Received December 24, 2019, accepted January 23, 2020, date of publication January 29, 2020, date of current version February 6, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2970203

BD-II NMA&SSI: An Scheme of Anti-Spoofing and Open BeiDou II D2 Navigation Message Authentication

ZHIJUN WU, YUN ZHANG, AND RUSEN LIU
School of the Electronic Information and Automation, Civil Aviation University of China, Tianjin 300300, China

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

This work was supported in part by the Joint Foundation of National Natural Science Committee of China, in part by the Civil Aviation Administration of China under Grant U1933108, in part by the Key Program of Natural Science Foundation of Tianjin under Grant 17JCZDJC30900, in part by the Scientific Research Project of Tianjin Municipal Education Commission under Grant 2019KJ117, and in part by the Fundamental Research Funds for the Central Universities of China under Grant 3122018D007 and Grant 3122018C003.

ABSTRACT Due to openness and lack of authentication, like other members of the Global Navigation Satellite System (GNSS) Club, BeiDou-II civilian navigation signals are vulnerable to all kinds of spoofing attacks. As a result, both the positioning and timing functions of BeiDou-II civil satellite navigation are likely to be controlled by the spoofer. In this paper, an anti-spoofing scheme of BeiDou-II Navigation Message Authentication & Spread Spectrum Information (BD-II NMA&SSI) is proposed by using SM cryptographic algorithms and spread spectrum information to resist spoofing attacks. The SM cryptographic algorithms are used for generating authentication information to detect spoofing attacks. The spread spectrum information is to protect the authentication information in the D2 navigation messages from modification. Experimental results show that the scheme guarantees the authenticity of BD-II satellite navigation messages, meets the requirement of anti-spoofing and takes a rather less effect on the satellite navigation system.

INDEX TERMS Anti-spoofing, BeiDou-II navigation, SM cryptographic algorithms, navigation message authentication, spread spectrum modulation.

I. INTRODUCTION

Recently, satellite navigation has been widely used in various fields of the world. From the perspective of civil navigation signal application, satellite navigation has been deployed in industries such as air traffic management (ATM) and marine transportation as an infrastructure [1]. With the development of technology, the security of satellite navigation system cannot be guaranteed [2]–[4]. There are many examples to illustrate the insecurity of GNSS signals. In February 2018, the US Maritime Administration discovered some strange phenomena. They found multiple GPS interference events on ships and aircraft operating in the Eastern Mediterranean Sea. These interferences can cause GPS signals to be lost. As a result, this situation will further affect devices based on GPS timing and communication [5]. Furthermore, Todd Humphreys' team successfully demonstrated the civil GPS receiver can be spoofed by the spoofer [6]. In their demonstration, the civil aviation unmanned aerial was controlled by the spoofer in flight phases, yet the pilot didn't know it [7]. Hence, the spoofing attack can seriously affect the positioning of civilian navigation devices.

The BeiDou-II civil satellite navigation system lacks navigation message protection. As a result, the system will face serious security threats and be vulnerable to spoofing attacks. In order to ensure the accuracy of the timing and positioning, the signal-based anti-spoofing methods and the information-based anti-spoofing method are proposed to resist the spoofing attack. Many scholars have applied signal-based anti-spoofing methods to satellite navigation systems. For example, Kyle D. Wesson, Brian L. Evants and Todd E. Humphrey [8] had developed a method based on received power estimation. Their method can distinguish the normal satellite signal from the multipath-affected signal, spoofing signal and jamming signal. According to the analysis of experimental results, the false alarm rate was set below 0.5%. When the interference signal was set as the spoofing signal, only 29.13% were detected as the spoofing

The associate editor coordinating the review of this manuscript and approving it for publication was Chi-Yuan Chen.

and others were considered as jamming. Since the above experimental results are theoretical values, the scheme still needs to be tested in a real spoofing environment in future work. Ali Jafarnia Jahromi and Ali Broumandan [9] proposed a method of several signal quality monitoring (SQM) metrics to detect spoofing signals. They detected spoofing signals by observing an abnormally shaped or asymmetric correlation peaks. They also calculated appropriate interference detection thresholds based on these metrics. However, the determination of these thresholds will change as the spoofing environment changes. Weikong Qi, Yu Zhang, Xiaohui Liu [10] developed an anti-spoofing method based on doppler frequency shift. According to the simulation result, when the receiver was dynamic and suffering the spoofing attack, the doppler frequency shift was abnormal. Based on this feature, the receiver can detect spoofing attacks in time. Nonetheless, the threshold of detecting spoofing attack is not easy to determine. The reason is that the threshold is not only related to the spoofing environment, but also related to the speed of the receiver in a variable speed motion.

As the environment changes, the signal-based anti-spoofing method is not accurate. However, contrary to information-based anti-spoofing methods, signal-based anti-spoofing methods are far from absolute [11]. As a branch of information-based anti-spoofing methods, cryptography-based anti-spoofing method have recently become more mature. Cryptography-based anti-spoofing methods have high security. Therefore, we propose an anti-spoofing based on SM series cryptographic algorithms. In this paper, we use the SM series cryptographic (SM2 [12], [13], SM3 [14] and SM4 [15]) algorithms to encrypt the navigation message information. In addition, in order to avoid the tampering of the authentication information, we propose to insert the SSI between subframe 1 and subframe 2 in D2 navigation messages to ensure the integrity of the authentication information.

The structure of this paper is arranged as follows. Section II introduces related works. Section III analyzes spoofing process and introduces the BeiDou-II D2 navigation messages. Section IV proposes the overall anti-spoofing scheme. Section V shows the experiments and results analysis. Section VI summaries this paper and discusses the future work.

II. RELATED WORKS

In order to achieve better resistance to spoofing attacks, many scholars have proposed cryptography-based anti-spoofing methods to ensure the integrity of navigation messages. These methods can be classified into Navigation Message Authentication (NMA), Spreading Code Authentication (SCA) and combined authentication method.

A. NAVIGATION MESSAGE AUTHENTICATION (NMA)

For civilian GNSS navigation messages, some scholars have proposed the NMA method. In this method, the sender generates authentication information by using encryption algorithms (eg. a digital signature or a navigation message authentication code). The receiver decrypts the authentication information through the key of the encryption algorithm. By analyzing the decrypted results, the receiver verifies the integrity of the navigation message. According to the above process, the receiver can achieve the purpose of resisting spoofing attacks.

Koichi CHINO [16] built an experimental platform of spoofing attacks to detect anti-spoofing performance. The sender encrypts the QZSS L1C/A partial navigation message by using the RSA asymmetric encryption algorithm. The ciphertext is called signature which is inserted into the QZSS L1SAIF navigation message for transmission. The receiver verifies the signature to decide whether the receiving message is spoofing message or not. However, this scheme does not take other factors such as signal transmission protocols, key management into consideration. Therefore, the overall security of the system cannot be effectively guaranteed. Kyle Wesson and Mark Rothlisberger [11] used elliptic curve digital signature algorithms to generate signatures for navigation messages. The sender inserts the signature into the GPS civil navigation message (CNAV) and transmits CNAV. The receiver authenticates the integrity of CNAV by decrypting the signature. In addition, this scheme can detect replay spoofing attacks with probability of detection greater than 0.97 for a false alarm probability of 0.001. However, this scheme lacks detection in a real environment to judge actual performance. Wu Zhijun [17] proposed a scheme to protect BeiDou-II navigation message based on ECDSA algorithm. He not only analyzed the authentication rate of their scheme in the gauss noise environments, but also designed a complete key exchange process based BeiDou-II navigation system. The experimental simulation shows that the BeiDou navigation system based on ECDSA encryption has a better anti-spoofing ability.

The above schemes are based on digital signatures to realize NMA. However, the scheme using signature will cause the problem of complicated calculation, large communication overhead and weak robustness of the system. Therefore, some scholars have proposed using Timed Efficient Steam Loss-Tolerant Authentication (TESLA) protocol to solve the above problem and resist spoofing attack. Ignacio Fernández Hernández [18] proposed a concept of one-way key chains for all senders and cross authentication based on the TESLA protocol. In this scheme, the sender encrypts the navigation message using a one-way key chain. The receiver only needs to receive this key from any satellite to perform identity authentication. This scheme not only enhances the robustness of the system, but also allows satellites to cross-identify neighboring satellites, which can cope with various multi-star spoofing problems. However, this scheme has poor detection performance for replay spoofing attacks in some environments. Gianluca Caparra [19] proposed the one-way key chains generation algorithm model for the TESLA protocol. 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.

The TESLA protocol requires loose time synchronization between the sender and the receiver. In addition, considering that an anti-spoofing scheme adopting only one encryption authentication scheme cannot resist multiple spoofing attacks, some scholars have proposed a scheme combining TESLA with other encryption algorithms. Muzi Yuan [20] used the ECDSA algorithm combined with the TESLA protocol to protect the BeiDou civil navigation signal. In their scheme, the ECDSA algorithm is used to ensure the reliability of the BeiDou civil signal in the transmission process. The TESLA protocol is used to improve the authentication efficiency of the receiver. Although the scheme has high authentication efficiency, the resistance performance against multi-star spoofing attacks remains to be analyzed. Andrew J. Kerns [21] proposed a hybrid scheme of ECDSA and TESLA. He gave a civil navigation message authentication scheme from the aspects of authentication efficiency and implementation feasibility. The experiment result shows that this scheme greatly reduced the overhead of the user terminal while protecting the navigation message.

B. SPREADING CODE AUTHENTICATION (SCA)

SCA is one of the cryptography-based anti-spoofing methods. The method protects unencrypted public spreading codes by inserting some unpredictable chips into the spreading code.

Oscar Pozzobon [22] proposed a concept of signal authentication sequence (SAS). 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. Oscar Pozzobon [23] further studied the SCA scheme to propose a novel scheme for authentication of open GNSS signals using supersonic codes (a solution that provides hybrid authentication). 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 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. G. Kuhn [24] proposed a concept of hidden markers to implement the secret transmission of spreading codes. The hidden marker is a rectangular pulse of 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.

