSS is very important for both military and civilian users. After the advent of navigation warfare theory, many countries have even improved the anti- interference capability of GNSS to a strategic level. At present, the interference to GNSS signals includes potential interference and human interference. Potential interference includes in-band RF interference, out-of-band RF interference, environmental interference, and mutual interference between GNSS systems. Human interference includes those described in Section II of this paper. At present, many corresponding anti- interference technologies have been developed for interference, but these technologies are mainly aimed at the user segment, and the anti-interference capabilities of the space segment and the control segment are not yet mature.

B. FUTURE RESEARCH OF GNSS

1) SPACE SEGMENT

The future GNSS space segment should have the following characteristics.

a) Satellite orbits are diversified. Future GNSS constellations can try a combination of multiple orbits, which will not only facilitate the care of key areas, but also improve system availability.

b) Networking. The satellites in the constellation realize the transmission of information by establishing satellite-to-satellite links. Networking is conducive to completing the constellation time keeping and precise orbit determination functions, reducing dependence on the ground control segment, and enabling autonomous navigation for a long time.

c) Synergy. The GNSS system’s space segments can work together to achieve higher accuracy.

d) In addition to the above development points, the space segment can also choose other information carriers to pass information to users, such as quantum communication.

2) CONTROL SEGMENT

The control segment of GNSS in the future can be improved in the following aspects.

a) The control segment maintains real-time monitoring of the working status of all satellites to improve the integrity of the system.

b) The control segment learns from each other through international exchanges and uses the most advanced orbit determination and orbit measurement technology in the world to improve the accuracy of satellite position prediction.

c) The control segment uses more accurate atomic clocks and advanced anti-spoofing technology strategies.

3) USER SEGMENT

The user segment of GNSS in the future should have the following characteristics.

a) Supporting multiple system compatibility

b) Implementing software radio to provide a more flexible navigation solution

c) Using the most advanced anti-interference technology

4) AN ADVICE FOR THE FUTURE GNSS

a) The state and government should pay attention to the research on deception and interference methods, and promote the innovation of anti-deception and interference methods. With the continuous development of technology, the government must pay attention to the study of deception and interference. Otherwise, once a new deception attack mode appears, the previous deception protection methods may fail.

b) The reliability and stability of anti-spoofing methods still need to be further enhanced. Spoofing interference has its own unique characteristics, but also has characteristics similar to noise, suppression interference, multipath and other factors. The reliability and stability of the current detection algorithm for spoofing interference still need to be further improved.

c) The state and the government should also pay attention to the research of deception jamming suppression and deception jamming back tracking technology. The current research on anti-spoofing attack technology basically belongs to the category of deception detection, and there are few studies on deception jamming suppression.

d) The fusion of antenna array technology. Antenna array technology can play an important role in deception interference detection, deception interference suppression, and even deception interference reverse positioning, which can be used as an important aspect of future research on anti-spoof interference technology.

e) The application of cryptographic technology should be used reasonably.

VII. CONCLUSION

GNSS can be used in military and civilian applications to provide continuous, secure and reliable positioning, speed measurement and timing services for users who require navigation and location services. GNSS has been widely used in all aspects of people's life and work, so the authenticity and integrity of satellite navigation signals are particularly important. Spoofing and jamming have strong concealment and great harm. If the receiver suffers spoofing and jamming but does not take any spoofing and interference detection or suppression measures, the positioning results calculated by the receiver according to spoofing signal positioning solution are likely to cause huge positioning deviation. The research on anti-spoofing technology in foreign countries started earlier and more mature. Domestic research scholars mainly study traditional anti-spoofing methods and pay less attention to it. Therefore, it is necessary to carry out related research on spoofing attack detection and jamming suppression technology. In-depth study of spoofing and jamming strategy is very helpful to design a reasonable and effective anti-spoofing method, which makes the anti-spoofing method more targeted. So far, most anti-spoofing methods need to change the receiver equipment to achieve the purpose of anti-spoofing, except for some deception detection methods that can be completed outside the receiver (such as antenna array detection, and angle of arrival detection methods), Because the anti-spoofing detection can only be carried out when the detection method reaches the signal level or the information level, it is necessary to change the receiver equipment.

