IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received May 9, 2020, accepted August 3, 2020, date of publication August 17, 2020, date of current version August 28, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3016971

Research on Multi-Peak Detection of Small Delay Spoofing Signal

JUNZHI LI, XIANGWEI ZHU, MINGJUN OUYANG, WANQING LI, ZHENGKUN CHEN, AND ZHIQIANG DAI

School of Electronics and Communication Engineering, Sun Yat-sen University, Guangzhou 510006, China

Corresponding author: Xiangwei Zhu (zhuxw666@mail.sysu.edu.cn)

This work was supported in part by the Key Special Projects of the National Key Research and Development Plan under Grant 2018YFB0505200, in part by the National Natural Science Foundation of China under Grant 61973328, and in part by the Project supported by the Major Research Plan of the National Natural Science Foundation of China under Grant 91938301.

ABSTRACT With the widespread application of GNSS systems in various fields, the problem of spoofing detection has drawn much attention from the satellite navigation community. The GNSS spoofing interference generally uses fake or replayed satellite signals to make the targeted receivers receive false GNSS signals and reduce the accuracy of calculated position and time information. In order to ensure and improve the security of GNSS services, in recent years, academia and industry have studied the spoofing detection technology from multiple aspects, and many theoretical results have been obtained. This paper starts the analysis from the acquisition phase of a receiver and analyzes the characteristics of the small-delay spoofing signal. Aiming at solving the problem that it is difficult to detect small-delay (0–2 chips) spoofed signals during the acquisition phase, the CNN (Convolutional Neural Network) based method is used to detect the small-delay spoofed signals effectively. According to the experimental simulation results, when the code phase difference between the spoofing signal and the authentic satellite signal is larger than 0.5 code chip, the CNN-based method achieves high detection accuracy. In addition, the algorithm can quickly detect the data without using any additional equipment. Therefore, low complexity is achieved. This makes the algorithm has a good engineering application prospect.

INDEX TERMS Acquisition phase, convolutional neural network (CNN), GNSS spoofing detection, small delay.

I. INTRODUCTION

With the development of the Global Navigation Satellite System (GNSS), the satellite navigation technology has been widely used in the military and civil fields, including military, aviation, communications, business, and many other fields [1], [2]. Nowadays, the rapid development and popularization of mobile communication, automobile, and other industries have made the GNSS be more deeply integrated into people's daily lives. People enjoy the great convenience brought by the GNSS. The importance of GNSS to the military field is self-evident, and it is an important support for electronic warfare, information warfare, and long-range warfare. Besides, it is one of the most basic and important technical means for the precision strike of missiles and other types of weapons. The GNSS can not only provide positioning and navigation but also many services, such as accurate time synchronization [1], [3]. In summary, the GNSS has strong application value in many fields, from financial transaction records to military and aerospace applications [4]–[6].

However, with the rapid development of technology, the vulnerability of GNSS signals to interference and spoofing has been gradually exposed. On the one hand, since the signals of navigation satellites are transmitted over a long distance, these signals are extremely weak when they reach the ground, and they are easily affected by interference signals in their frequency bands [7], [8]. On the other hand, because civil signals are publicly used in the international scope, they are not confidential since they are easy to decipher, thus making receivers extremely vulnerable to interference attacks [9].

The GNSS interference technologies generally include suppressing interference, spoofing interference, and others [10], [11]. The suppressing interference is less difficult

The associate editor coordinating the review of this manuscript and approving it for publication was Tawfik Al-Hadhrami.

to implement. The principle is to suppress the reception of the front-end satellite signals by sending a high-power interference signal in the coverage area of a jammer to make it non-working. However, the power required for implement the suppressing interference is too large to be found, and it is easy to find, so its interference source also has the risk of being attacked [12].

The GNSS spoofing can be divided into generative spoofing interference and transponder spoofing interference in terms of the generation mode of spoofing signals. The transponder spoofing interference is realized by recording the authentic satellite signals and transmitting them to the target receiver through a GNSS signal simulator or transponder with a certain delay, thus making the attacked target calculate the wrong position and time information. The realization of the generative spoofing interference is more complex; namely, attackers extract location, time, satellite ephemeris, and other related information from the authentic satellite signals and align false GPS signal carriers with the authentic GPS signals. Then, a GPS spoofing signal, including specific position and misleading time, is generated by a program and transmitted to the target GPS receiver via antenna, thus making the GPS receiver calculate the wrong position and time information. In contrast to the suppressive interference, the spoof interference does not require strong signal transmission power, and can even perform spoofing (such as generative spoofing interference) without relying on the GNSS systems, which is more threatening to the receiver [13]; also, since it can make the user terminal output wrong position and time information without being found, it is most concealing and destructive.

Recent international GNSS spoofing attack incidents have proven the threat of spoofing interference attacks. In 2011, Iranian engineers used the GPS spoofing interference technology to capture the RQ-170 unmanned surveillance aircraft produced by the US military [14]. In 2012 and 2013, the Humphreys team successfully tricked the unmanned helicopter system and positioning navigation device of the ‘‘White Rose’’ yacht [15], [16]. In 2017, GPS spoofing interference attacks in the Black Sea caused the GPS positioning system of dozens of ships were out of work. In 2018, the Russian air defense system in Syria found multiple drones approaching Russian military facilities. The Russian military successfully controlled six UAVs approaching Russian military facilities using the ‘‘vehicle yard’’ active interference system. These spoofing incidents have further increased our awareness of the potential harm of spoofing attacks.

The high-developing software radio technology has made spoofing interference easier to implement, more flexible and diversified, and less costly. Thus, anti-spoofing is no longer a concern of only military users because civilians can also be highly affected by decreased safety and reliability of GNSS applications caused by spoofing [17]. Therefore, it is crucial to study the GNSS spoofing interference detection technology to ensure the satellite navigation system can provide end-users with normal and safe navigation, positioning, and timing services.

The research of the anti-spoofing interference has been increasing both in the industry and the academia, and the detection technology of spoofing interference has become a research hotspot in the field of satellite navigation. During recent research on GNSS spoofing interference detection, academia has proposed many detection methods from different levels of the receiver.

In [18], it was proposed to use the correlation feature between two receivers to detect spoofing signals. However, this method requires using two receivers. In addition, in the spoofing environment, it is impossible to know the information from which of the receivers is reliable, so the detection performance cannot be guaranteed. Signal power detection technology is also an effective detection method. In this method, the receiver continuously monitors the power-related parameters, which may be abnormal when spoofing attacks are present. The power-related parameters include C/N_0 (carrier-to-ratio) [19], Signal Quality Monitoring (SQM) [20], absolute power [21], and distribution verification of correlator output [22]. These technologies require the receiver to have high precision in measuring the received signal’s parameters and complex hardware. In addition, the absolute power detection is easily affected by antenna type, antenna attitude, and multipath, and it requires additional energy detection devices on the receiver side to achieve it. It should be pointed out when the spoofed signal is transmitted together with the noise, the C/N_0 detection method easily leads to misjudgment.

In [23], [24], a GPS spoofing detection scheme based on the direction of arrival was proposed. This scheme judges the arrival angle of signals by resolving the changes of signals of different antennas, to distinguish whether the current target is subjected to GPS spoofing. However, when the target receiver can receive only one or two GPS signals or the GPS spoofing system is deployed in the direction of the satellite-to-target connection, the GPS spoofing cannot be effectively detected by analyzing the direction of arrival of the received signals. Thus, this detection method requires receivers to use multiple antennas, which significantly increases the hardware cost.