C. COMBINED AUTHENTICATION METHOD

There are some schemes that combine navigation message authentication with spreading code authentication. For example, Gkougkas [25] proposed a two-component signal based on the combination of NMA and SCA. One signal component is a normal navigation signal, which uses an encryption algorithm to protect the navigation message. The other signal component is a low power authentication signal that is used to verify the reliability of the spreading code. The sender can modulate and transmit information through the two-component signal to protect the navigation message. However, the receiver receiving the key may be delayed in release, which will affect the real-time location of the system. Davide Margaria and Beatrice Motella [26] proposed a scheme based on SCA and NMA. From the perspective of navigation message authentication, the scheme used a TESLA keychain to encrypt navigation messages. From the perspective of spreading code authentication, the scheme used code-shift-keying (CSK) modulation to insert message authentication code into the spreading code. Both authentication schemes are implemented by a tentative time schedule. The experimental results show that the scheme has better resistance to estimated spoofing attacks and can meet different security requirements of users. However, this scheme requires the receiver to have loose time synchronization. Davide Margaria and Beatrice Motella [27] analyzed the feasibility of existing civil GNSS signal authentication schemes. By combining multiple spoofing methods, they proposed a more comprehensive encryption and authentication scheme for the next generation of civilian GNSS signals. However, the feasibility of scheme strongly depends on the complexity and compatibility of the receiving system.

Combined with the research status in recent years, a navigation message authentication scheme can be designed to utilize different components of the signal. According to the above description, the NMA methods denote the protection of the navigation message (the full data frame or a portion of it), and the SCA methods implement protection for spreading codes. Therefore, both NMA and SCA methods can protect the transmission of civil navigation signals to a certain extent. Combining the advantages of NMA scheme and SCA scheme, we propose an anti-spoofing scheme called BD-II-NMA&SSI based on navigation message authentication and spread spectrum information protection.

III. THE SPOOFING PROCESS ANALYSIS AND BD-II D2 NAVIGATION MESSAGE INTRODUCTION

Since the signal parameters and message structure of civil satellite navigation systems have been opened to the public, malicious spoofers are likely to forge civilian satellite navigation signals. A spoofer can launch a spoofing attack to affect

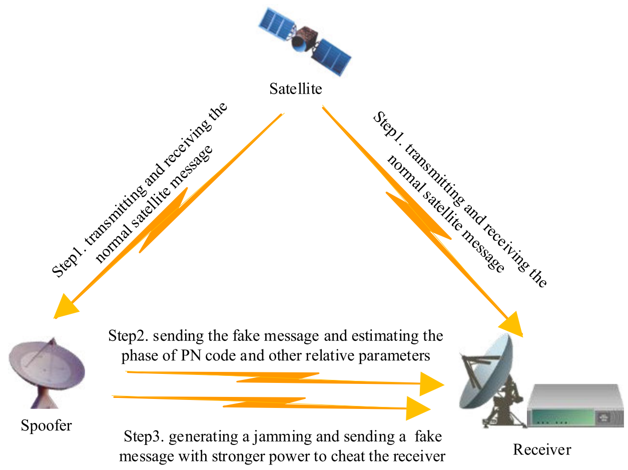

Satellite
Step1. transmitting and receiving the normal satellite message
Step1. transmitting and receiving the normal satellite message
Step2. sending the fake message and estimating the phase of PN code and other relative parameters
Spoofer
Step3. generating a jamming and sending a fake message with stronger power to cheat the receiver
Receiver

FIGURE 1. Spoofing process.

and even control the receiver's positioning result. Figure 1 is the process of spoofing structure diagram assumed in this paper [17].

Step 1: Under normal circumstances, both the deceiver and the receiver will receive satellite signals transmitted from the satellite. The spoofer generates a spoofing signal after analyzing the satellite signal.

Step 2: In order to spoof the receiver more effectively, the spoofer not only gradually adjusts the PN (pseudo-noise) code phase of the spoofing signal and the spoofing signal carrier phase, but also gradually increases the power of the spoofing signal.

Step 3: The spoofer generates a blocking signal to force the receiver to re-acquisition of the satellite signal. Since the power of the spoofing signal received by the receiver is greater than the power of the true signal, the receiver considers the spoofing signal to be a true signal and receives it, while the true signal is considered to be multipath interference and is not captured by the receiver. The spoofer gradually controls the phase-locked loop of the receiver and affects the positioning result of the receiver (user) [28].

A. SPOOF ATTACK ANALYSIS

According to the spoofing information sent by the spoofer, the spoofing attack can be divided into the meaconing attack and the generated spoofing attack [29], [30]. The characteristics of these spoofing attacks are as follows.

Meaconing attack refers to the spoofing attack that the spoofer will perform high-power broadcasting of non-real-time satellite signals, thereby affecting the positioning result of the receiver. Although the navigation message of the military satellite signal is encrypted and the encryption key is not disclosed, the spoofing mode of the broadcast non-real-time satellite signal has a certain adverse effect on the military satellite navigation signal receiver. The main role of this kind of attack is to interfere with the normal positioning of the receiver. The spoofer needs to design and implement the meaconing attack and add some spoofing strategies in order to increase the possibility of successful spoofing attacks.

In generating spoofing attack, the spoofing message is generated by the spoofer itself. Since military navigation messages are encrypted, generating spoofing attacks have a greater impact on civilian receivers that receive unencrypted satellite navigation messages. According to the civilian signal parameters and the civil satellite navigation message structures in the interface control document (ICD) [31], the malicious spoofer can easily generate and falsify civilian signals. The spoofer will suppress the real signal by transmitting a high-power signal and induce the target receiver to follow the tracking loop of the deceptive signal. Compared with non-human interference, the most obvious feature of spoofing attacks is hiding. Non-human interference that refers to the interference caused by the channel or the natural environment in addition to people intentionally interfering with the navigation signals will reduce the accuracy of navigation positioning and timing functions.However, the navigation accuracy is not reduced under the spoofing attack, which makes it difficult for the receiver to detect and resist spoofing attacks [32].

Spoofing attacks (see Figure 1) can also be classified into ''single star spoofing'' and ''multi-star spoofing''. Table 1 shows the meaning and classification of ''single star spoofing'' and ''multi-star spoofing''.

TABLE 1. The meaning and classification of "single star spoofing" and "multi-star spoofing".

	Classification		Meaning
Spoofing attacks	Single star spoofing	Same single-star spoofing	The receiver is receiving a navigation message from a satellite while the spoofer launches a spoofing attack based on navigation messages from the same satellite.
		Different single-star spoofing	The receiver is receiving a navigation message from a satellite while the spoofer launches a spoofing attack based on navigation messages from the other satellites.
	Multi-star spoofing		Spoofer forged the navigation message of multiple satellites.

The method designed in this paper mainly resists the ''same single-star spoofing'' based on the spoofing situation in Fig.1[17].

If the current receiver receives the mth satellite, under ''same single-star spoofing'', meaconing means that the satellite navigation message transponded by the spoofer is form the past mth satellite. Generated spoofing attack refers that a spoofer sends the mth satellite navigation messages containing tampering information.

When the spoofer launches ''same single-star spoofing'' based on Fig.1, the receiver suffers from interference from the blocking signal during the process of receiving the navigation message. Therefore, the receiver can detect whether the receiver is subjected to a spoofing attack by verifying the continuity of the navigation messages. If the spoofer initiates meaconing, the receiver can authenticate the continuity of the currently received navigation message with the previously received navigation message while the message does not change. When the receiver found that the authentication cannot be successful, the receiver can determine that the current receiver is in the meancoining attack. If the spoofer initiates a generating spoofing attack, the receiver can authenticate the authenticity and integrity of the locating information. When the receiver found that the authentication fails, the receiver can determine that the current receiver is under the generating spoofing attack. Therefore, if the receiver can authenticate the time information and the basic navigation information in time, the meaconing and the generated spoofing attack will be resisted under the ‘‘same single star spoofing’’.

B. BEIDOU-II D2 NAVIGATION MESSAGE

The BD-II navigation messages consist of D1 and D2 navigation messages. In general, the number of D2 navigation messages received by the receiver is greater than the number of D1 navigation messages during a fixed period, even if only 5 GEO satellites broadcast the D2 information while 32 MEO satellites broadcast the D1 information. The reason is that the rate of D2 is 500 bps and the rate of D1 is 50 bps. Hence, a receiver is more likely to select the information of the D2 navigation message for position location. In view of this situation, the anti-spoofing method designed in this paper is mainly to protect the D2 navigation message.

The BeiDou D2 navigation message is transmitted in the form of main-frame, which consists of 5 subframes (subframe 1 to 5). Each subframe has its own page number, which is used to distinguish the same subframe of different main frames.

According to the basic navigation information and time information in the received messages from the four satellites, the receiver can calculate its own position information. Basic navigation information is a collection of parameters that contain weekly count, user range accuracy index, autonomous satellite health flag, clock correlation parameter and etc... With these parameters, the receiver can calculate the position information of the satellite. In the D2 navigation message, the basic navigation information is transmitted through ten consecutive subframes 1 which is called a group of subframe 1. It can be identified by page number 1 to page 10 to distinguish different subframes 1 as shown in the Fig. 2.

The time information includes weekly count information and second of week (SOW) information. In the D2 navigation message, the weekly count information is distributed in page 1 of subframe 1 and updated every hour. The SOW is distributed in each subframe and updated every 0.06 seconds.

According to the previous analysis of the spoofing process in Fig. 1 and the structure of D2 navigation messages, the receiver needs to accomplish two missions to resist the ‘‘same single star spoofing’’ attack. The first one is satellite position information authentication, which can be completed by verifying the digital signature of the basic navigation information (BNI). The second one is time information authentication, which authenticates the continuity and authenticity of time information. Since the weekly count information belongs to the basic navigation information and is protected by the digital signature, the time information authentication refers to the authentication of the SOW. Based on the structure of the BeiDou-II D2 navigation message, the time information authentication can be classified into page time authentication and group time authentication. Page time authentication refers to detecting whether the SOW information between different pages in a group of subframes 1 is true and continuous. Group time authentication refers to detecting whether the SOW information between each group of subframes 1 is true and continuous. The receiver can authenticate time information by authenticating all group time information or authenticating all page time information. However, the authentication costs of the two methods are different. The receiver needs to select the appropriate method for time information authentication according to its own security requirements and hardware performance.

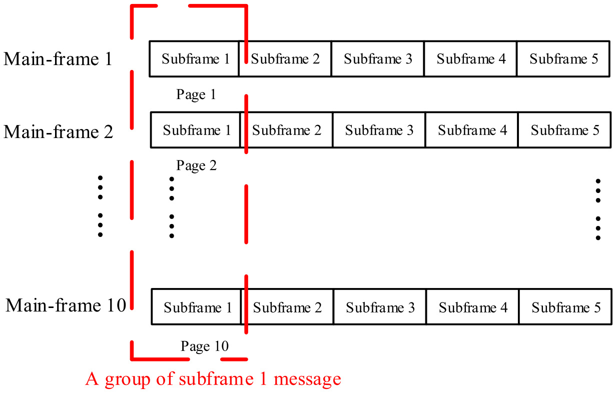


FIGURE 2. The basic navigation information in D2 navigation messages.