From the survey summarized in this article, it is found that no deception method can make all anti-spoofing technologies ineffective, and no anti-spoofing method can resist all deception attacks. Therefore, the future direction is to study a more complete anti-deception system as the deception model continues to advance. At the same time, we must also focus on the suppression of spoofed signals so that the satellite navigation system can provide services more safely and stably. In addition, people's growing dependence on GNSS has become a major incentive for criminals to attack and navigate civilian signals. In order to maintain the security of public services and ensure national security, continuous attention and tracking research on the text encryption technology for navigation and civil signals is required.

REFERENCES

[1] D. Margaria, B. Motella, M. Anghileri, J. Floch, I. Fernández-Hernández, and M. Paonni, “Signal structure-based authentication for civil GNSSs: recent solutions and perspectives,” *IEEE Signal Processing Magazine*, vol. 34, no. 5, pp. 27-37, Sep. 2017.

[2] S. Lo, D. D. Lorenzo, P. Enge, D. Akos, and P. Bradley, “Signal Authentication, A Secure Civil GNSS for Today,” *Inside GNSS*, vol. 4, no. 5, pp. 30-39, 2009.

[3] D. Yuan, H. Li, F. Wang, and M. Lu, “A GNSS acquisition method with the capability of spoofing detection and mitigation,” *Chinese Journal of Electronics*, vol. 27, no. 1, pp. 213-222, Jan. 2018.

[4] F. Wang, H. Li, and M. Lu, “GNSS spoofing detection based on unsynchronized double-antenna measurements,” *IEEE Access*, vol. 6, pp. 31203-31212, 2018.

[5] M. G. Amin, P. Closas, A. Broumandan, and J. L. Volakis, “Vulnerabilities, threats, and authentication in satellite-based navigation systems,” *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1169-1173, Jun. 2016.

[6] M. L. Psiaki, and T. E. Humphreys, “GNSS spoofing and detection,” *Proceedings of the IEEE*, vol. 104, no.6, pp. 1258-1270, Jun. 2016.

[7] S. Han, C. Lei, W. Meng, and C. Li, "Improve the security of GNSS receivers through spoofing mitigation," *IEEE Access*, vol. 5, pp. 21057-21069, Sep. 2017.

[8] A. Broumandan, R. Siddakatte, and G. Lachapelle, "Feature paper: An approach to detect GNSS spoofing," *IEEE Aerospace and Electronic Systems Magazine*, vol. 32, no. 8, pp. 64-75, Jun. 2017.

[9] Schmidt, Desmond & Radke, Kenneth & Camtepe, Seyit & Foo, Ernest & Ren, Michał. (2016). A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures. ACM Computing Surveys. 48. 1-31. 10.1145/2897166.

[10] G. X. Gao, M. Sgammini, M. Lu, and N. Kubo, "Protecting GNSS Receivers From Jamming and Interference," Proceeding of The IEEE, vol. 104, no. 6, pp. 1327-1337, Jun. 2016.

[11] L. Heng, D. B. Work, and G. X. Gao, "GPS signal authentication from cooperative peers," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 4, pp. 1794-1805, Aug. 2015.

[12] M. L. Psiaki, T. E. Humphreys, and B. Stauffer, "Attackers can spoof navigation signals without our knowledge. Here's how to fight back GPS lies," *IEEE Spectrum*, vol. 53, no. 8, pp. 26-53, Aug. 2016.

[13] L. A. van Mastrigt, A. J. van der Wal, and P. J. Oonincx, "Exploiting the doppler effect in GPS to monitor signal integrity and to detect spoofing," in *Proc. 2015 International Association of Institutes of Navigation World Congress (IAIN)*, Prague, Czech Republic, 2015.

[14] X. Xie, M. Lu, and D. Zeng, "Research on GNSS generating spoofing jamming technology," in *Proc. IET International Radar Conference 2015*, Hangzhou, China, 2015.

[15] H. Shen, "BeiDou-I satellite short message communication technology and application," *Practical Electronic*, vol. 23, pp. 106, 2014.

[16] C. Wullems, O. Pozzobon, and K. Kubik, "Signal authentication and integrity schemes for next generation global navigation satellite systems," in *Proc. European Navigation Conference GNSS*, Munich, Germany, 2005.

[17] A. Jovanovic, C. Botteron, and P. Fariné, "Multi-test detection and protection algorithm against spoofing attacks on GNSS receivers," in *Proc. 2014 IEEE/ION Position, Location and Navigation Symposium - PLANS 2014*, Monterey, CA, USA, 2014, pp. 1258-1271.

[18] C. Jiang, S. Chen, Y. Chen, Y. Bo, Q. Xia, and B. Zhang, "Analysis of the baseline data based GPS spoofing detection algorithm," in *Proc. 2018 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, Monterey, CA, USA, 2018, pp. 397-403.