In [25], [26], a method for automatic gain control (AGC) detection was introduced. Namely, by delaying and amplifying the spoofing, the mixed noise signal is also amplified, so the AGC gain is quickly reduced. Therefore, the main idea of the AGC detection method is to detect spoofing signal by monitoring this abnormal change. However, the AGC module is expensive, which leads to a decrease in the algorithm value.

A detection method based on the signal arrival time was proposed in [27]. In this method, by detecting the time difference between the times when the signal arrives at the receiver, it is determined whether there is a spoofing signal. The application of this method is limited mainly to forwarding spoofing, which has little effect on generative spoofing signals and can even eliminate authentic signals and retain spoofing signals. In [28], the Doppler frequency shift-based detection method was proposed. The principle of this method is that when a receiver moves randomly, the Doppler frequency difference between the authentic satellite signals is non-linear in the time domain, while that between spoofing signals is linear. However, this method is only suitable for detecting the spoofing signals transmitted by a single antenna.

In [29], an anti-spoofing algorithm based on a single receiver pseudo-range difference was proposed. This algorithm can be used to detect simple and intermediate spoofing attacks and meaconing attacks. Further, an adaptive spoofing suppression algorithm based on a multi-antenna array was proposed in [30]. This algorithm can adaptively generate zeros using the cross-correlation gain of multi-antenna arrays and suppress multiple spoofing signals simultaneously. In [31], [32], a low-cost inertial measurement unit (IMU) spoofing detection method was proposed. This method judges whether there is a spoofing attack by comparing the consistency of equivalent acceleration and angular velocity. In [33], an innovative INS-assisted spoof monitoring method was presented. The principle of this method is to detect spoofing signals by detecting abnormal measurements of the angular state of aircraft. However, devices such as IMU and INS are expensive and thus are not widely used in civil applications. A spoofing interference detection method based on the S-curve-bias (SCB), which gradually adjusts the dynamic characteristics of the signal, was proposed in [34]. The experimental results have shown that SCB has the potential of detecting spoofing interference. In [35], a detection method based on double-antenna power measurements was proposed. This method can be used in the unsynchronized case.

The multi-peak detection method [36] is applied during the acquisition phase. The principle is to determine the spoofing signals by detecting whether there are two or more correlation peaks in a two-dimensional matrix of the Doppler frequency and code phase. This method is generally applicable to situations where the code phase of the spoofing and authentic satellite signals has a large offset, but when the code phase shift of spoofing signals is small (for instance, less than one chip), the number of peaks cannot be detected effectively.

This paper starts from the multi-peak detection direction, and studies the spoofing detection in the case that the code phase of the spoofed signal differs from that of the authentic satellite signal by 0–2 chips. Based on the idea of deep learning, a convolutional neural network (CNN) is used to detect spoofing signals during the acquisition phase. The experimental simulation results, at the code phase difference between the spoofed and authentic satellite signals of 0.5 chips or more, show that the spoofing signals can be effectively identified.

The rest of the paper is organized as follows. In Section II, the signal model is presented and analyzed. In Section III, a CNN-based GNSS spoofing interference detection algorithm is introduced. The simulation results and performance of the proposed algorithm in detecting spoofing signals are presented in Section IV. The conclusions are given in Section V.

II. SIGNAL MODEL AND ANALYSIS

A. SIGNAL MODEL

A general internal structure of a universal GNSS receiver is shown in Fig. 1. In most GNSS receivers, the received RF signal is converted into an intermediate frequency (IF) signal, which is then processed.

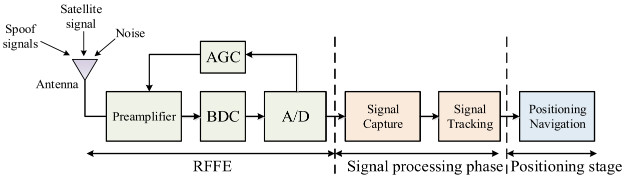

FIGURE 1. The internal structure of universal GNSS receiver.

In the presence of spoofing interference, the received IF signal of a single antenna receiver can be expressed as:

$$S_R(t) = S_T(t) + S_S(t) + n_0(t) \tag{1}$$

In (1), $S_R(t)$ denotes the received IF signal, t denotes time in seconds, $S_T(t)$ and $S_S(t)$ denote the authentic satellite signal and spoofing signal, respectively; $n_0(t)$ denotes the additive white Gaussian noise (AWGN) with zero mean and variance $\boldsymbol{\sigma}^2$.

The authentic satellite signal can be expressed as:

$$\begin{aligned} S_T(t) = &\sum_{i=1}^{M} \sqrt{P_i^T} C_i\left(t-\boldsymbol{\tau}_i^T\right) D_i^T\left(t-\boldsymbol{\tau}_i^T\right) \\ &\times \cos\left[2\boldsymbol{\pi}\left(f_{IF}+f_{D,i}^T\right)t+\boldsymbol{\varphi}_i^T\right)\right] \end{aligned} \tag{2}$$

where M represents the number of authentic satellite signals in the received signal, P_i^T denotes the received power of the i-th signal; $C_i(t)$ denotes the spreading code of the i-th satellite, $D_i^T(t)$ denotes the data bit of the i-th navigation message; f_{IF} represents the IF signal, $f_{D,i}^T$ denotes the Doppler frequency of the i-th authentic satellite signal; $\boldsymbol{\tau}_i^T$ represents the code phase of the i-th signal; and lastly, $\boldsymbol{\varphi}_i^T$ denotes the initial carrier phase of the authentic satellite signal.

The spoofing signal has the same signal structure as the authentic satellite signal, so the spoofing signal can be expressed as:

$$\begin{aligned} S_S(t) = &\sum_{i=1}^{N} \sqrt{P_i^S} C_i\left(t-\boldsymbol{\tau}_i^T\right) D_i^S\left(t-\boldsymbol{\tau}_i^S\right) \\ &\times \cos\left[2\boldsymbol{\pi}\left(f_{IF}+f_{D,i}^S\right)t+\boldsymbol{\varphi}_i^S\right)\right] \end{aligned} \tag{3}$$

where N denotes the number of satellites included in the spoofing, P_i^s denotes the received signal's power of the ith satellite, and $D_i^s(t)$ denotes the ith signal's data bit stream; $\boldsymbol{\tau}_i^s$ denotes the ith signal's code phase, $f_{D,i}^S$ denotes the Doppler frequency shift of the ith authentic satellite signal, and $\boldsymbol{\varphi}_i^s$ represents the initial carrier phase.

Based on (1) and (3), in a spoofing interference environment, the signal received by a receiver represents a mixture of spoofing and authentic signals. In general, spoofing will include most or all the satellites in the authentic satellite. Therefore, in the receiver acquisition and channel tracking, the processed signal actually represents the superposition of authentic and spoofing signals.

B. MODEL ANALYSIS

The transponder spoofing interference principle is to forward the authentic satellite navigation signal to the target receiver with a certain delay and amplification to cause a positioning error. Generally, a large-delay spoofing signal denotes an interfering signal with a delay of more than two chips. This characteristic is used in the multi-peak detection algorithms to detect spoofing signals. When the forwarding delay of a spoofing signal is large, the detection of the forwarding-type spoofing interference is realized by detecting the number of relevant peaks that exceed the capture threshold during the signal acquisition process.