IV. BD-II NMA&SSI ANTI-SPOOFING SCHEME

Based on the above analysis of the satellite navigation system spoofing process and the analysis of the BeiDou-II D2 navigation message, the anti-spoofing method designed in this paper is shown in Fig. 3.

The overall authentication framework shown in Fig. 3 mainly includes satellite location authentication (signature verification), group time authentication and page time authentication.

The ground control station uploads GPSSS (Generator Polynomial of Spectrum Spreading Sequence), BNI (Basic Navigation Information, which is important positioning information in Beidou-II D2 navigation message) and signature information to the satellite. The signature for BNI is generated by private key encryption. The private key, public key and key are generated in the ground control center. The symmetric key is used to generate ciphertext

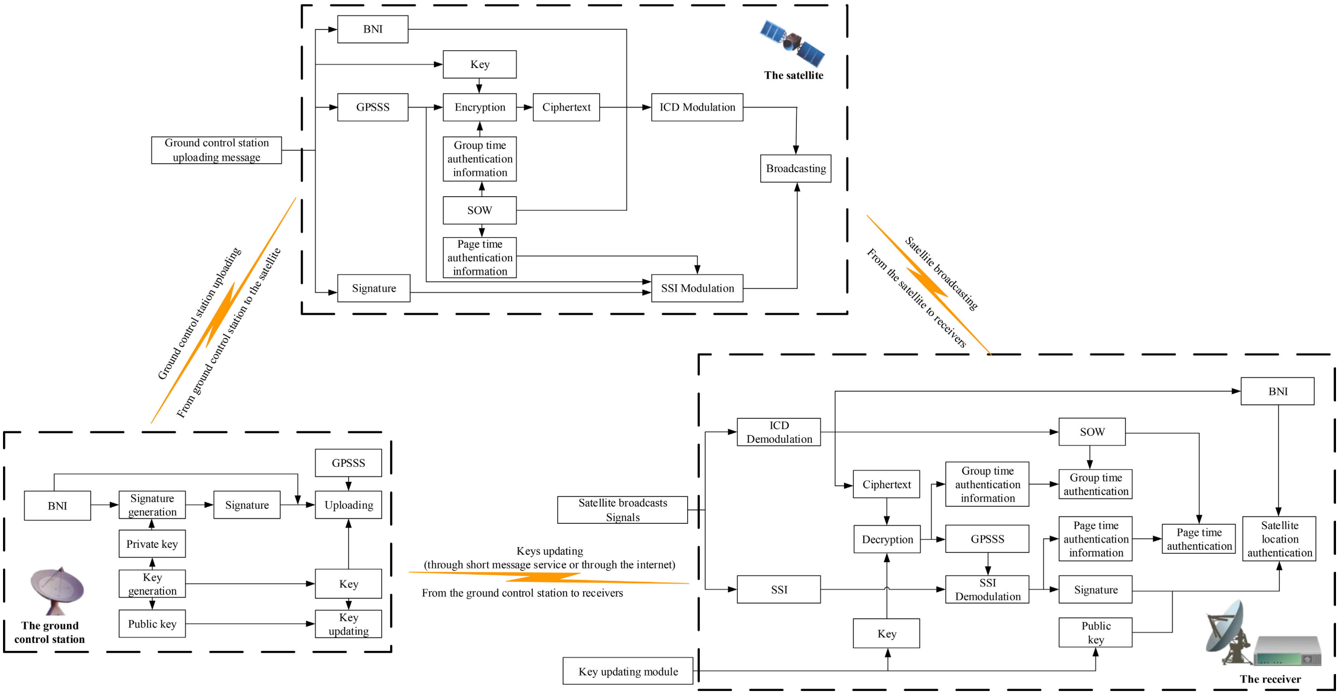

BNI
Key
GPSSS
Encryption
Ciphertext
ICD Modulation
The satellite
Ground control station uploading message
Group time authentication information
Broadcasting
SOW
Page time authentication information
Signature
SSI Modulation
Ground control station uploading
From ground control station to the satellite
Satellite broadcasting
From the satellite to receivers
GPSSS
BNI
Signature generation
Signature
Uploading
Private key
Key generation
Key
Public key
Key updating
The ground control station
Satellite broadcasts Signals
Keys updating
(through short message service or through the internet)
From the ground control station to receivers
Key updating module
ICD Demodulation
BNI
SOW
Ciphertext
Group time authentication information
Group time authentication
Decryption
GPSSS
Page time authentication information
Page time authentication
Satellite location authentication
SSI
SSI Demodulation
Signature
Key
Public key
The receiver

FIGURE 3. The overall structure of the main frame with authentication function.

information on the satellite side and decrypt the ciphertext on the receiver. Symmetric key and public key will transmit to the receiver through the short message service or through the internet.

The satellite generates SOW through its own atomic clock. Based on SOW, group authentication information and page authentication information are generated. The group time authentication information and GPSSS is protected by ciphertext which is replaced the reserved bits in the navigation message to transmit. This ciphertext is encrypted by the symmetric key. The signature and the page time authentication information are protected by spread spectrum information, which is inserted between subframe 1 and subframe 2 in D2 navigation message. The location of the spread spectrum information and the ciphertext information is as shown in Fig. 4.

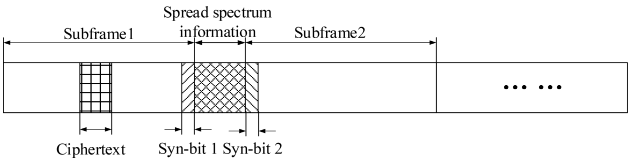


FIGURE 4. The location of the spread spectrum information and the ciphertext information.

The satellite will broadcast the navigation message as shown in Fig 4. The normal navigation message (subframe 1 to 5) is modulated according to the spreading sequence specified in the ICD[31] (Referred to as ICD modulation). The SSI modulated based on GPSSS, which is referred to as SSI modulation.

When the receiver receives the satellite signal, it needs to synchronize the signal (ie, capture and tracking). When the synchronization error of the received signal is within a certain controllable range, the receiver starts demodulating the satellite signals to obtain various information transmitted by the satellites. In BD-ICD [31], each subframe has synchronization bit information which is fixed to 11100010010. As shown in Fig. 4, the added synchronization bit information at the end of subframe 1 is Syn-bit 1, and the inherent synchronization bit information at the front of subframe 2 is Syn-bit2. The receiver obtains spread spectrum information by extracting information between Syn-bit 1 and Syn-bit 2. After the receiver extracts all the spread spectrum information in a group of subframes 1, the receiver uses the decrypted GPSSS to perform spread demodulation. When the receiver continuously receives and demodulates a group of subframes 1 (ie, 10 consecutive pages of subframe 1), the receiver will initiate group time verification, page time verification, and satellite position verification.

A. SM CRYPTOGRAPHY ALGORITHMS

The SM cryptography algorithm includes SM1, SM2, SM3, SM4, SM7 and SM9 issued by China cryptography administration. SM2 and SM9 algorithms were unanimously adopted as international standards at the 55th ISO/IEC Information Security Subcommittee (SC27) meeting. These two digital signature mechanisms are the main part of the ISO / IEC 14888-3 / AMD1 standard development project. SM2, SM3, SM4 are used in our scheme. The corresponding national standard codes for SM2, SM3, and SM4 are GB/T 32918.1/2/3/4-2016, GB/T32905-2016, and GB/T32907-2016. Their characteristics are shown in Table 2.

TABLE 2. The characteristics of SM cryptography algorithms.

Algorithm	Feature	Length(bit)		
		Plaintext	Key	Cyphertext
SM2	Asymmetric encryption	256	Public: 256 Private: 128	512
SM3	Hash function	Variable	Null	256
SM4	Symmetric encryption	128	128	128

SM2 algorithm is firstly issued by the China State Cryptography Administration in 2012. It uses the private key to encrypt the plaintext. The output ciphertext is named signature. The ciphertext is decrypted by the public key. This process is called signature verification. The encryption strength of SM2 is stronger than RSA-2048 and its speed of encryption is faster than RSA-2048. The elliptic curve of the SM2 is derived from the ECC-256. The detailed process of SM2 signature generation and signature verification is shown in [12], [13].

SM3 algorithm is used for calculating the hash value of the bit string. The length of input bit string is uncertain. The length of output bit string is 256 bits. The main processes of SM3 are padding and contractive iteration, whose details are seen in the literature [14].

SM4 algorithm is a block cipher algorithm with 128-bit data block and 128-bit key. On the encryption side, key extension algorithm adopts 32-round nonlinear iteration structure. The decryption algorithm is consistent with the structure of the encryption algorithm, and is only reversed in the order of the round keys [15]. The detail process of encryption and decryption reference literature [15].

B. INFORMATION AUTHENTICATION

There are three kinds of information authentication processes involved in this method, namely group time authentication, page time authentication, and signature authentication. Their authentication process is as follows.

1) GROUP TIME AUTHENTICATION AND GPSSS

The group time authentication information and GPSSS transmitted by SM4 encryption. The specific structure of the ciphertext information is shown in Fig. 5.

The GPSSS is used for demodulating the spread spectrum information that is inserted between subframe 1 and 2. Considering that satellite systems typically use an 11-stage shift register to generate a spreading code sequence [31], GPSSS is generated using a shift register with a stage less than or equal to 11. In addition, a codebook of GPSSS is preset. The ID, an 8-bit data in Fig. 5, represents GPSSS.

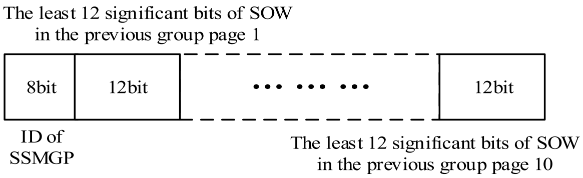

The least 12 significant bits of SOW
in the previous group page 1
8bit
12bit
••• ••• •••
12bit
ID of
SSMGP
The least 12 significant bits of SOW
in the previous group page 10

FIGURE 5. The structure of ciphertext.