[19] G. Caparra, S. Ceccato, S. Sturaro, and N. Laurenti, "A key management architecture for GNSS open service navigation message authentication," in *Proc. 2017 European Navigation Conference (ENC)*, Lausanne, Switzerland, 2017, pp. 287-297.

[20] Y. Hu, S. Bian, B. Li, and L. Zhou, "A novel array-based spoofing and jamming suppression method for GNSS Receiver," *IEEE Sensors Journal*, vol. 18, no. 7, pp. 2952-2958, Apr. 2018.

[21] S. Bian, Y. Hu, and B. Ji, "Research status and prospect of GNSS anti-spoofing technology," *Scientia Sinica Informationis*, vol. 47, no. 3, pp. 275-287, 2017.

[22] N. Zhang, "A case study on the application of GPS forward spoofing jamming in UAV," Aerospace China, vol. 7, pp. 40-42, 2015.

[23] T. E. Humphreys, "UT Austin Researchers Spoof Superyacht at Sea," *The University of Texas at Austin*, [Online]. Available: http://www.engr.utexas.edu/features/superyacht-gps-spoofing

[24] M. L. Psiaki, T. E. Humphreys, "Protecting GPS from spoofers is critical to the future of navigation," *IEEE Spectrum*, [Online]. Available: https://spectrum.ieee.org/telecom/security/protecting-gps-from-spoofers-is-critical-to-the-future-of-navigation

[25] United States Department of Transportation, "2017-005A-Black Sea-GPS Interference," *Marad*, [Online]. Available: https://www.maritime.dot.gov/content/2017-005a-black-sea-gps-interference

[26] D. Goward, "Mass GPS Spoofing Attack in Black Sea?," *The Maritime Executive*, [Online]. Available: https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea

[27] R. Morales-Ferre, P. Richter, E. Falletti, A. Fuente, and E. S. Lohan, "A Survey on Coping With Intentional Interference in Satellite Navigation for Manned and Unmanned Aircraft," *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*, vol. 22, no. 1, pp. 249-291, 2020.

[28] L. Wang, R. Wu, W. Wang, D. Lu, and Q. Jia, "Joint GNSS Interference Mitigation Approach for Jamming and Spoofing Based on Multi-antenna Array," *Journal of Electronics and Information Technology*, vol. 38, no. 9, pp. 2344-2350, Sep. 2016.

[29] K. Dong, Z. Zhang, and X. Xu, "A hybrid interference suppression scheme for global navigation satellite systems," in *Proc. 2017 9th International Conference on Wireless Communications and Signal Processing (WCSP)*, Nanjing, China, 2017.

[30] P. Risbud, N. Gatsis, and A. Taha, "Vulnerability analysis of smart grids to GPS spoofing," *IEEE Transactions on Smart Grid*, vol. 10, no.4, pp. 3535-3548, Jul. 2018.

[31] C. Konstantinou, M. Sazos, A. S. Musleh, A. Keliris, A. Al-Durra, and M. Maniatakos, "GPS spoofing effect on phase angle monitoring and control in a real-time digital simulator-based hardware-in-the-loop environment," *IET Cyber-Physical Systems: Theory & Applications*, vol. 2, no. 4, pp. 180-187, Dec. 2017.

[32] R. T. Ioannides, T. Pany, G. Gibbons, "Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1174-1194, Jun. 2016.

[33] J. Li, J. Zhang, S. Chang, and M. Zhou, "Performance evaluation of multimodal detection method for GNSS intermediate spoofing," *IEEE Access*, vol. 4, pp. 9459-9468, Sep. 2016.

[34] S. Han, D. Luo, W. Meng, and C. Li, "Antispoofing RAIM for dual-recursion particle filter of GNSS calculation," *IEEE Transactions on Aerospace & Electronic Systems*, vol. 52, no. 2, pp. 836-851, Apr. 2016.

[35] X. Ouyang, F. Zeng, P. Hou, and R. Guo, "Analysis and evaluation of spoofing effect on GNSS receiver," in Proc. 2015 IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom), Beijing, China, 2015.

[36] K. Wesson, M. Rothlisberger, and T. Humphreys, "Practical cryptographic civil GPS signal authentication," *Navigation*, vol. 59, no.3, pp. 177-193, Feb. 2012.