In the capture phase, the multi-peak detection algorithm determines the number of peaks that exceed the preset correlation peak threshold to detect the spoofing. Generally, if there is only an authentic satellite signal in the received satellite signal, there will be only one correlation peak that exceeds the preset correlation peak threshold, as shown in Figs. 2 and 3. In contrast, when a spoofing signal exists, two or more correlation peaks will exceed the preset threshold, as shown in Fig. 4.

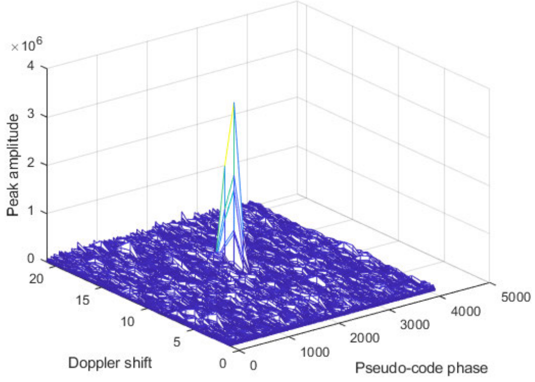

FIGURE 2. The authentic satellite signal in the acquisition phase.

Accordingly, in the acquisition stage, by detecting the peaks larger than the correlation peak threshold, the presence of a spoofing interference signal can be detected. However, this holds for situations where the phase values of the spoofing interference signal and authentic satellite signal are quite different, i.e., when an offset is two or more chips, as shown in Fig. 5.

When the phase difference between the spoofing and authentic satellite signal is less than two chips, the performance of the traditional multi-peak detection method in identifying the spoofing signal is reduced, especially when the spoofing signal delay is less than one chip. As presented in Fig. 6, when the phase of the spoofing signal differs from that of the authentic satellite signal by one chip, there is only one peak, so it is more difficult to distinguish whether there is a spoofing signal.

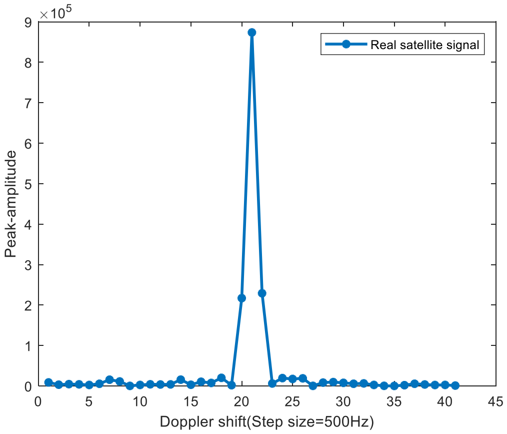

FIGURE 3. The amplitude peak of the authentic signal peak.

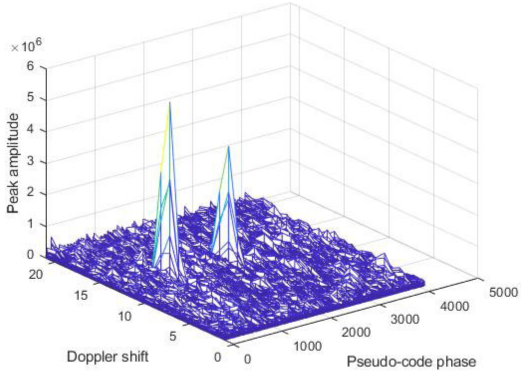

FIGURE 4. Spoofing and authentic signals in the acquisition phase.

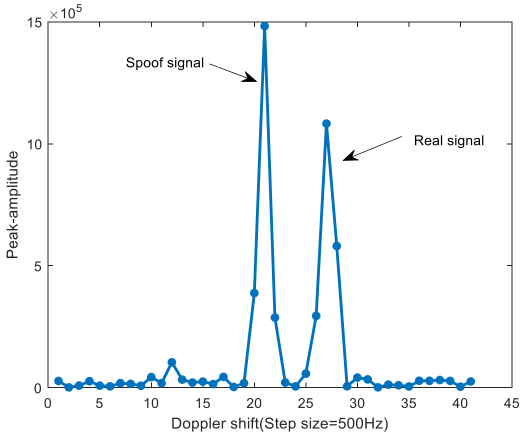

FIGURE 5. Spoofing signal code phase with a three-chip delay.

To improve the performance of the multi-modal detection method in the acquisition stage, the CNN-based method is used to detect small-delay spoofing signals.

III. SMALL-DELAY SPOOFING DETECTION METHOD BASED ON CNN

The CNNs have made great success in the fields of image recognition, video recognition, and speech recognition.

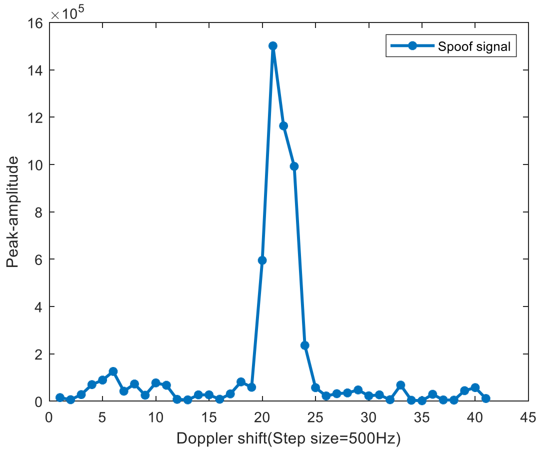

FIGURE 6. Spoofing signal with a one-chip delay.

However, the application of deep learning in the field of navigation signal processing has been relatively rare. In this paper, a CNN-based method that represents a combination of deep learning and satellite communication technology is used to detect the GNSS spoofing signal.

A. ALGORITHM

The GNSS receiver estimates the Doppler shift and pseudo-code phase of satellite navigation signals by searching for correlation peaks in the two-dimensional matrix. In the capture phase, it is more effective to determine whether there is a spoofing signal based on the number of found correlation peaks. However, when the forwarding delay of a spoofed signal is less than two chips, the correlation peaks of the authentic navigation signal and spoofing signal overlap, and generally, only one correlation peak appears, which makes the spoofing detection difficult. Hence, the spoofing signal detection base on the number of correlation peaks is not reliable in all cases. To overcome this problem, a CNN-based method is developed to extract the characteristics of the small-delay spoofing signal from the image field. The flowchart of the proposed algorithm is shown in Fig. 7.

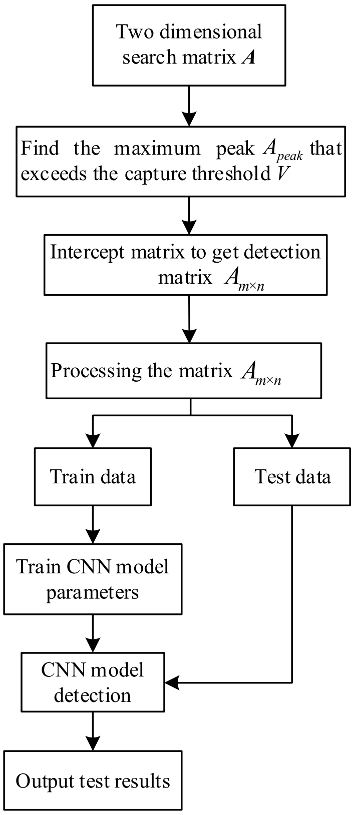
Two dimensional search matrix A
Find the maximum peak A_{peak} that exceeds the capture threshold V
Intercept matrix to get detection matrix $A_{m\times n}$
Processing the matrix $A_{m\times n}$
Train data
Test data
Train CNN model parameters
CNN model detection
Output test results

FIGURE 7. The flowchart of the CNN-based spoofing detection algorithm.