The group time authentication information is used for proving that SOW is continuous in present and previous group of subframe 1. The group of subframe 1 is consisting of 10 pages, each page has a SOW. Its 12 least significant bits is used for authenticating. Hence, there are total 120 bits in 10 pages used as group time authentication information in Fig. 5.

According to the number of reserved bits in subframe 1 of each page, the 128-bit ciphertext data is permutated. The result of permutation is illustrated in the Table 3.

TABLE 3. Cipher permutated in the subframe 1.

Ciphertext position	The reserved bits position
1-29	45-73 bits reserved in page 3
30-37	103-110 bits reserved in page 4
38-45	103-110 bits reserved in page 5
46-53	103-110 bits reserved in page 6
54-61	103-110 bits reserved in page 7
62-67	105-110 bits reserved in page 8
68-75	103-110 bits reserved in page 9
76-128	58-110 bits reserved in page 10

When the receiver receives all the ciphertext in the Table 3, the ciphertext will be decrypted by the SM4 algorithm. The receiver extracts GPSSS and group time authentication information from the decrypted ciphertext. The GPSSS is used for spreading spectrum demodulation. The group time authentication information is used for group time authentication. The process of group time authentication is shown in Fig. 6.

As shown in Fig. 6, in order to determine whether the received group of subframe 1 is true and continuous, the receiver compares the obtained SOW of the group of subframe 1 with the decrypted group time authentication information. If the two are consistent, the group time authentication is successful. If the two are inconsistent, the group time authentication fails, which means that the information may be spoofed and page time authentication is required.

2) PAGE TIME AUTHENTICATION AND SATELLITE LOCATION AUTHENTICATION

The SSI is inserted between the D2 navigation message subframe 1 and the subframe 2. The spread spectrum information includes page time authentication information and the signature. The purpose of adding spread spectrum information is to ensure the security of the authentication information which includes page time authentication information and the signature. Due to the lack of GPSSS, the spoofer cannot

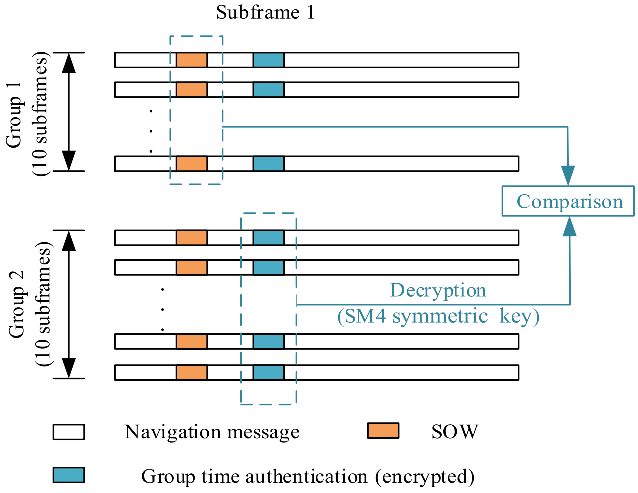


FIGURE 6. Group time authentication.

extract the spread spectrum information from the noise and modify the authentication information in advance. When the spoofing attack is performed, the continuity of the navigation message will be destroyed. Hence, the spoofing attack can be detected in time by the page time authentication. Furthermore, if the spoofer attempts to modify the basic navigation information, the receiver can determine whether the received satellite navigation information is untrustworthy or not by signature verification in the spread spectrum information.

Due to the long length of a signature, the signature is split into 10 parts and inserted into the spread spectrum information of the different pages of the subframe 1 respectively. Each part of the signature is called the signature fragment. As the page number is different, the length of the page time authentication information and the length of the signature fragment are also different. The length of the page time authentication information and the length of the signature fragment information corresponding to each page are as shown in Table 4.

TABLE 4. The length of the page time authentication information and the length of the signature.

Page number	Signature fragment	Page time authentication information
1	53	2
2	51	4
3	51	4
4	51	4
5	51	4
6	51	4
7	51	4
8	51	4
9	51	4
10	51	4
Sum	512	38

Due to the presence of noise, the spread spectrum information may be disturbed, causing some of the information bits to be in error during transmission. In order to prevent from this happening, several check bits are inserted into spread spectrum information. For the purpose of avoiding to increase the hardware complexity of the satellite receiver due to the insertion of check bits in spread spectrum information, the check algorithm that uses the BCH (15,11,1) [31], which is the same as that used in the BeiDou-II. During the transmission of spread spectrum information, an 11-bit data is input the BCH (15, 11, 1) algorithm, through calculation, 4-bit is output as check bits. The overall structure of spread spectrum information is shown in Fig. 7.

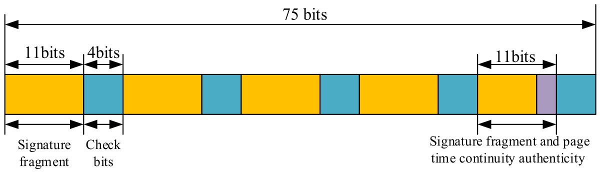


FIGURE 7. The overall structure of the spread spectrum information.

After receiving all the spread spectrum information corresponding to a group of subframe 1, the receiver uses the GPSSS to perform spread spectrum demodulation on the spread spectrum information. The demodulated information is shown in Fig. 7. After the BCH check, the receiver extracts the signature fragment and page authentication information according to Table 4. The receiver concatenates the signature fragments of each page to form 512-bit signature for signature authentication. In addition, the page time authentication information of each page will perform page time authentication according to the SOW information of the previous page.

a: PAGE TIME AUTHENTICATION

In the ten consecutive subframe 1, several the most significant bits (MSBs) in the SOW is same. Thus, the page time authentication information includes the several least significant bits (LSBs) of SOW in the previous subframe 1. The process of page time authentication is shown in the Fig.8.

As is shown in the Fig. 8, when the receiver demodulates the spread spectrum information, the page time authentication information will be compared with the corresponding SOW in the previous subframe 1. If the authentication is successful, it indicates that each page of subframe 1 is consecutive. If the authentication fails, the receiver may be subject to a blocking attack. The receiver receives the navigation message information discontinuously. The currently received navigation message may be a spoofing message. The receiver needs to perform signature verification on the currently received navigation message.

b: SATELLITE LOCATION AUTHENTICATION

Basic navigation information in a group of subframe 1 will be authenticated by the signature in the spread spectrum information. The process of signature verification is shown in Fig. 9.

As shown in Fig. 9, after the signature information is obtained, the receiver generates a digest value for the received

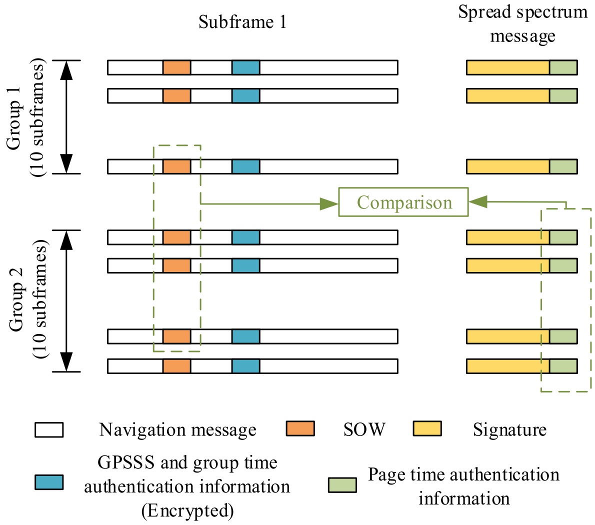


FIGURE 8. Page time authentication.

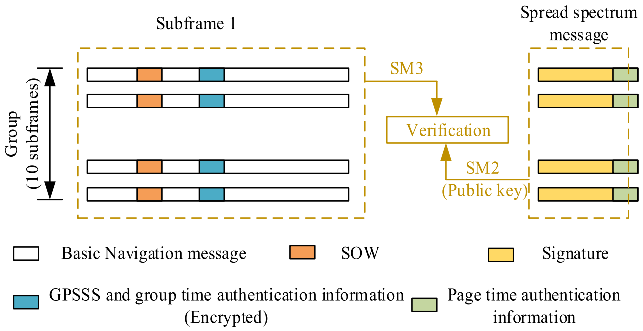


FIGURE 9. Satellite location authentication.

basic navigation information by the SM3 algorithm. The receiver uses the digest value and the public key information as input to verify the signature. If the verification is successful, it indicates that the basic navigation information received by the receiver is true, otherwise, the receiver is under spoofed. The receiver needs to delete the spoofing message and uses the navigation message from other satellites to realize the positioning service.

C. KEYS UPDATING

In the navigation message, the signature is verified by the public key and the ciphertext is decrypted by the symmetric key. Users can update these keys in two ways. One through the short message service (SMS) of BeiDou navigation system. The other through the digital certificate stored on the internet.

All receivers have a same master key of 256 bits, which is protected by the high-strength cryptographic algorithm. This algorithm is only known to the receiver manufacturer and not disclosed to the public.

The process of symmetric key updating is shown in Fig. 10.

A set of plaintexts is repeatedly encrypted, that is multiple iterations, using the SM4 cryptographic algorithm with a fixed key called input key or master key. According to SM4 standard [15], the contents of input key could be same with plaintext. Therefore, this scheme sets the input key to be the same as the plaintext content in the SM4 encryption process, and the number of repeated encryptions is equal to the number of iterations. The number of iterations can be updated by key update information.

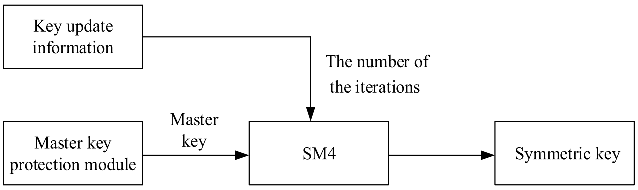


FIGURE 10. Symmetric key updating.

The updated symmetric key is the result of multiple iterations of SM4 encryption. The iterations of SM4 encryption is described in the update message. As long as the user updates the number of iterations, the user can update the symmetric key through the SM4 algorithm, which avoids the leakage of information caused by publicly transmitting the symmetric key.

1) THE KEY UPDATE THROUGH THE SMS

Since SMS lacks protection for transmitted information, the spoofer can forge SMS messages to spoof the receiver. When the public key and the number of iteration are updated by SMS, the transmission information needs to be encrypted and authenticated. In order to achieve this function of encryption and authentication, the receiver needs to obtain the preset key from the Internet in advance.