[37] L. Huang, Z. Lv, and F. Wang, "Spoofing pattern research on GNSS Receivers," *Journal of Astronautics*, vol. 33, no. 7, pp. 884-890, Jul. 2012.

[38] J. Zidan, E. I. Adegoke, E. Kampert, S. A. Birrell, C. R. Ford and M. D. Higgins, "GNSS Vulnerabilities and Existing Solution: A Review of the Literature," *IEEE Access*, vol. 4, pp. 1-17, 2016.

[39] Z. Gao, and F. Meng, "Principle and simulation research of GPS repeater deception jamming," *Journal of Telemetry, Tracking and Command*, vol. 32, no. 6, pp. 44-47, Nov. 2011.

[40] L. Huang, H. Gong, X. Zhu, and F. Wang, "Research of re-radiating spoofing technique to GNSS timing receiver," *JOURNAL OF NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY*, vol. 35, no. 4, pp. 93-96, Aug. 2013.

[41] S. Wang, J. Gao, Y. Wang, J. Liu, and H. Li, "GPS repeater deception jamming technology based on delay control," *MISSILES AND SPACE VEHICLES*, vol. 352, no. 2, pp. 103-106, 2017.

[42] M. Shi, S. Chen, and Z. Liu, "Analysis and optimizing of time-delay in GPS repeater deception," *Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition)*, vol. 29, no.1, pp. 56-61, Feb. 2017, pp. 1430-1434.

[43] S. Bian, Y. Hu, C. Chen, Z. Li, and B. Ji, "Research on GNSS repeater spoofing technique for fake Position, fake time & fake velocity," in *Proc. 2017 IEEE International Conference on Advanced Intelligent Mechatronics (AIM)*, Munich, Germany, 2017.

[44] L. Scott, "Anti-spoofing & authenticated signal architectures for civil navigation systems," in Proc. Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003), Portland, OR, Sep. 2003, pp. 1543-1552.

[45] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the spoofing threat," *GPS World*, vol. 20, no.1, pp. 28-39, Jan. 2009.

[46] B. Dai, M. Xiao, and S. Huang, "GPS spoofing and inducing model of UAV," *Communications Technology*, vol. 50, no. 3, pp. 496-501, Mar. 2017.

[47] L. He, W. Li, and C. Guo, "Study on GPS generated spoofing attacks," *Application Research of Computers*, vol. 33, no. 8, pp. 2405-2408, Aug. 2016.

[48] M. Shi, S. Chen, H. Wu, and H. Mao, "A GPS spoofing pattern based on denial environment," *Journal of Air Force Engineering University (Natural Science Edition)*, vol. 16, no.6, pp. 27-31, Dec. 2015.

[49] S. Huang, S. Chen, B. Yang, and H. Wu, "A power control strategy of multiple GNSS spoofing signals," *Journal of Air Force Engineering University (Natural Science Edition)*, vol. 18, no. 1, pp. 76-80, Feb. 2017.

[50] E. Schmidt, Z. Ruble, D. Akopian and D. J. Pack, "Software-defined radio GNSS instrumentation for spoofing mitigation: A Review and a Case Study," *IEEE Transactions on Instrumentation and Measurement*, vol. 68, no. 8, 2768-2784, 2019.

[51] H. Wang, Z. Yao, Z. Fan, and T. Zheng, "Experiment study of spoofing jamming on GPS receiver," *Fire Control & Command Control*, vol. 41, no. 7, pp. 184-187, Jul. 2016.

[52] K. Ma, X. Sun, and Y. Nie, "Research on key technologies of GPS generated spoofing," *Aerospace electronic confrontation*, vol. 30, no. 6, pp. 24-26+34, 2014.

[53] D. Fabio, (2015, Mar. 18). "GNSS interference, threats, and countermeasures," *Radar Receivers*, [Online]. Available: http://www.artechhouse.com/Main/Books/GNSS-Interference-Threats-and-Countermeasures-2216.aspx

[54] T. E Humphreys, "Detection strategy for cryptographic GNSS anti-spoofing," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 2, pp. 1073-1090, Apr. 2013.

[55] J. T. Curran, and C. O'Driscoll, "Message authentication, channel coding & anti-spoofing," in Proc. Proceedings of the 29th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2016), Portland, Oregon, Sep. 2016, pp. 2948-2959.

[56] B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller, "An in-line anti-spoofing device for legacy civil GPS receivers," in *Proc. Proceedings of the 2010 International Technical Meeting of The Institute of Navigation*, San Diego, CA, Jan. 2010, pp. 698-712.