B. DATA PROCESSING

A GNSS receiver that uses the FFT algorithm to capture the IF signal estimates the Doppler shift and code phase of the satellite navigation signal by searching the correlation peaks in the two-dimensional matrix. In this work, the Doppler frequency shift search range is set to [−5 kHz, 5 kHz], and the spoofing signal delay relative to the authentic satellite signal is from zero to two chips. The steps of obtaining the dataset are as follows:

- **Step 1**: Search a two-dimensional matrix $\boldsymbol{A}$ to find peak A_{peak} that is greater than the capture threshold $\boldsymbol{V}$.
- **Step 2**: In the two-dimensional matrix $\boldsymbol{A}$, intercept the data in the range of [−2 kHz, 2 kHz] on the Doppler frequency shift axis and the chip range of [−2, 2] on the code phase axis around the location of the highest peak A_{peak} to obtain the detection matrix $A_{m\times n}$, as shown in Fig. 8. Among them, $m = 4/\Delta f_D + 1, n = 4/\Delta T_{CA} + 1$, where Δf_D and ΔT_{CA} represent the Doppler frequency shift search step and code phase search step, respectively.
- **Step 3**: Set all data in matrix $A_{m\times n}$ that are below the threshold $\boldsymbol{V}$ to zero to obtain a new matrix $Q_{m\times n}$, as shown in Fig. 9.
- **Step 4**: Normalize the non-zero data of the newly-obtained matrix $Q_{m\times n}$ to obtain the target matrix $B_{m\times n}$

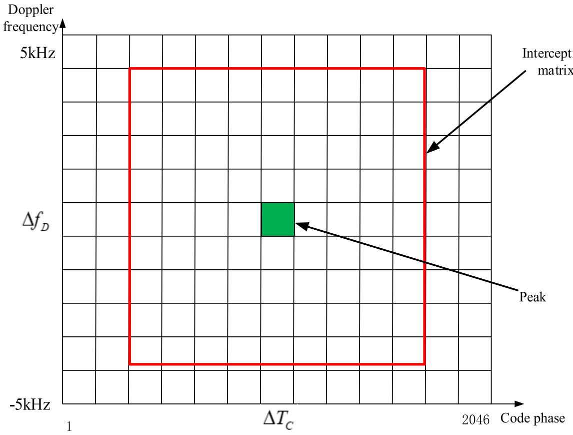

FIGURE 8. Example of interception matrix.

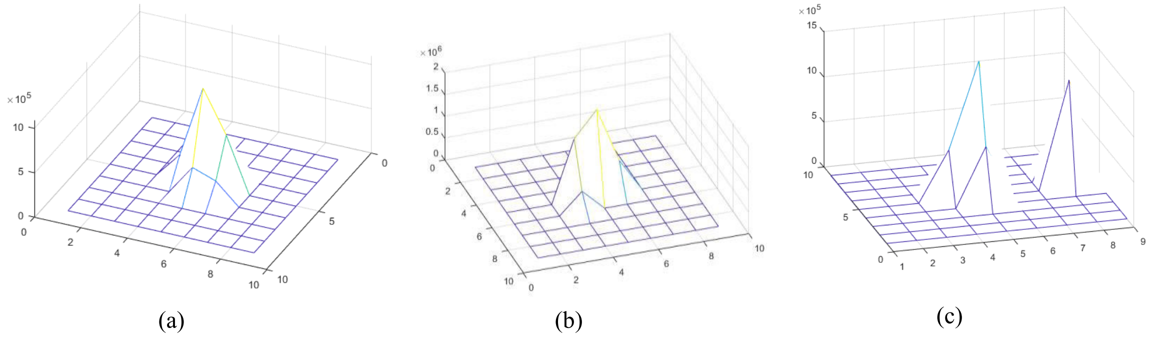

FIGURE 9. Schematic diagram of the three-dimensional peak values after matrix truncation. (a) Three-dimensional peak value of the authentic signal; (b) Three-dimensional peak value of the authentic signal containing a 0.5-chips-delay spoofing signal; (c) Three-dimensional peak value of the authentic signal containing a 1.5-chips-delay spoofing signal.

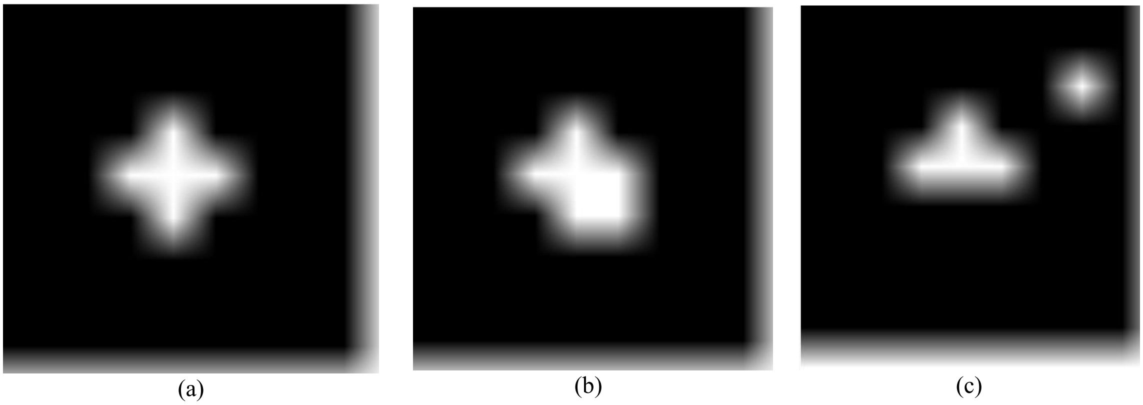

FIGURE 10. Schematic diagram of the three-dimensional peak values after matrix truncation. (a) The gray image converted from the authentic signal interception matrix; (b) The gray image converted from the interception matrix when there is a 0.5-chips-delay spoofing signal; (c) The gray image converted from the interception matrix when there is a 1.5-chips-delay spoofing signal.

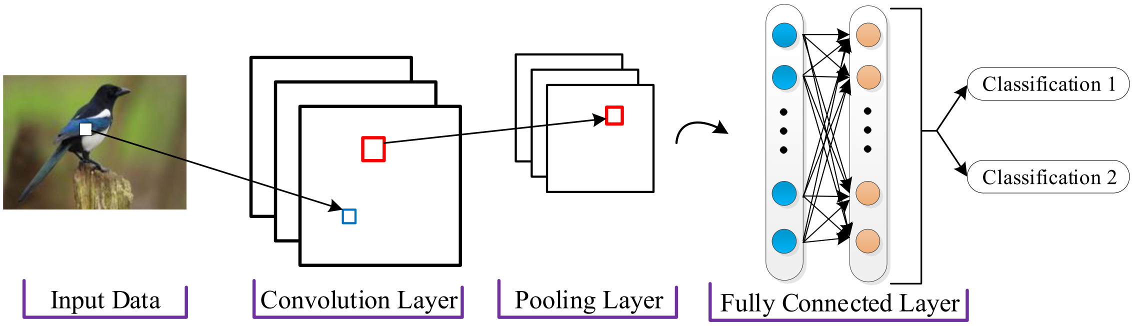

FIGURE 11. Schematic diagram of the CNN network structure.

and transform it into a gray-scale image, as shown in Fig. 10.