Each receiver has a unique preset data packet which can be downloaded from the website of receiver manufacturer when the receiver is firstly used. The preset data packet contains the preset key and its authentication information. The data packet is encrypted by the master key for transmission. Once the receiver updates the keys through SMS, the preset key will be obtained from the data packet, as shown in Fig. 11.

As shown in the Fig. 11, once the receiver has downloaded its own data packet, the receiver will automatically obtain the ciphertext. Only the master key that protected by the master key protection module can be used for decrypting the ciphertext to obtain the plaintext. The plaintext consists of the preset key and its digest value, named digest 1. Meanwhile, another digest value, denoted as digest 2, is calculated by the SM3 algorithm on the obtained preset key in the receiver. If the digest 1 is the same as the digest 2, the receiver will save the preset data packet previously downloaded from the website. Otherwise, the preset information packet should be deleted and the data packet should be re-downloaded. For purpose of security consideration, the preset key is deleted after the key exchange process was completed.

In the process of SMS key update, symmetric encryption algorithm and asymmetric encryption algorithm are used for data protection. These two algorithms are determined by the receiver manufacturer in consultation with the ground control

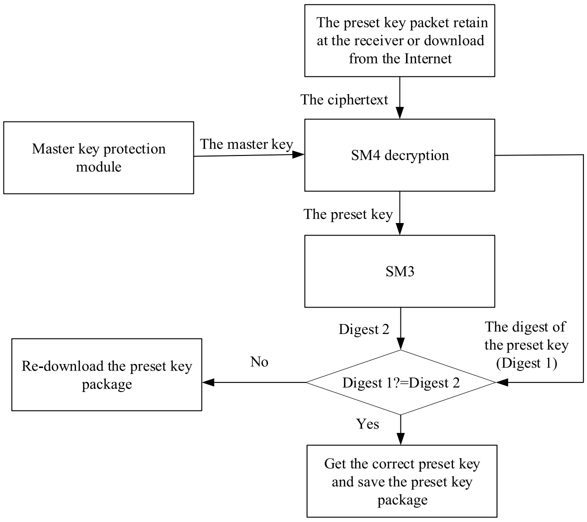

The preset key packet retain at the receiver or download from the Internet
The ciphertext
Master key protection module
The master key
SM4 decryption
The preset key
SM3
Digest 2
The digest of the preset key (Digest 1)
Re-download the preset key package
No
Digest 1?=Digest 2
Yes
Get the correct preset key and save the preset key package

FIGURE 11. The preset key obtained from the data packet.

center. In order to ensure the security and reliability of the two cryptographic algorithms, specific algorithm details are not disclosed to the user. Both algorithms are solidified in the receiver chip. When SMS is used for key update, the programs of the two algorithms are activated. The process of keys update through SMS is shown in the Fig. 12.

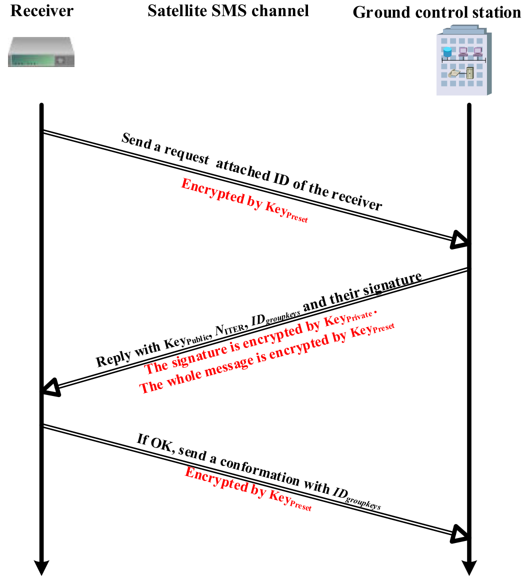

Receiver
Satellite SMS channel
Ground control station
Send a request attached ID of the receiver
Encrypted by Key$_{Preset}$
Reply with Key$_{Public}$, N_{ITER}, $ID_{groupkeys}$ and their signature
The signature is encrypted by Key$_{Private}$ •
The whole message is encrypted by Key$_{Preset}$
If OK, send a conformation with $ID_{groupkeys}$
Encrypted by Key$_{Preset}$

FIGURE 12. Key updating through the SMS.

There are a few kinds of keys are involved in the process of key exchange through the SMS, for a clearer expression, the abbreviations of keys and others are shown in Table 5.

The receiver will send a request message attached its own ID to the ground control station when Key$_{Public}$ and N$_{ITER}$ need to be updated. The request is a message that encrypted by a symmetric encryption algorithm with Key$_{Preset}$. Once the encrypted request message is received by the ground control station, it gets the corresponding Key$_{Preset}$ from the preset key database on the basis of the receiver's ID. After the encrypted request message is decrypted by Key$_{Preset}$, a signature of the Key$_{Public}$, N$_{ITER}$ and the ID$_{groupkeys}$ is generated by an asymmetric encryption algorithm with Key$_{Private}$. Then, the receiver through Key$_{Preset}$ encryption receive Key$_{Public}$, N$_{ITER}$, the ID$_{groupkeys}$ and their signature. When receiver obtains the content of cyphertext, it will recover Key$_{Public}$ and verify the signature through the received Key$_{Public}$. The receiver will transmit a confirmation information to the ground control station and update Key$_{Group}$ (contains Key$_{Public}$ and N$_{ITER}$) once the verification is successful. Otherwise, the receiver will delete this Key$_{Group}$, ID$_{groupkeys}$ and signature, and transmit a request to ground control station again.

TABLE 5. The abbreviations of keys and related information.

Abbreviation	Meaning
Key$_{Public}$	The public key of current navigation message
Key$_{Private}$	The private key of current navigation message
Key$_{Preset}$	The preset key
Key$_{Group}$	The group of keys (contains Key$_{Public}$ and N$_{ITER}$)
N$_{ITER}$	The number of the iterations of SM4 encryption
ID$_{groupkeys}$	ID of the group of keys

2) THE KEY UPDATE THROUGH DIGITAL CERTIFICATE

In our scheme, this digital certificate meets the standard of X509. A digital certificate maily contains the number of version, the number of certificate serial, the validity of certificate, SM2 public key, the name of issuer and subject name. SM2 public key mainly contains Key$_{Public}$ and the N$_{ITER}$ which is used for generating current symmetric key. The subject name is the code number of key management center in ground control station. The number of certificate serial is the ID of the Key$_{Group}$. After the certificate is invalid, the user needs to update the certificate through the Internet.

D. OVERALL AUTHENTICATION PROCESS

The overall information authentication process includes the message sending process at the transmitting end, the message receiving and authentication process at the receiving end. Through the analysis of the message receiving and authentication process, the scheme is further simplified and the anti-spoofing performance of the scheme is theoretically analyzed.

1) THE MESSAGE SENDING PROCESS

The procedures of message transmitting are shown in Fig. 13.

The content of GPSSS and group time authentication information should be encrypted by SM4 to obtain the ciphertext before the satellite transmitting messages. The ciphertext

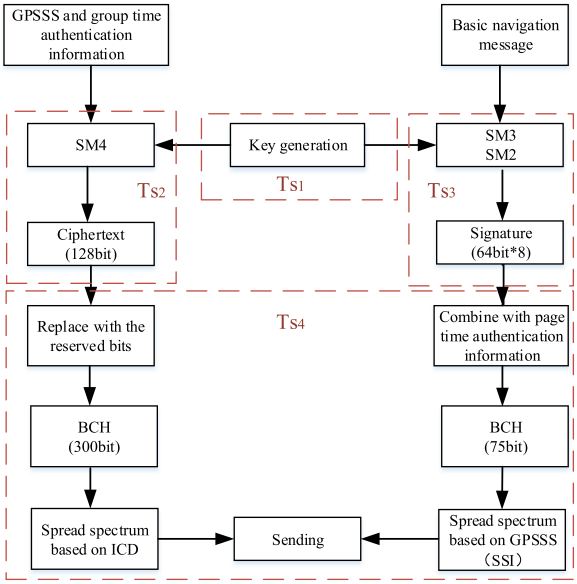

GPSSS and group time authentication information
Basic navigation message
SM4
Key generation
SM3 SM2
Ts2
Ts1
Ts3
Ciphertext (128bit)
Signature (64bit*8)
Ts4
Replace with the reserved bits
Combine with page time authentication information
BCH (300bit)
BCH (75bit)
Spread spectrum based on ICD
Sending
Spread spectrum based on GPSSS (SSI)

FIGURE 13. The procedures of the message transmitting.

replaces the corresponding reserved bits, which is shown in the Table 3. Meanwhile, the signature is generated by using SM2 and SM3 algorithms. The signature is split and combined with the page time authentication information, which is illustrated in the Table 4.

The check bits in these two kinds of information are generated by the BCH. Both of two messages are modulated by the respective spread spectrum sequences. The time spent in each procedure is shown in Table 6.

TABLE 6. The time consumption of each procedure (Before transmitting).

Procedure	The consumed time
Key generation	Ts_1
Encryption	Ts_2
Signature generation	Ts_3
Authentication messages modulation	Ts_4

Although many steps are taken before the message is transmitted, there is no significant time delay during the normal message transmitting. This situation is due to two reasons. One is that the ciphertext of the GPSSS and group time authentication information are generated before the next message transmitting. The other is that the satellite can get basic navigation information from the ground segment in advance and the signature is generated before the message transmitting. Therefore, the delay of signature generating does not affect the normal message transmitting. In general, these steps would not affect the normal message transmission excessively.

2) THE MESSAGE RECEIVING AND AUTHENTICATION PROCESS

The process of message authentication is shown in Fig. 14.

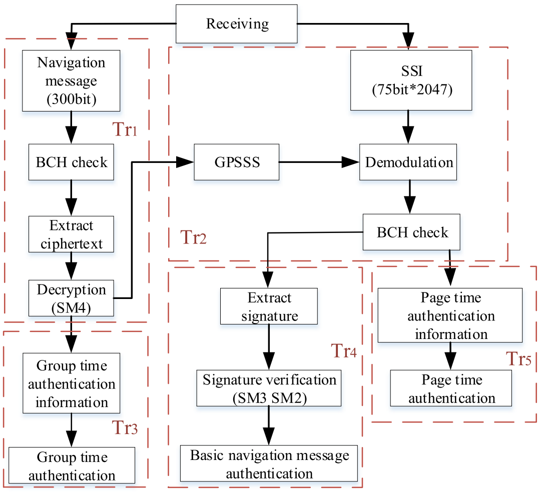

Receiving
Navigation message (300bit)
SSI (75bit*2047)
Tr1
BCH check
GPSSS
Demodulation
Extract ciphertext
Tr2
BCH check
Decryption (SM4)
Extract signature
Page time authentication information
Tr4
Tr5
Group time authentication information
Signature verification (SM3 SM2)
Page time authentication
Tr3
Group time authentication
Basic navigation message authentication

FIGURE 14. The procedures of message authentication.