[57] G. Zhang, Y. Zhang, and Y. Tian, "Research of Beidou navigation satellite system (BDS) spoofing detection based on DOD and PTD," *Applied Science and Technology*, vol. 46, no. 2, pp. 35-41, Mar. 2019.

[58] W. Qi, Y. Zhang, and X. Liu, "A GNSS anti-spoofing technology based on Doppler shift in vehicle networking," in *Proc. 2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*, Paphos, Cyprus, USA, Sep. 2016, pp. 725-729.

[59] A. Broumandan, A. Jafania-Jahromi, V. Dehghanian, J. Nielsen, and G. Lachapelle, "GNSS spoofing detection in handheld receivers based on signal spatial correlation," in *Proc. Proceedings of the 2012 IEEE/ION Position, Location and Navigation Symposium*, Myrtle Beach, SC, USA, Apr. 2012, pp. 479-487.

[60] J. Tu, X. Zhan, M. Chen, H. Gao, and Y. Chen, "GNSS intermediate spoofing detection via dual-peak in frequency domain and relative velocity residuals," *IET Radar, Sonar&Navigation*, vol. 14, no. 3, pp. 439-447, 2020.

[61] L. Yao, Z. Geng, Y. Su, and J. Nie, "The characteristics of single antenna repeater jamming coordinates mappings," *GNSS World of China*, vol. 40, no. 5, pp. 19-24, Oct. 2015.

[62] A. Broumandan, A. Jafarnia-Jahromi, S. Daneshmand, and G. Lachapelle, "Overview of spatial processing approaches for GNSS structural interference detection and mitigation," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1246-1257, Jun. 2016.

[63] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans, "GNSS signal authentication via power and distortion monitoring," *IEEE Transactions on Aerospace Electronic Systems*, vol. 54, no. 2, pp. 739-754, Apr. 2018.

[64] D. Borio, "PANOVA tests and their application to GNSS spoofing detection," *IEEE Transactions on Aerospace & Electronic Systems*, vol. 49, no. 1, pp. 381-394, Jan. 2013.

[65] D. Borio, and C. Gioia, "A sum-of-squares approach to GNSS spoofing detection," *IEEE Transactions on Aerospace & Electronic Systems*, vol. 52, no. 4, pp. 1756-1768, Aug. 2016.

[66] E. Falletti, B. Motella, and M. T. Gamba, "Post-correlation signal analysis to detect spoofing attacks in GNSS receivers," in *Proc. 2016 24th European Signal Processing Conference (EUSIPCO)*, Budapest, Hungary, Aug. 2016, pp. 1048-1052.

[67] P. Y. Hwang, and G. A. Mcgraw, "Receiver autonomous signal authentication (RASA) based on clock stability analysis," in *Proc. 2014 IEEE/ION Position, Location and Navigation Symposium - PLANS 2014*, Monterey, CA, USA, May. 2014, pp. 270-281.

[68] D. Yuan, H. Li, and M. Lu, "A method for GNSS spoofing detection based on sequential probability ratio test Position," in *Proc. 2014 IEEE/ION Position, Location and Navigation Symposium - PLANS 2014*, Monterey, CA, USA, May. 2014, pp. 351-358.

[69] F. Wang, H. Li, and M. Lu, "ARPSO-MLE based GNSS anti-spoofing method," in *Proc. 2015 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, Ningbo, China, Sep. 2015.

[70] J. N. Gross, C. Kilic, and T. E. Humphreys, "Maximum-likelihood power-distortion monitoring for GNSS signal authentication," *IEEE Transactions on Aerospace & Electronic Systems*, vol. 55, no. 1, pp. 1-6, Feb. 2019.

[71] Z. Zhang, X. Zhan, and Y. Zhang, "GNSS spoofing localization based on differential code phase," in *Proc. 2017 Forum on Cooperative Positioning and Service (CPGPS)*, Harbin, China, May. 2017, pp. 338-344.

[72] Y. Li. B. Wei, and X. Gan, "Research on anti-spoofing technology for navigation satellite receiver," *Radio Engineering*, vol. 46, no. 3, pp. 49-53, 2016.

[73] K. Ali, E. G. Manfredini, and F. Dovis, "Vestigial signal defense through signal quality monitoring techniques based on joint use of two metrics," in *Proc. 2014 IEEE/ION Position, Location and Navigation Symposium - PLANS 2014*, Monterey, CA, USA, Jul. 2014, pp. 1240-1247.