- **Step 5**: Use the obtained data for CNN training and classification.

C. CNN DETECTION ALGORITHM SETTING

The advantages of convolutional neural networks have widely been studied in the field of deep learning. Their main advantages become even more obvious when the network input is a multi-dimensional image so that the image can be directly used as a network input, thus avoiding complex feature extraction and data reconstruction processes necessary in the traditional recognition algorithms. Therefore, the CNN method can be used to classify data with small differences, which cannot be achieved by using traditional multi-peak detection algorithms.

CNNs are mainly trained using gradient descent and back propagation algorithms. The general CNN network structure includes the input layer, convolutional layer, excitation layer, pooling layer, and fully-connected layer, as shown in Fig. 11.

In [37], [38], the operation principles and formulas of CNNs were introduced in detail, so they are not provided in this article in detail. The function of each CNN layer is explained in the following.

1) INPUT LAYER

The input layer is the same as that in the traditional neural network/machine learning. The neural network model requires input data preprocessing for further operations. Common input-layer preprocessing includes averaging, normalization, and PCA/SVD dimensionality reduction. The data has been processed before, and it is normalized here.

2) CONVOLUTIONAL LAYER

The convolutional layer does not recognize the entire picture data simultaneously, but it is the first local perception of each feature in the picture. For a black and white image with only one layer, the convolution process can be expressed as:

$$x_i = \sum X * K_i + b_i \tag{4}$$

where x_i represents the ith feature map of the convolution layer, K_i represents the ith convolution kernel, and b_i represents the ith offset parameter. The convolutional layer can effectively extract the features of normal and spoofing signals in the image.

3) INCENTIVE LAYER

The excitation layer performs a non-linear mapping on the output result of the convolution layer using the excitation function after the convolution summation. Commonly used excitation functions include Sigmoid function, Tanh function, ReLU, Leaky ReLU, ELU, and Maxout. In this paper, the ReLU excitation function is used mainly due to its fast iteration speed, simple gradient solution formula, and absence of gradient disappearance and gradient explosion. Since the picture size considered in this work is small, and the data features are simple, the effect of using the ReLU excitation function is better. The ReLU function is expressed as follows:

$$f(x_i) = \max(0, x_i) \ . \tag{5}$$

4) POOLING LAYER

Pooling is also called subsampling or downsampling, and it is mainly used for feature dimensionality reduction, reduction of the number of data and parameters, overfitting reduction, and model's fault tolerance improvement. Polling mainly includes Maximum Pooling and Average Pooling. In this paper, Maximum Pooling is used.

5) FULLY-CONNECTED LAYER

After convolution, excitation, and pooling layers, the fully-connected layer is used, which learns high-quality features of an image. In this work, a dropout operation is added before the fully-connected layer to randomly delete some neurons in the neural network to prevent the overfitting. Then, the data of the fully-connected layer are input to the classifier to obtain the classification result. Also, the sigmoid function is used as an activation function, and it is defined as:

$$f(x) = \frac{1}{1+e^{-x}}. \tag{6}$$

It should be noted that the convolution number, excitation, and pooling parameters are different for different Doppler frequency shift search step and code phase search step in the two-dimensional search, which will be explained in the next section.

As well-know, the k-nearest neighbor (kNN) is a basic classification and regression method, and it has been commonly used in the image classification field. The main principle of the kNN is to determine the image to be recognized and to find k closest images among all training images based on a certain distance metric, and then, based on the k nearest neighbors' information, determine the most corresponding category as an output result. In this work, the kNN algorithm is used to detect spoofing signals to compare it with the detection effect of the CNN-based method.

IV. SIMULATION SETUP AND RESULTS

A. SIMULATION SETUP

In the simulations, the sampling frequency of the GNSS IF signal was set to 16.367667 MHz, the IF frequency was set to 4.123968 MHz, and the navigation message data were randomly generated. The signal-to-noise ratio of the simulated satellite navigation signal was between -15 dB and -10 dB. The simulated spoofing signal differed from the authentic signal mainly in the Doppler frequency shift, pseudo-code phase, and power. Because it is difficult to keep the spoofed signal accurately synchronized with the authentic satellite signal, in the experiment, the Doppler shift difference changed randomly within the range of ±1 kHz, and the code phase difference varied from 0 to 2 chips. The spoofing signal power was greater than the authentic signal power 1 dB–2 dB. The simulation data in the experiment included 200,000 datasets, which were divided into two categories:

- H_0: 100,000 datasets, including only the authentic satellite signal;
- H_1: 100,000 datasets, including both the authentic signal and the spoofing signal.

The H_1 data were further categorized based on the code phase difference ΔT of the spoofing signal and the authentic signal. The value of ΔT changed from zero to two chips with a step size of 0.1 chips. There were 20 categories in total, and each category consisted of 10,000 datasets. Also, 7000 datasets of various data types corresponding to H_1 were combined with 7000 datasets of H_0 data, so a total of 140,000 datasets were used for CNN training, and the remaining 60,000 datasets were used as test data.

In the simulation experiment, the Doppler frequency shift search step was 500 Hz and 250 Hz, respectively, and the code phase search step was 0.5 chip and 0.25 chip, respectively. In the situation, the relevant parameters can be changed

TABLE 1. Simulation settings.

Doppler shift search step Δf_D (Hz)	Code phase search step ΔT_{CA} (chip)	Detection matrix	CNN structure (a×b indicates window size)
500	0.5	9x9	Conv1: 2×2, pool1:4×4
	0.25	9x17	Conv1: 2×2, pool1:1×2, Conv2: 3×3, pool2:2×2
250	0.5	17x9	Conv1: 2×2, pool1:1×2, Conv2: 3×5, pool2:2×2
	0.25	17x17	Conv1: 2×2, pool1:2×2, Conv2: 3×3, pool2:2×2

according to the acquisition mode of a receiver, and in this work, only the simulation comparative analysis of our settings was conducted.

To evaluate the detection effect, different pseudo-code search steps were used so that the size of the target matrix $B_{m\times n}$ also changed. The simulation parameters are presented in Table 1.

B. SIMULATION RESULTS

The accuracy of the spoofing signal detected by the kNN classifier at different Doppler frequency shift search steps and pseudo-code phase search step conditions, when the spoofing signal deviated from the normal satellite signal by different chip amounts, is presented in Fig. 12. As displayed in Fig. 12, as the delay of the spoofing signal increased, the detection accuracy rate also increased. When the delay of the spoofing signal exceeded the value of one chip, the detection probability could reach 100% under different conditions. Thus, the greater the delay of the spoofing signal was, the easier it was to identify it. In addition, with the decrease in the Doppler frequency shift search step and pseudo-code phase search step, the detection probability increased, which conformed with the principle of the receiver's accuracy of signal acquisition; namely, the smaller the search step is, the stronger the signal acquisition capability will be. When the spoofing signal delay was small (e.g., below 0.4 chips), the detection probability of the signal was relatively low, but the overall detection probability was higher than 90%.