The message authentication procedures of Fig.14 are as follows.

1) When Syn-bit 1 in the subframe 1 are received by receiver, the receiver stores the SSI. In our scheme, the storage time is about 0.15s.(SSI length is 75 bit and D2 navigation message transmitting speed is 500 bps, so SSI transmission takes 0.15s) Then, receiver continues to receive and demodulate the message of subframe 2.
2) After a group of subframe 1 is received by the receiver and the errors are corrected through the BCH code, the ciphertext is extracted from the navigation message. This ciphertext is decrypted by using the symmetric key of SM4 algorithm to get two types of information, the GPSSS and group time authentication information. The former is used for SSI demodulation. The latter is used for authenticating a group of SOW information. In order to verify the continuity of group time, it is necessary to compare the SOW in the received previous group of subframe 1 with received group time authentication information. If the comparison result is completely consistent, then the subframe 1 in the two groups will be true and time-continuous. Otherwise, the satellite navigation message may be fake. In this case, it is necessary to authenticate the page time and verify the integrity of the basic navigation information.
3) After performing the BCH code correcting on demodulated SSI, the page time authentication information and the signature of the basic navigation information are extracted.
4) For the purpose of performing page time authentication, it is necessary to compare the SOW in the received previous subframe 1 with the page time authentication information. If the comparison result is completely consistent, then the subframe 1 in the two pages will be true and time-continuous. Otherwise, the satellite navigation message may be fake. In this case, it is

necessary to verify the signature of the basic navigation information.

5) The obtained signature in step 3) is verified by the public key of SM2 algorithm and the digest of the received basic navigation information. If the signature verified successfully, the basic navigation information is trustable. Otherwise, it is fake. The receiver needs to delete the spoofing message and use the navigation message from other satellites to implement the positioning service. It should be noted that the digest information of basic navigation information is obtained through the calculation of SM3 algorithm.

3) AUTHENTICATION TIME CONSUMING AND SCHEME SIMPLIFICATION

The time consumption of each procedure in the Fig 14 is shown in Table 7.

TABLE 7. The time consumption of each procedure (After receiving).

Procedure	The consumed time
Satellite navigation signal demodulation	Tr_1
SSI demodulation	Tr_2
Group time authentication	Tr_3
Page time authentication	Tr_4
Signature verification	Tr_5

In BD-II-NMA&SSI scheme, the core is to verify the authenticity of time information (group time and page time) and the basic navigation information. With the update of navigation information, there are two cases of authentication of navigation information. First, when the basic navigation information has not changed (not updated within one hour [31]), only one successful authentication is required, and the basic navigation information that pass the authentication is retained. Second, when basic navigation information changes, it is necessary to verify its integrity in time.

If the receiver's authentication requirements for navigation message are not too high, it is only necessary to perform authentication on group time. The page time information does not need to be authenticated during the entire process. When the basic navigation information does not change, the signature information only needs to be authenticated once. In this case, for a low-demand anti-spoofing receiver, it is not necessary to always demodulate the spread spectrum information including the signature fragment and the page time authentication information. Therefore, for the low-demand anti-spoofing receiver, only the group time information authentication and the navigation message demodulation are time-consuming under the condition that the basic navigation information does not change. The authentication time consuming in two cases is shown in Table 8.

Therefore, based on the different requirements of anti-spoofing, selecting the appropriate authentication scheme can reduce the authentication time.

TABLE 8. The authentication time consuming in different cases.

Receiver	Basic navigation information	
	Not change (The signature was verified successfully)	Change
Normal receiver	$Tr_1+Tr_2+Tr_3+Tr_4$	$Tr_1+Tr_2+Tr_3+Tr_4+Tr_5$
Low-demand anti-spoofing receiver	Tr_1+Tr_3	$Tr_1+Tr_2+Tr_3+Tr_5$

4) THEORETICAL ANALYSIS OF ANTI-SPOOFING PERFORMANCE

From the perspective of the spoofer, the spoofer may perform spoofing attacks as shown in Table 9. BD-II NMA&SSI scheme can effectively resist these spoofing attacks, and the specific resistance process is as shown in Table 9.

TABLE 9. The spoofing measures and anti-spoofing approaches.

Spoofing measures	Anti-spoofing approaches
Launching a blocking attack on the receiver, forcing the receiver to recapture the signal to implement the spoofing attack.	The continuity of the page-to-page or group-to-group is broken. The receiver authenticate the group time and page time to detect this kind of spoofing.
Modifying the basic navigation information without the private key	Owning to the existing of the signature, in case the spoofer modifies the basic navigation information, the verification of signature is failed.
Modifying the basic navigation information with the private key	If the spoofer gets the private key in some way, the signature also would not be modified. Due to the spread spectrum modulation, the signature will be hidden into the noise. After the receiver and the spoofer getting the GPSSS, the correct signature has been transmitted to receiver. The correct signature information cannot successfully authenticate fake satellite navigation information. Thus, the signature verification is failed.

From the perspective of the receiver, the receiver may bring different authentication results for the three authentication methods. The combination of these different authentication results can determine whether the current received signal is subject to a spoofing attack or not. The specific analysis is shown in Table 10.

Table 10 shows that the proposed BD-II-NMA&SSI scheme can detect spoofing attacks from three aspects, group time authentication, page time authentication and signature verification, though the spoofer adopts different spoofing attacks.

V. SIMULATION EXPERIMENT AND RESULT ANALYSIS

In order to verify the effectiveness of the proposed scheme, an experimental framework was built, as shown in Fig. 15. Two kind of tools are used to perform the experiments. The MATLAB platform is used for simulating the satellite navigation message transmitting and receiving process.

TABLE 10. **The analysis of the authentication results.**

Item	Group time authentication	Page time authentication	Signature verification	Analysis
1	Fail	Fail	Fail	Generating spoofing attack (The spoofer modified satellite navigation message)
2	Fail	Fail	Success	Meaconing (The spoofer replays the previous group of subframe 1)
3	Success	Success	Fail	Generating spoofing attack (The spoofer modified basic navigation information)
4	Success	Success	Success	True Signal (Trusted message)

The Visual Studio-OPENSSL platform is used for accomplishing message encryption, decryption, signature generating, message verification and etc. In this experiment, our method for updating the key is obtained by downloading a digital certificate from the Internet.

In the part of raw data collection, the related devices and configuration are shown in the Table 11.

TABLE 11. **The devices of experiment.**

Basic information	Parameter
Antenna	GPS-703-GGG NovAtel
Receiver	FlexPak6 NovAtel
experiment computer 1	Pentium(R)Dual-Core CPU T4500 @ 2.30GHz/3GB RAM
experiment computer 2	Intel(R) Core (TM) CPU I7-6700HQ @2.59GHz/32GB RAM

The data used in the experiment is the real-time BeiDou-II navigation satellite signal received in North China. The details of the experimental data are shown in Table 12.

The part of navigation message generation and the part of navigation message transmission are illustrated in section V part A. In the key update process, the default is that the receiver has obtained the correct keys through the digital certificate. The receiver can perform navigation message authentication based on these keys. In the section V part B, the performance analysis for the three authentication methods (group time authentication, page time authentication, satellite location authentication) in this scheme is described.

TABLE 12. **The details of experiment data.**

Item	Parameters
Time	2:00pm~9:00pm, September 10th, 2017
Position	North China
Satellite number	2
Average carrier-to-noise ratio	43.4209dB
Data size	123MB

A. VERIFICATION PROCEDURES

The verification procedures are shown as follows.

a: Key generation

The parameter of elliptic curve in the SM2 algorithm has been illustrated in the reference [13] According to these parameters, the public key and private key of SM2 is generated. The symmetric key of SM4 is a group of random number.

b: Message encryption

The plaintext consists of the GPSSS and group time authentication information. In the simulation, the ID of codebook presents the GPSSS. The codebook of the GPSSS refers to the PN code table in the BD-II ICD [31] of different satellites. In our scheme, the GPSSS uses the PN code of satellite No.13.

c: The signature generating

The signature of the basic navigation information is generated by the private key of SM2 algorithm.

d: Generating satellite navigation signal with authentication function

The synchronization bits (Syn-bit 1) of the spread spectrum messages are the barker codes "1111100110101" and the synchronization bits (Syn-bit 2) of normal messages are also barker codes "11100010010". All the messages get the check bits through the BCH (15,11,1). Finally, the normal subframe 1 message is 300bits and the spread spectrum information of each subframe is 75 bits.

e: Transmitting process

The noise of the transmitting channel is gauss noise. According to relationship between carrier-to-noise (CNR) and signal-to-noise (SNR) in the literature [33], the relationship is shown in (1). The center frequency of BD-II signal (B1I) is 1561.098MHz and the 1 dB bandwidth of it is 4.092MHz. The sample frequency (f_s) is 8.184MHz.

$$SNR + 10\lg(\frac{f_s}{2}) = SNR + 69.12\text{dB} = CNR \qquad (1)$$

According to the Table 12, the average CNR is 43.4209dB. Calculated by formula (1), the SNR is no more than -25.69dB. The modulation and demodulation process are shown in Fig. 16 and Fig. 17.

B. SIGNAL VERIFICATION AND RESULT ANALYSIS

In the simulation, after BCH check and accomplishing the relative steps of signal verification, both the true and fake signals are tested. The test for time consuming and noise effect are shown as follows.