[74] Y. Wei, H. Li, and M. Lu, "Spoofing profile estimation-based GNSS spoofing identification method for tightly coupled MEMS INS-GNSS integrated navigation system," *IET Radar, Sonar&Navigation*, vol. 14, no. 2, pp. 216-225, 2020.

[75] A. Felski, "Methods of improving the jamming resistance of GNSS receiver," *Annual of Navigation*, vol. 23, no. 1, pp. 49-53, Dec. 2016.

[76] C. -L. Chang, "Multiplexing scheme for anti-jamming global navigation satellite system receivers," *IET Radar, Sonar and Navigation*, vol. 6, no. 6, pp. 443-457, July. 2012.

[77] L. Wang, S. Li, Y. Zhang, and R. Wu, "Spoofing interference suppression in GNSS using repeated CLEAN," *Journal of Signal Processing*, vol. 31, no. 12, pp. 1636-1641, Dec. 2015.

[78] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandan, and G. Lachapelle, "A GNSS structural interference mitigation technique using antenna array processing," in *Proc. 2014 IEEE 8th Sensor Array and Multichannel Signal Processing Workshop (SAM)*, A Coruna, Spain, Jun. 2014, pp. 109-112.

[79] D. Ge, G. Zhou, D. Xu, and R. Mao, "GPS receiver anti-deceptive jamming method based on space-time multi-antenna null," *Journal of Sichuan Ordnance*, vol. 36, no. 8, pp. 41-45, Aug. 2015.

[80] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, "Receiver-autonomous spoofing detection: experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer," in Proc. *ION 2009 International Technical Meeting*, Anaheim, CA, Jan. 2009, pp. 124-130.

[81] P. Wang, Y. Wang, E. Cetin, A. G. Dempster, and S. Wu, "GNSS jamming mitigation using adaptive-partitioned subspace projection technique," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 55, no. 1, pp. 343-355, Feb. 2019.

[82] G. Xu, F. Shen, M. Amin, and C. Wang, "DOA classification and CCPM-PC based GNSS spoofing detection technique, " in *Proc. 2018 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, Monterey, CA, USA, Apr. 2018, pp. 389-396.

[83] R. Shi, and J. Liang, "Detection on navigation deception signals based on INS and GNSS attitude measurement," in *Proc. The 9th China Satellite Navigation Conference*, Harbin, China, May. 2018, pp. 23-27.

[84] E. G. Manfredini, F. Dovis, and B. Motella, "Validation of a signal quality monitoring technique over a set of spoofed scenarios," in *Proc. 2014 7th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, Noordwijk, Netherlands, Dec. 2014, pp. 1-7.

[85] A. J. Jahromi, A. Broumandan, S. Daneshmand, G. Lachapelle, and R. T. Ioannides, "Galileo signal authenticity verification using signal quality monitoring methods," in *Proc. 2016 International Conference on Localization and GNSS (ICL-GNSS)*, Barcelona, Spain, Jun. 2016, pp. 1-8.

[86] A. Broumandan, A. Jafarnia-Jahromi, G. Lachapelle, and R. T. Ioannides, "An approach to discriminate GNSS spoofing from multipath fading," in *Proc. 2016 8th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, Noordwijk, Netherlands, Feb. 2017, pp. 1-10.

[87] T. Kim, C. S. Sin, S. Lee, and J. H. Kim, "Analysis of effect of anti-spoofing signal for mitigating to spoofing in GPS L1 signal," in *Proc. 2013 13th International Conference on Control, Automation and Systems (ICCAS 2013)*, Gwangju, South Korea, Oct. 2013, pp. 523-526.

[88] M. Berardo, E. G. Manfredini, F. Dovis, and L. L. Presti, "A spoofing mitigation technique for dynamic applications," in Proc. 2016 8th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), Noordwijk, Netherlands，Dec. 2016, pp. 1-7.

[89] L. Zhao, Z. Miao, B. Zhang, B. Liu, G. Li, and X. Zhou, "A novel spoofing attack detection method in satellite navigation tracking phase," *Journal of Astronautics*, vol. 36, no. 10, pp. 1172-1177, Oct. 2015.

[90] S. Bhamidipati, T. Y. Mina, and G. X. Gao, "GPS time authentication against spoofing via a network of receivers for power systems," in *Proc. 2018 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, Monterey, CA, USA, Apr. 2018, pp. 1485-1491.