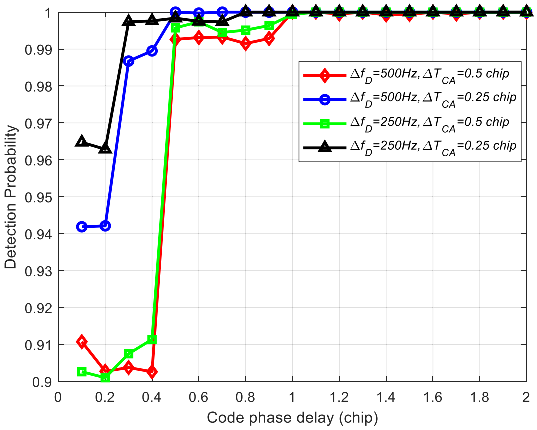

FIGURE 12. The false alarm probability of the kNN algorithm under different conditions.

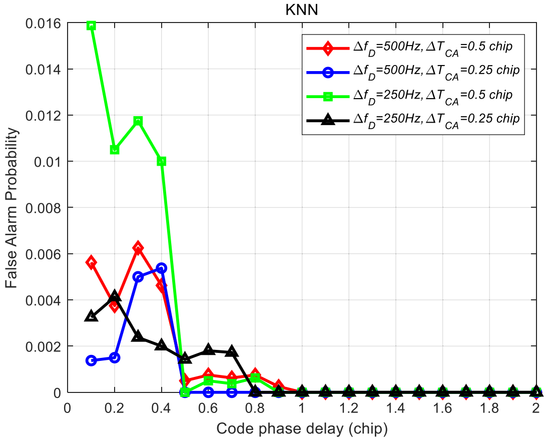

FIGURE 13. The false alarm probability of the kNN algorithm under different conditions.

The false alarm probability of the kNN algorithm under different conditions is shown in Fig. 13, where as the delay of the spoofing signal increased, the false alarm probability of the kNN algorithm gradually decreased. When the spoofing signal delay was larger than one chip, the false alarm probability was close to zero. When the spoofing signal delay was larger than 0.5 chips, the false alarm probability was below 0.002. When the spoofing signal delay was smaller than 0.5 chips, the false alarm probability was relatively poor. In Fig. 13, the false alarm probability is basically below 0.006, but the green line has a higher false alarm probability. Also, the larger the chip offset of the spoofing signal is, the lower the false alarm probability is, and the easier it is to detect spoofing interference.

The accuracy of the spoofing signal detected by the CNN classifier under different Doppler frequency shift search steps and code phase search step conditions, when the spoofing signal deviated from the normal satellite signal by a different number of chips, is presented in Fig. 14. As shown in Fig. 11, as the chip offset gradually increased, the detection probability gradually increased. When the spoofed signal was shifted from the normal satellite signal by less than 0.4 chips, the detection probability was relatively low. When the time delay of the spoofing signal was larger than 0.4 chips, the accuracy of CNN's recognition of the spoofed signal was higher than 96%, and as the Doppler frequency shift and the code phase search step decreased, the detection probability gradually increased; the detection probability even

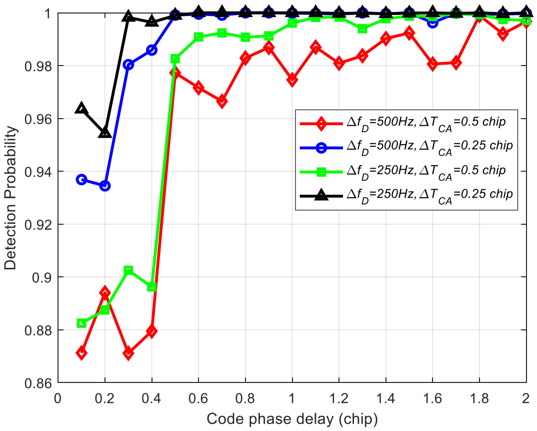

FIGURE 14. **The detection rate of the CNN algorithm under different conditions.**

reached 100% when the time delay of the spoofing signal was 0.5 chips. This result shows that when the code phase difference between the spoofing signal and the authentic signal is small, the CNN achieves poor performance in the spoofing signal recognition. This is mainly because when the chip offset is too small, the peak values of the spoofing and authentic signals almost overlap, so it is difficult to identify them. On the other hand, when the delay of the spoofing signal is small, the chip offset is directly missed due to the large step size of the code phase search. The combination of these two results in low detection probability.

The false alarm probability of the CNN algorithm under different conditions is presented in Fig. 15. As shown in Fig. 15, when the delay of the spoofing signal increased, the false alarm probability of the CNN algorithm decreased. When the spoofing signal delay was above 0.5 chips, the false alarm probability was close to zero. The false alarm probability was relatively poor when the spoofing signal delay was less than 0.5 chips, which indicated that the smaller the chip delay of the spoofing signal was, the greater the probability of false alarm was, and the larger the chip delay of the spoofing signal was, the smaller the false alarm probability and the higher the detection probability were, thus the spoofing signal was easier to detect. This result is consistent with the results in Fig. 14.

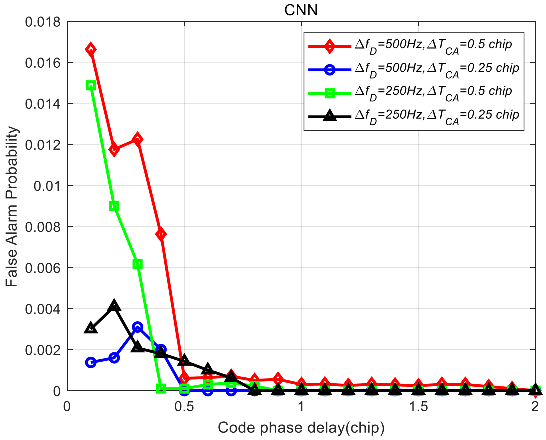

FIGURE 15. **The false alarm probability of the CNN algorithm under different conditions.**

In addition, the results presented in Figs. 12 and 14 show that the detection probability of the kNN was slightly higher than that of the CNN, but the detection probabilities of the two algorithms were very close, and their performances were relatively similar. In order to evaluate the performance of the proposed CNN-based detection methods further, the two detection methods were compared from another point of view.

The detection probabilities of the two methods at the same Doppler frequencies of the spoofing and authentic signals are given in Table 2. As presented in Table 2, at different search step values, the CNN and kNN methods had the detection probabilities of more than 96%, which demonstrated high effectiveness of both methods in the spoofing signal identification.