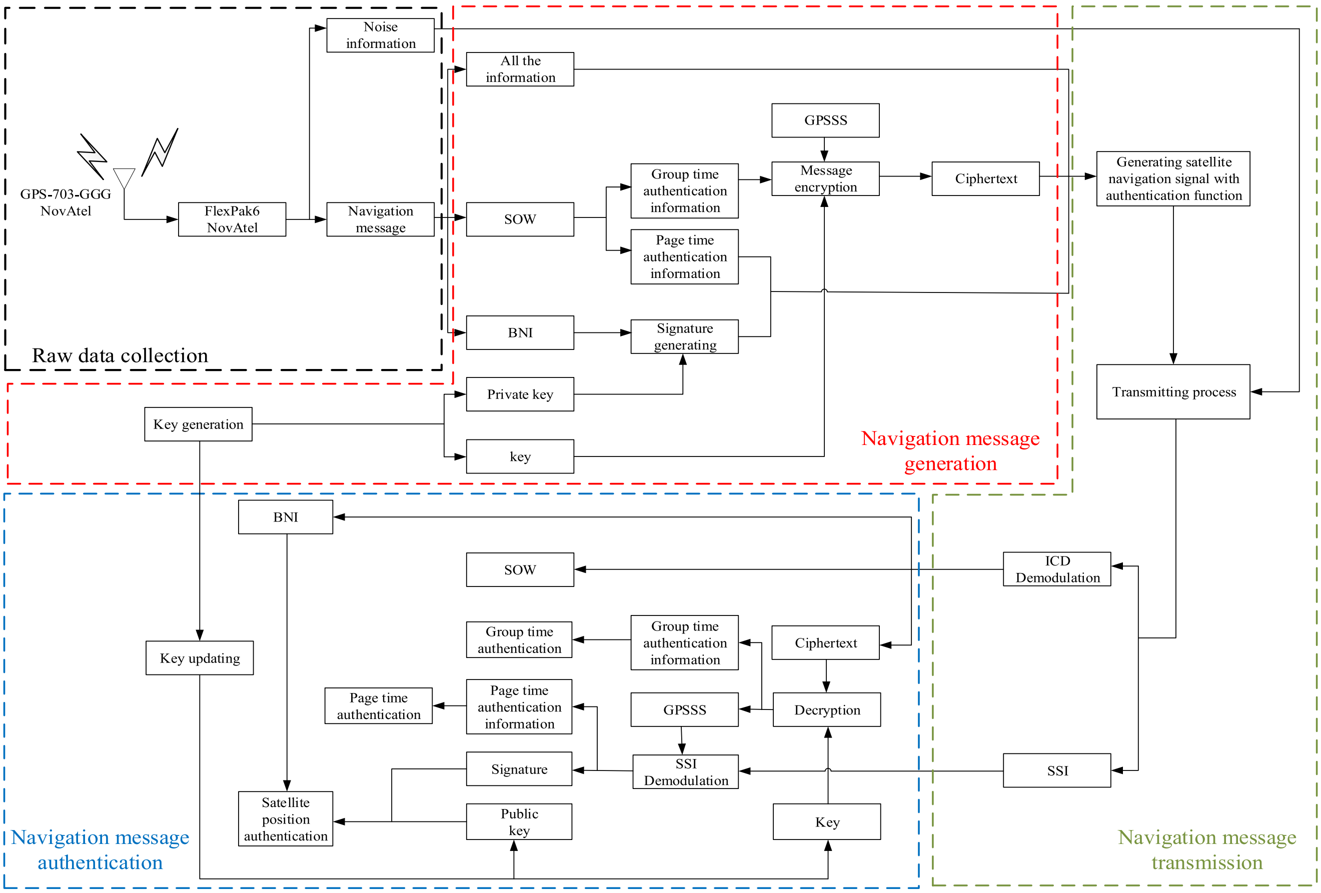

Noise information
All the information
GPS-703-GGG NovAtel
FlexPak6 NovAtel
Navigation message
SOW
GPSSS
Group time authentication information
Message encryption
Ciphertext
Generating satellite navigation signal with authentication function
Page time authentication information
BNI
Signature generating
Raw data collection
Private key
Key generation
key
Transmitting process
Navigation message generation
BNI
SOW
ICD Demodulation
Group time authentication
Group time authentication information
Ciphertext
Key updating
Page time authentication
Page time authentication information
GPSSS
Decryption
Signature
SSI Demodulation
SSI
Satellite position authentication
Public key
Key
Navigation message authentication
Navigation message transmission

FIGURE 15. The experimental framework.

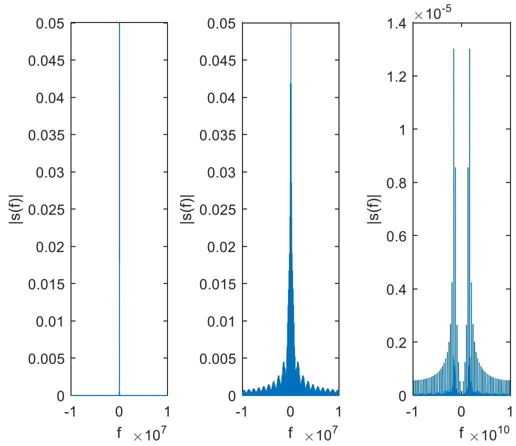


FIGURE 16. The process of signal transmitting. (Amplitude spectrum/Spread Spectrum modulation/Carrier modulation).

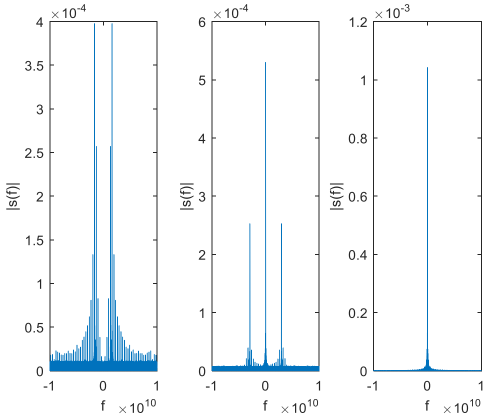


FIGURE 17. The process of signal receiving. (Add noise signal/Carrier demodulation/Spread Spectrum demodulation).

a: Time Consuming

Owning to signal verification process, some steps will be added to the normal signal transmitting and receiving. The consumed time is shown in the Table 13 and Table 14.

Taking the consumption time listed in Table 13 and Table 14 into account, the total time for transmitting the message is only 0.569 seconds. The time taken to insert the authentication spread spectrum information in the navigation message is 0.03 seconds. This time is very short and can be ignored during the information transmission process. When the receiver receives all the authentication message, the authentication result will be gotten before receiving subframe 3. The reason is that the total time consumed in the message receiving process is only 0.4485 seconds, which is less than 0.6 seconds per subframe. On the condition that the

TABLE 13. **Consumed time before transmitting the messages.**

Process	Time consuming (s)
Key generation (Ts_1)	0.182
Encryption (Ts_2)	0.003
Generated signature (Ts_3)	0.266
Authentication messages modulated by GPSSS (Ts_4)	0.3 0.03/ subframe
Total time for transmitting the messages (Ts_1+Ts_2+Ts_3+Ts_4)	0.569

TABLE 14. **Consumed time after message receiving.**

Process	Time consuming(s)
Satellite navigation signal demodulation and SSI demodulation (Tr_1+Tr_2)	0.267 0.0267/subframe
Group time authentication (Tr_3)	0.005(successful)/0.004(fail)
Page time authentication (Tr_4)	0.015(successful)/0.015(fail)
Signature verification (Tr_5)	0.156(successful)/0.168(fail)
Total time for receiving the message (Tr_1+Tr_2+Tr_3+Tr_4+Tr_5)	0.4485

receiver does not receive all the authentication message, the receiver needs to wait 45 seconds and receive the authentication message of next group.

b: Noise effect

Due to our scheme based on the navigation message and cryptography algorithm, the authentication results should be correct when there is no bit error caused by the noise. Therefore, the power of noise affects not only the results of error correction of BCH, but also the detection of probability (P_d). In the experiment, when the SNR is gradually decreasing, the probability of the detection result is shown in Fig. 18.

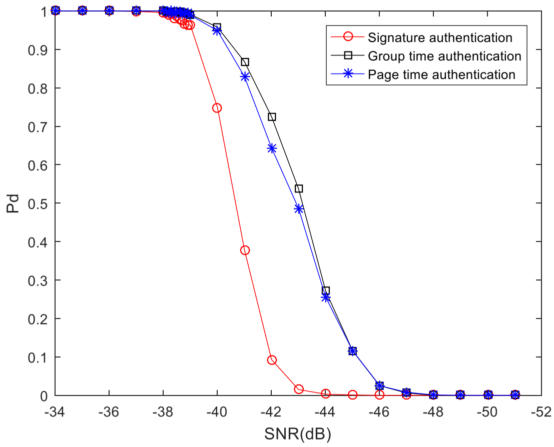


FIGURE 18. **The relationship between the SNR and the probability of authentication.**

In the experimental environment, the carrier-to-noise ratio is 43.4209dB, and the corresponding signal-to-noise ratio is −25.69dB. According to the analysis in Fig. 18, our scheme can resist the spoofing attack under this SNR.

The authentication success rate of signature, group time authentication and page time authentication are *P1*, *P2* and *P3*. In Fig. 18, when the SNR is lower than -33dB, *P1* begins to below 100%. When the SNR is lower than -35dB, *P1*, *P2* and *P3* all below 100%. Overall, the signature authentication rate curve drops faster than the other two. The reason is that the signature contains more authentication information than the other two. In the case of large noise, the signature authentication information is more prone to error.

Considering that the navigation message is repeated broadcast, when the authentication rate of *P1*, *P2* and *P3* exceed a certain threshold, the authentication can be considered successful. In the optimized scheme, the detection rate of the scheme can be expressed as follows.

$$P_d = \begin{cases} 1(P_1 + P_2 + P_3)/3 \geq threshold \\ P_1 \quad Others \end{cases} \tag{2}$$

When the threshold values are 0.99 and 0.995, this scheme is compared with the scheme of T. Humphreys [28] applied in the BeiDou-II D2 navigation message. The comparison results are shown in Fig. 19.

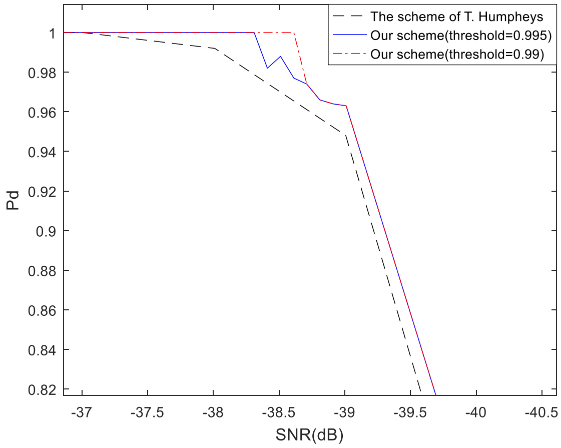


FIGURE 19. **The comparison between our scheme and the scheme of T. Humpheys.**

In Fig. 19, our scheme has a better resistance to noise than the scheme of T. Humpheys in the same SNR conditions. The reason is that only the basic navigation information is certified in this scheme, while T. Humpheys' scheme authenticates the overall message. To general chip receivers, its positioning results are based on basic navigation information, and less attention is paid to ionospheric parameters and other information. Therefore, this scheme is suitable for the actual portable receiver or chip receiver. In addition, the threshold value can be adjusted as the receiver at different locations to improve the anti-noise performance of the scheme.