[91] J. Wang, H. Li, X. Cui, and M. Lu, "A new method in acquisition to detect GNSS spoofing signal," in *Proc. Proceedings 2013 International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC)*, Shenyang, China, Dec. 2013, pp. 2913-2917.

[92] L. Cai, X. Sun, G. Fan, and C. Wu, "Deception detection method in multipath environment," *Modern Defence Technology*, vol. 45 no. 5, pp. 72-77+99, Oct. 2017.

[93] H. Li, and X. Wang, "Detection of GPS spoofing through signal multipath signature analysis," in *Proc. 2016 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, Vancouver, BC, Canada, May. 2016, pp. 1-5.

[94] A. Khalajmehrabadi, N. Gatsis, D. Akopian, and A. F. Taha, "Real-time rejection and mitigation of time synchronization attacks on the global positioning system," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 8, pp. 6425-6435, Aug. 2018.

[95] N. Carson, S. M. Martin, J. Starling, and D. M. Bevly, "GPS spoofing detection and mitigation using cooperative adaptive cruise control system," in *Proc. 2016 IEEE Intelligent Vehicles Symposium (IV)*, Gothenburg, Sweden, Jun. 2016, pp. 1091-1096.

[96] S. Han, D. Luo, W. Meng, and C. Li, "A novel anti-spoofing method based on particle filter for GNSS," in *Proc. 2014 IEEE International Conference on Communications (ICC)*, Sydney, NSW, Australia, Jun. 2014, pp. 5413-5418.

[97] S. Shang, H. Li, C. Peng, and M. Lu, "A Novel Method for GNSS Meaconer Localization Based on a Space-Time Double Difference Model," *IEEE Transactions on Aerospace and Electronic Systems*, 2020, DOI 10.1109/TAES.2020.2974034

[98] K. D. Wesson, B. L. Evans, and T. E. Humphreys, "A combined symmetric difference and power monitoring GNSS anti-spoofing technique," in *Proc. 2013 IEEE Global Conference on Signal and Information Processing*, Austin, TX, USA, Dec. 2013, pp. 217-220.

[99] Y. Gao, H. Li, M. Lu, and Z. Feng, "Intermediate spoofing strategies and countermeasures," *Tsinghua Science and Technology*, vol. 18, no. 6, pp. 599-605, Dec. 2013.

[100] X. Liu, and L. Zhang, "Research and implementation of GNSS anti-spoofing interference positioning algorithm based on multiple antennas," in *Proc. The 12th Signal and Intelligent Information Processing and Applications National Academic Conference*, Hangzhou, China, Apr. 2018.

[101] X. Chen, G. Lenzini, M. Martins, S. Mauw and J. Pang, "A trust framework for evaluating GNSS signal integrity," in *Proc. 2013 IEEE 26th Computer Security Foundations Symposium, New Orleans*, LA, USA, Jun. 2013, pp. 179-192.

[102] D. Maier, K. Frankl, R. Blum, B. Eissfeller, and T. Pany, "Preliminary assessment on the vulnerability of NMA-based Galileo signals for a special class of record & replay spoofing attacks"," in *Proc. 2018 IEEE/ION Position Location and Navigation Symposium (PLANS)*, Monterey, CA, USA, 2018, pp. 63-71.

[103] K. CHINO, D. MANANDHAR, and R. SHIBASAKI, "Authentication technology using QZSS," In *Proc. 2014 IEEE/ION Position, Location and Navigation Symposium - PLANS 2014*, Monterey, CA, USA, May. 2014, pp. 367-372.

[104] Z. Wu, R. Liu and H. Cao, "ECDSA-based message authentication scheme for BeiDou-II navigation satellite system," *IEEE Transactions on Aerospace and Electronic Systems*, Oct. 2018.

[105] Z. Wu, Y. Zhang, and R. Liu, "BD-II NMA&SSI: An scheme of anti-spoofing and open BeiDou II D2 navigation message authentication," *IEEE Access*, vol. 8, pp. 23759-23775, 2020.

[106] M. Luk, A. Perrig, and B. Whillock, "Seven Cardinal Properties of Sensor Network Broadcast Authentication," in *Proc. Proceedings of the 4th ACM Workshop on Security of ad hoc and Sensor Networks*, Alexandria, VA, USA, Oct. 2006.

[107] G. Caparra, S. Sturaro, N. Laurenti, and C. Wullems, "Evaluating the security of one-way key chains in TESLA-based GNSS navigation message authentication schemes," In *Proc. 2016 International Conference on Localization and GNSS (ICL-GNSS)*, Barcelona, Spain, Aug. 2016, pp. 1-6.