TABLE 2. **Detection probability of the *k* NN and CNN at the same doppler frequency.**

Doppler shift	Code phase search	Detection probability	
search step	step	CNN	kNN
(Hz)	(chip)	(%)	(%)
500	0.5	97.64	98.03
	0.25	99.27	99.34
250	0.5	97.20	96.98
	0.25	99.94	99.95

The time-consuming statistics of the CNN and kNN methods for a single dataset detection under different conditions are presented in Table 3. In Table 3, it can be seen that at the constant Doppler frequency shift search step, when the code phase search step decreased, the detection time of the CNN and kNN also increased. In addition, at the constant dimension, even when the delay time of the spoofing signal changed, the detection times of the two algorithms were similar. However, under the same conditions, the time taken by the CNN to detect a single set of data was much shorter than that of the kNN. This was mainly because the CNN could directly recognize the new data by the trained model without the need for additional training steps. In contrast, the kNN needed to calculate the distance between unknown samples and all known samples for each data classification. Besides, the larger the data dimension and the larger the data amount were, the lower the data processing efficiency of the kNN, and the higher its computational complexity were. Moreover, as the computing power of the chip increases, the detection time will continue to decrease. Thus, when the kNN

TABLE 3. **Detection probability of the *k* NN and CNN at the same doppler frequency.**

Detection model	Doppler shift	Detection time	
	step	0.25 chip	0.5 chip
	(Hz)	(ms)	(ms)
CNN	500	0.0176	0.0120
	250	0.0294	0.0193
KNN	500	2.9026	1.942
	250	3.7741	2.9241

method is used to detect and deceive signals, a compromise must be considered in terms of detection accuracy, detection time, and computational complexity. Compared with the kNN, the application of CNN algorithm is more feasible in engineering practice.

V. DISCUSSION

Since the spoofing signal is transmitted by the deceptive equipment after a series of processing, it is different from the authentic satellite signal in the path and delay, so it is difficult to achieve accurate synchronization with the authentic satellite signal, which makes it impossible for the spoofing signal to have a 0 chip delay. In addition, if there is such a special delay of 0 chip, the identification with CNN algorithm will not get good results, which requires the additional detection method of signal power to achieve.

In order to achieve the effect of deception, the power of the spoofing signal must be higher than that of the authentic satellite signal, so whether there is deception interference can be judged by the value of the peak value A^2. If A^2 is less than the threshold $\boldsymbol{\rho}_1$, the signal has not been searched; if A^2 is greater than the threshold $\boldsymbol{\rho}_1$ and greater than the threshold $\boldsymbol{\rho}_2$ meanwhile, the signal in search cell is the authentic signal; if A^2 is greater than the threshold $\boldsymbol{\rho}_2$, it is determined that the signal in search cell is a spoofing signal. Among them, $\boldsymbol{\rho}_1$ is the capture threshold and $\boldsymbol{\rho}_2$ is the maximum acquisition credible threshold. With the help of CNN detection algorithm, the detection of 0-chip delay spoofing signal can be realized.

In the future, our research will be implemented in a real software receiver system in the following ways: Firstly, in normal environment and environment with deception, a large number of two-dimensional search matrix data including authentic signals and spoofing signals are collected respectively in the receiver. Secondly, the target data set is obtained by processing the obtained data, which is trained to obtain the training model. Finally, the trained model is embedded into the receiver software system to detect deception signals. According to this method, our subsequent work will be implemented in a real software receiver system to verify its detection performance.

VI. CONCLUSION

This paper studies the detection of a small-delay spoofing signal in the acquisition phase based on deep learning. Through the analysis of the signal model and principles of the GNSS system in the acquisition stage and the two-dimensional search matrix processing in the acquisition stage, the spoofing signal recognition in the GNSS system is respectively realized by the kNN and CNN methods. The experimental results show that both methods achieve better detection effect when the code phase shift between the spoofing and authentic signals is equal to or larger than 0.5 chips. The validity of the proposed CNN-based detection method is verified by the experiment and simulation. In the case of a small-delay spoofing signal, the accuracy of the kNN is slightly higher than that of the CNN, but on the whole, the detection results of the two algorithms are relatively similar. However, the kNN has higher complexity, so the CNN method can be considered as more suitable for engineering applications.

The experimental results show that when the spoofing signal delay is small, the detection probabilities of the kNN and CNN are low, while the probabilities of false alarm are high. This is mainly because the correlation peak of a small-delay spoofing signal is relatively close to the correlation peak of the authentic signal, and the correlation peak of the real signal is even superimposed on all of them. When either CNN or kNN method is used for spoofing signal detection, the characteristic of the peak number in the image is not obvious, so an effective spoofing signal identification is impossible.

It should be noted that the proposed CNN-based spoofing signal detection method is in the phase of theoretical analysis and research, and the actual testing and verification in the software receiver system will be part of our future work.

REFERENCES

[1] 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, 2016.

[2] F. Wang, H. Li, and M. Lu, "GNSS spoofing countermeasure with a single rotating antenna," *IEEE Access*, vol. 5, pp. 8039–8047, 2017.

[3] Y. Wang, J.-M. Hao, W.-P. Liu, and X. Wang, "Dynamic evaluation of GNSS spoofing and jamming efficacy based on game theory," *IEEE Access*, vol. 8, pp. 13845–13857, 2020.

[4] S. Han, L. Chen, W. Meng, and C. Li, "Improve the security of GNSS receivers through spoofing mitigation," *IEEE Access*, vol. 5, pp. 21057–21069, 2017.

[5] A. Broumandan and G. Lachapelle, "Spoofing detection using GNSS/INS/Odometer coupling for vehicular navigation," *Sensors*, vol. 18, no. 5, p. 1305, Apr. 2018.

[6] Y. Montgomery, E. Humphreys, M, Ledvina, "Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer," in *Proc. Int. Tech. Meeting Inst. Navigat.*, 2009, pp. 124–130.

[7] E. Axell, E. G. Larsson, and D. Persson, "GNSS spoofing detection using multiple mobile COTS receivers," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Apr. 2015, pp. 3192–3196.

[8] L. A. Dobryakova, L. S. Lemieszewski, and E. F. Ochin, "GNSS spoofing detection using static or rotating single-antenna of a static or moving victim," *IEEE Access*, vol. 6, pp. 79074–79081, 2018.

[9] Y. Liu, S. Li, Q. Fu, and Z. Liu, "Impact assessment of GNSS spoofing attacks on INS/GNSS integrated navigation system," *Sensors*, vol. 18, no. 5, pp. 1433–1445, 2018.

[10] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proc. IEEE*, vol. 104, no. 6, pp. 1258–1270, Jun. 2016.

[11] 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.

[12] Y. Gao, Z. Lv, and L. Zhang, "Two-step trajectory spoofing algorithm for loosely coupled GNSS/IMU and NIS sequence detection," *IEEE Access*, vol. 7, pp. 96359–96371, 2019.

[13] J. Zidan, E. Adegoke, E. Kampert, S. Birrell, C. Ford, and M. Higgins, "GNSS vulnerabilities and existing solutions: A review of the literature," *IEEE Access*, early access, Feb. 13, 2020.

[14] A. Rawnsley. *Iran's Alleged Drone Hack: Tough, But Possible*. Accessed: Dec. 2011. [Online]. Available: http://www.wired.com/dangerroom/2011/12/iran-drone-hack-gps

[15] 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. IEEE/ION Position, Location Navigat. Symp. (PLANS)*, Monterey, CA, USA, May 2014, pp. 1240–1247.

[16] J. Bhatti and T. E. Humphreys, "Hostile control of ships via false GPS signals: Demonstration and detection," *Navigation*, vol. 64, no. 1, pp. 51–66, Mar. 2017.

[17] F. Wang, H. Li, and M. Lu, "GNSS spoofing detection and mitigation based on maximum likelihood estimation," *Sensors*, vol. 17, no. 7, pp. 1532–1547, 2017.