C. COMPARISON

Combining with the other studies about anti-spoofing based on the NMA, the comparison among their feature and performance is shown in Table 15.

TABLE 15. **Comparison among our scheme and other schemes.**

Aspects	The scheme of Tang Chao [30]	The scheme of T. Humpheys [28]	Our scheme
Satellite platform	BeiDou-II	GPS	BeiDou-II
Used cryptogram	ECDSA	ECDSA	SM2 SM3 SM4
Authentication method	DSA	DSA	DSA and SSI protection
Defending generation spoofing attack	YES	YES	YES
Defending meaconing attack	NO	NO	YES
Navigation message designing	Not mentioned	YES	YES
Key updating	YES	Not mentioned	YES
Signature information protect	NO	NO	YES

The SM2, SM3 and SM4 algorithms are independently developed by State Cryptography Administration. SM2 has become an international standard. SM3 and SM4 are also gradually recognized internationally. The random number generator of SM2, SM3 and SM4 algorithms designed by State Cryptography Administration. The design of random number generator details are not open to the public, which guarantees the security of our scheme. As is illustrated in the Table 9 in section IV, under the circumstance that the spoofer only replays the past message and the signature is not modified in the ''same single-star spoofing'', our scheme can detect it but the scheme of Tang Chao [30] or the scheme of T. Humpheys [28] cannot. The reason is that our scheme can detect the continuity of navigation messages. Our scheme also protects the signature and time authentication message from being modified by using the spread spectrum modulation, which prevents some special circumstances, for instance, private key leakage.

VI. CONCLUSION

Based on the analysis of the spoofing attack, this paper proposed an anti-spoofing method of BD-II-NMA&SSI based on the D2 satellite navigation message. We use SM4 algorithm to encrypt time authentication messages. The SM2&SM3 algorithms are used for generating the signature. Also, we conceal it into the D2 navigation message with the spread spectrum modulation technology. The paper has proven that through this scheme can successfully detect the ''same single-star spoofing attack''. The research also shows that the encryption and verification time are not affect the operation of satellite navigation system excessively. The effect between the gauss noise power and detection probability has also been tested in the simulation to evaluate the performance of this scheme.

In future research, interference like multipath signals, block signals, etc., can be considered to test our scheme. The research will use the authentication protocol (like TESLA) to avoid changing of frame structure and achieve the aim related to this paper.

REFERENCES

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

[2] B. Forssell, "The dangers of GPS/GNSS," in *Proc. Coordinates Mag.*, May 2009, pp. 6–8.

[3] C. J. Wullems, "A spoofing detection method for civilian L1 GPS and the E1-B galileo safety of life service," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 48, no. 4, pp. 2849–2864, Oct. 2012.

[4] T. E. Humphreys, "Detection strategy for cryptographic GNSS anti-spoofing," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 2, pp. 1073–1090, Apr. 2013.

[5] United States Department of Transprotatioin. *Eastern Mediterranean Sea-GPS Interference*. Accessed: Feb. 19, 2019. [Online]. Available: https://www.maritime.dot.gov/content/2018-007-eastern-mediterranean-sea-gps-interference

[6] T. E. Humphreys, "Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing," *Univ. Texas at Austin*, pp. 1–16, Jul. 2012. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.665.3693&rep=rep1&type=pdf

[7] Inside GNSS. *GPS Spoofing Experiment Knocks Ship Off Course*. Accessed: Jul. 2013. [Online]. Available: https://insidegnss.com/gps-spoofing-experiment-knocks-ship-off-course/

[8] K. D. Wesson, B. L. Evans, and T. E. Humphreys, "A combined symmetric difference and power monitoring GNSS anti-spoofing technique," in *Proc. IEEE Global Conf. Signal Inf. Process.*, Dec. 2013, pp. 217–220.

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

[10] W. Qi, Y. Zhang, and X. Liu, "A GNSS anti-spoofing technology based on Doppler shift in vehicle networking," in *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Sep. 2016, pp. 725–729.

[11] K. D. Wesson, M. P. Rothlisberger, and T. E. Humphreys, "A proposed navigation message authentication implementation for civil GPS anti-spoofing," in *Proc. 24th Int. Tech. Meeting Satellite Division The Inst. Navigat. (ION GNSS)*, Portland, OR, USA, 2011, pp. 3129–3140.

[12] *Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves, Part 1: General*, Standard GB/T 32918.1-2016, Standardization Administration of the People's Republic of China, National Standard of the People's Republic of China, 2016.

[13] *Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves, Part 2: Digital Signature Algorithm*, Standard GB/T 32918.2-2016, Standardization Administration of the People's Republic of China, National Standard of the People's Republic of China, 2016.

[14] *SM3 Cryptographic Hash Algorithm*, Standard GB/T32905-2016, Standardization Administration of the People's Republic of China, National Standard of the People's Republic of China, 2016.

[15] *SM4 Block Cipher Algorithm*, Standard GB/T 32907-2016, Standardization Administration of the People's Republic of China, National Standard of the People's Republic of China, 2016.

[16] K. Chino, D. Manandhar, and R. Shibasaki, "Authentication technology using QZSS," in *Proc. IEEE/ION Position, Location Navigat. Symp. (PLANS)*, May 2014, pp. 367–372.

[17] Z. Wu, R. Liu, and H. Cao, "ECDSA-based message authentication scheme for BeiDou-II navigation satellite system," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 55, no. 4, pp. 1666–1682, Aug. 2019.

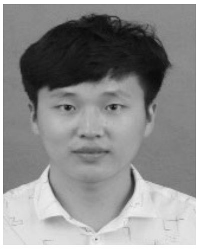
[18] I. Fernández-Hernández, V. Rijmen, G. Seco-Granados, J. Simon, I. Rodríguez, and J. D. Calle, "A navigation message authentication proposal for the galileo open service," *J Inst Navig*, vol. 63, no. 1, pp. 85–102, Mar. 2016.

[19] 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. Int. Conf. Localization (ICL)*, Barcelona, Spain, Jun. 2016, pp. 1–6.

[20] 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," in *Proc. China Satell. Navigat. Conf. (CSNC)*, 2017, pp. 69–80.

[21] A. J. Kerns, K. D. Wesson, and T. E. Humphreys, "A blueprint for civil GPS navigation message authentication," in *Proc. IEEE/ION Position, Location Navigat. Symp. (PLANS)*, Monterey, CA, USA, May 2014, pp. 262–269.
[22] O. Pozzobon, "Keeping the spoofs out: Signal authentication services for future GNSS," in *Proc. GNSS*, May 2011, pp. 48–55.
[23] O. Pozzobon, G. Gamba, and M. Canale, "From data schemes to supersonic codes. GNSS authentication for modernized signals," *Inside GNSS*, vol. 10, no. 1, pp. 55–64, Jan. 2015.
[24] M. G. Kuhn, "An asymmetric security mechanism for navigation signals," in *Information Hiding* (Lecture Notes in Computer Science), vol. 3200. Berlin, Germany: Springer-Verlag, 2004, pp. 239–252.
[25] E. Gkougkas, D. Dötterböck, T. Pany, and B. Eissfeller, "A low-power authentication signal for open service signals," in *Proc. 30th Int. Tech. Meeting Satell. Division Inst. Navigat. (ION GNSS)*, Portland, Oregon, Dec. 2018, pp. 3865–3878.
[26] B. Motella, D. Margaria, and M. Paonni, "SNAP: An authentication concept for the Galileo open service," in *Proc. IEEE/ION Position, Location Navigat. Symp. (PLANS)*, Monterey, CA, USA, Apr. 2018, pp. 967–977.
[27] D. Margaria, B. Motella, M. Anghileri, J.-J. Floch, I. Fernandez-Hernandez, and M. Paonni, "Signal structure-based authentication for civil GNSSs: Recent solutions and perspectives," *IEEE Signal Process. Mag.*, vol. 34, no. 5, pp. 27–37, Sep. 2017.
[28] K. Wesson, M. Rothlisberger, and T. Humphreys, "Practical cryptographic civil GPS signal authentication," *J. Inst. Navigat.*, vol. 59, no. 3, pp. 177–193, Sep. 2012.
[29] D. Liu, J. Lv, and M. Rui, "The research and prospect of spoofing and anti-spoofing technology in the satellite navigation system," *Commun. Technol.*, vol. 50, no. 5, pp. 837–843, Sep. 2017.
[30] C. Tang, X. Sun, and Y. Ji, "Research on GNSS civil navigation message encryption authentication technology," in *Proc. Comput. Simulation*, Sep. 2015, pp. 86–108.
[31] *Beidou Navigation Satellite System Signal in Space Interface Control Document, Open Service Signal (Version 2.1)*, document P 020180507527106075323, China Satellite Navigation Office, Beidou-II System Interface Control document (BDS-ICD), Nov. 2016. [Online]. Available: http://www.beidou.gov.cn/xt/gfxz/201805/P020180507527106075323.pdf
[32] X. Cheng, G. Chen, and L. Ji, "Data security application based on BeiDou-II satellite navigation system," in *Proc. Inf. Secur. Commun. Privacy*, 2011, pp. 43–45.
[33] X. Ba, H. Liu, and Y. Zheng, "An effective GNSS receiver carrier-to-noise ratio estimation method," *J. Wuhan Univ.*, vol. 36, no. 4, pp. 457–460 and 466, 2011.

ZHIJUN WU received the B.S. and M.S. degrees in information processing from Xidian University, China, and the Ph.D. degree in cryptography from the Beijing University of Posts and Telecommunications, China. He was a Professor with the Department of Communication Engineering, Civil Aviation University of China. His research areas are denial-of-service attacks, and security in big data and cloud computing.



YUN ZHANG received the B.S. degree in communication engineering from the University of Jinan, China. He is currently pursuing the master's degree in information security with the Civil Aviation University of China. His research interest includes satellite information security.

RUSEN LIU received the B.E. degree in electronic information engineering from the Civil Aviation University of China, Tianjin, China, in 2015, and the M.E. degree in information and communication engineering from the School of Electronics and Information and Automation, Civil Aviation University of China. His research interest includes satellite information security.