[108] I. Fernández-Hernández, V. Rijmen, G. Seco-Granados, J. Simon, I. Rodriguez, and J. D. Calle, "A navigation message authentication proposal for the Galileo open service," *Navigation*, vol. 63, no.1, pp. 85-102, 2016.

[109] M. Yuan, Z. Lv, H. Chen, J. Li, and G. Ou, "An implementation of navigation message authentication with reserved bits for civil BDS anti-spoofing," *China Satellite Navigation Conference (CSNC) 2017 Proceedings*, vol. 2, pp. 69-80, 2017.

[110] A. J. Kerns, K. D. Wesson, and T. E. Humphreys, "A blueprint for civil GPS navigation message authentication," in *Proc. 2014 IEEE/ION Position, Location and Navigation Symposium - PLANS 2014*, Monterey, CA, USA, 2014, pp. 262-269.

[111] O. Pozzobon, "Keeping the spoofs out: signal authentication services for future GNSS," *Inside GNSS*, Jun. 2011, pp. 48-55.

[112] O. Pozzobon, G. Gamba, S. Fantinato, and G. Hein, "From data schemes to supersonic codes: GNSS authentication for modernized signals," *Inside GNSS*, vol. 10, no.1, pp. 55-64, Feb. 2015.

[113] M. G. Kuhn, "An asymmetric security mechanism for navigation signals," in *Proc. Proceedings of the 6th international conference on Information Hiding*, 2004, pp. 239-252.

[114] I. Fernández-Hernández, I. Rodríguez, G. Tobías, J. D. Calle, E. Carbonell, G. Seco-Granados, et at. "Galileo's commercial service: testing GNSS high accuracy and authentication," *Inside GNSS*, vol. 10, no. 1, pp. 38-48, Feb. 2015.

[115] A. Rügamer, M. Stahl, I. Lukcin, G. Rohmer, "Privacy protected localization and authentication of georeferenced measurements using Galileo PRS," in *Proc. 2014 IEEE/ION Position, Location and Navigation Symposium - PLANS 2014*, Monterey, CA, USA, Jul. 2014, pp. 478-486.

[116] J. M. Anderson, K. L. Carroll, N. P. DeVillbiss, J. T. Gillis, J. C. Hinks, et al. "Chips-Message Robust Authentication(Chimera)for GPS Civilian Signals," in *Proc. 30th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2017)*, Nov. 2017, pp. 2388-2416.

[117] J. T. Curran, and M. Paonni, "Securing GNSS: an end-to-end feasibility study for the Galileo open service," in Proc. Proceedings of the 27th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2014), Tampa, Florida, Sep. 2014, pp. 2828-2842.

[118] B. Motella, D. Margaria, M. Paonni, "SNAP: an authentication concept for the Galileo open service," in *Proc. Proceedings of IEEE/ION PLANS 2018*, Monterey, CA, 2018, pp. 967-977.

[119] T. Zhang, J. Gao, and F. Ye, "Anti-spoofing algorithm based on adaptive Kalman filter for high dynamic positioning," in *Proc. IEEE 2017 Progress in Electromagnetics Research Symposium - Fall (PIERS - FALL)*, Singapore, 2017, pp. 838-845.

[120] J. T. Curran, M. Navarro, M. Anghileri, P. Closas, and S. Pfletschinger, "Coding Aspects of Secure GNSS Receivers," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1271-1287, 2016.

[121] Y. Sun, and L. Fu, "A New Threat for Pseudorange-Based RAIM:Adversarial Attacks on GNSS Positioning," *IEEE Access*, vol. 7, pp. 126051-126058, 2019.

[122] Y. Liu, S. Li, Q. Fu, Z. Liu, and Q. Zhou, "Analysis of Kalman Filter Innovation-Based GNSS Spoofing Detection Method for INS-GNSS Integrated Navigation System," *IEEE SENSORS JOURNAL*, vol. 19, no. 13, pp. 5167-5178, 2019.

[123] M. Sun, L. Zhang, J. Bao, Y. Yan, "RF fingerprint extraction for GNSS anti-spoofing using axial integrated Wigner bispectrum," *Journal of Information Security and Applications*, vol. 35, pp. 51-54, 2017

[124] D. Borio, C. Gioia, E. Pons, and G. Baldini, "GNSS Receiver Identification Using Clock-Derived Metrics," *Sensors*, vol. 17, no. 9, 2017.