[18] W. Hanlon, L. Psiaki, and E. Humphreys, "Real-time spoofing detection using correlation between two civil GPS receiver," in *Proc. 25th Int. Tech. Meeting Satell. Division Inst. Navigat. (ION GNSS)*, 2001, pp. 3584–3590.

[19] V. Dehghanian, J. Nielsen, and G. Lachapelle, "GNSS spoofing detection based on receiver C/N$_0$ estimates," in *Proc. ION GNSS Meeting*, Nashville, TN, USA, Sep. 2012, pp. 2878–2884.

[20] C. Sun, J. W. Cheong, A. G. Dempster, H. Zhao, and W. Feng, "GNSS spoofing detection by means of signal quality monitoring (SQM) metric combinations," *IEEE Access*, vol. 6, pp. 66428–66441, 2018.

[21] A. Jahromi, A. Broumandan, and J. Nielsen, "GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N$_0$ measurements," *Int. J. Satell. Commun. Netw.*, vol. 30, no. 4, pp. 181–191, 2012.

[22] M. Troglia Gamba, M. D. Truong, B. Motella, E. Falletti, and T. H. Ta, "Hypothesis testing methods to detect spoofing attacks: A test against the TEXBAT datasets," *GPS Solutions*, vol. 21, no. 2, pp. 577–589, Apr. 2017.

[23] P. Mark, T. Humphreys, and S. Brian, "Attackers can spoof navigation signals without our knowledge. Here's how to fight back GPS lies," *IEEE Spectr.*, vol. 53, no. 8, pp. 26–53, Aug. 2016.

[24] Y. Montgomery, E. Humphreys, and M. Ledvina, "A multi-antenna defense: Receiver-autonomous GPS spoofing detection," *Inside GNSS*, vol. 4, no. 2, pp. 40–46, 2009.

[25] M. Akos, "Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC)," *Navigation*, vol. 59, no. 4, pp. 281–290, 2012.

[26] H. Borowski, O. Isoz, and M. Eklof, "Detecting false signals with automatic gain control," *GPS World*, vol. 23, no. 4, pp. 38–43, 2015.

[27] S. Cho, S. Mi, S. Lim, D. Hwang, S. Lee, and C. Park, "Design of a TOA-based anti-spoofing method for GPS civil signal," in *Proc. ION GNSS PNT Symp.*, Savannah, GA, USA, Sep. 2008.

[28] J. Tu, X. Zhan, X. Zhang, Z. Zhang, and S. Jing, "Low-complexity GNSS anti-spoofing technique based on Doppler frequency difference monitoring," *IET Radar, Sonar Navigat.*, vol. 12, no. 9, pp. 1058–1065, Sep. 2018.

[29] K. Liu, W. Wu, Z. Wu, and L. He, "Spoofing detection algorithm based on pseudorange differences," *Sensors*, vol. 18, no. 10, pp. 3197–3210, 2018.

[30] G. Fan, X. Gan, B. Yu, Q. Rong, and C. Sheng, "Adaptive spoofing suppression algorithm for GNSS based on multiple antennas array," *Sensors*, vol. 20, no. 4, p. 1115, Feb. 2020.

[31] R. Xu, M. Ding, and Y. Qi, "Performance analysis of GNSS/INS loosely coupled integration systems under spoofing attacks," *Sensors*, vol. 18, no. 12, pp. 4108–4192, 2018.

[32] C. James, B, Ali, "On the use of low-cost IMUs for GNSS spoofing detection in vehicular applications," in *Proc. Int. Tech. Symp. Navigat. Timing (ITSNT)*, Toulouse, France, 2017, pp. 1–8.

[33] C. Tanil, S. Khanafseh, M. Joerger, and B. Pervan, "Kalman filter-based INS monitor to detect GNSS spoofers capable of tracking aircraft position," in *Proc. IEEE/ION Position, Location Navigat. Symp. (PLANS)*, Apr. 2016, pp. 1027–1034.

[34] W. Wang, N. Li, R. Wu, and C. Pau, "Detection of induced GNSS spoofing using S-curve-bias," *Sensors*, vol. 19, no. 4, pp. 922–934, 2019.

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

[36] E. Humphreys, M. Ledvina, and L. Psiaki, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proc. 21st Int. Tech. Meeting Satell. Division Inst. Navigat.*, 2008, pp. 2314–2325.

[37] K. O'Shea and R. Nash, "An introduction to convolutional neural networks," *Neural Evol. Comput.*, 2015. [Online]. Available: https://arxiv.org/abs/1511.08458

[38] N. Guberman, "On complex valued convolutional neural networks," *Comput. Sci.*, 2016. [Online]. Available: https://arxiv.org/abs/1602.09046

JUNZHI LI received the master's degree in communication engineering from Yunnan Minzu University, China, in 2018. He is currently pursuing the Ph.D. degree in communication engineering with the College of Electronics and Communication Engineering, Sun Yat-sen University, China.

His current research interests include global navigation satellite system signal acquisition and tracking and GNSS spoofing and anti-spoofing technology.

XIANGWEI ZHU received the M.S. degree in communication engineering, in 2003, and the Ph.D. degree in information and communication engineering from the College of Electronic Science and Engineering, National University of Defense Technology, Changsha, China, in 2007.

He is currently a Professor with the College of Electronics and Communication Engineering, Sun Yat-sen University. His current research interests include global navigation satellite systems, time synchronization, intelligent signal processing, and instrument design.

MINGJUN OUYANG received the master's degree from the University of Chinese Academy of Sciences, in 2018. He is currently pursuing the Ph.D. degree in communication engineering with the College of Electronics and Communication Engineering, Sun Yat-sen University, China.

He has served as a GNSS Algorithm Engineer with Hi-Target Surveying and Mapping Instrument, from 2018 to 2019. His current research interests include GNSS precise positioning, GNSS precise time and frequency transfer, GNSS fusion inertial navigation algorithm, and software development.

WANQING LI received the B.S. degree in electronic information engineering from the Guilin University of Electronic Technology, Guilin, China, in 2018. She is currently pursuing the master's degree in information and communication engineering with Sun Yat-sen University, Guangzhou, China.

Her research interests include satellite navigation and the reliability and accuracy of low-cost positioning.

ZHENGKUN CHEN received the B.S. degree in surveying engineering from Central South University, Changsha, China, in 2013, and the M.S. degree in electronics and communication engineering from the National University of Defense Technology, Changsha, in 2015. He is currently pursuing the Ph.D. degree in information and communication engineering with Sun Yat-sen University, Guangzhou, China.

His research interests include high-precision and high-integrity of comprehensive positioning, navigation, and timing (PNT).

ZHIQIANG DAI received the B.S. degree from the School of Geodesy and Geomatics, Wuhan University, China, in 2009, the M.S. degree from the Shanghai Astronomical Observatory, Chinese Academy of Sciences, in 2012, and the Ph.D. degree from the School of Geodesy and Geomatics, Wuhan University, in 2016.

From 2017 to 2019, he worked as a Postdoctoral Researcher with Hi-Target Surveying Instrument Company Ltd., and Wuhan University. He is currently an Assistant Professor with the School of Electronics and Communication Engineering, Sun Yat-sen University. He is mainly involved in the theory of GNSS/SBAS precise data processing, real-time PPP, multi-sensor navigation data fusion, and the algorithm and software development.