Satellite Spoofing Identification Method Based on Radio Frequency Feature Extraction

Yu Jiang and Yuexiu Xing
School of Cyberspace Security, Southeast University, Nanjing, 210096, China.
Email: jiangyu@seu.edu.cn

Abstract. The interference and spoofing for satellite navigation systems pose great challenges to the safety of satellite communications. Radio fingerprint based physical layer security technique is an effective approach to solve these problems. According to the characteristics of satellite communication, this paper presents a spatial radio fingerprint extraction method based on constellation figure. The K-mean clustering algorithm is adopted to extract the radio fingerprint features related to the spatial distribution characteristics of satellites from constellation figure to identify the spoofing signals. From theoretical analysis, the spatial RF fingerprint features are extracted from the actual satellite signal and the spoofing identification is achieved based on the forged signals generated by the universal software radio peripheral (USRP) to verify the validity and practicality of the proposed method. The proposed method can identify spoofing targets without demodulating the satellite signal and can be used alone or in combination with existing spoofing target identification methods to increase the recognition rate.

1. Introduction
The global navigation satellite system (GNSS) receives satellite signals on the ground and in the air all day long to provide position, velocity and time (PVT) services. World powers are developing their own satellite navigation systems, the United States’ global positioning system (GPS), Galileo in Europe, the BDS (BeiDou navigation satellite system) in China, and the GLONASS (global navigation satellite system) in Russia. These systems have promoted the rapid development of navigation system.

GNSS plays a major role in everyday life and it has brought tremendous changes in numerous application fields. The current positioning and time service has been widely used in many areas. However, while GNSS is widely used, its vulnerability has gradually emerged. The interference seriously threatens the satellite navigation system which is particularly vulnerable to spoofing attacks compared to other types of interference.

The existing anti-interference techniques can be divided into three categories [1-2]. The first category is signal encryption and authentication technology which uses modern cryptography to improve security. This technology is equivalent to adding a secure transmission protocol to the original satellite communication system and it involves the transformation of the original system [3-4]. The second is signal feature detection technology with many research results, and the proposed method belongs to this category. Dehghanian et al. [5] developed a multiple spoofing detection technique based on signal power measurement under various multipath conditions. Jafarnia et al. [6] proposed a spoofing detection method by monitoring the unreasonable changing of the clock state. Psiaki et al. [7] developed a dual-antenna spoofing detection algorithm based on differential carrier phase. Lim et al. [8] proposed a method to determine the spoofing signal by detecting the correlation distortion of C/A code in the GPS L1 band. The third category is auxiliary information detection
technology [9] which relies on the existence of auxiliary information and the application scenario of the terminal.

This paper proposes a satellite spoofing interference identification method based on RF feature extraction, which belongs to the signal feature detection technology. Different from the existing methods, we extract the spatial RF fingerprint characteristics through the constellation figure of satellite signals and the RF fingerprint characteristics can be used to identify the spoofing signals. Finally, the RF fingerprint characteristics are extracted from the constellation figure from actual satellite signal measurement to verify the performance of the proposed method, and further work are given according to the experimental results.

2. System Model

The navigation message is represented by the data code \( D(t) \) with code rate of 50 b/s. PRN codes is modulated with \( D(t) \) and the L1 band carrier is modulated with the combination code to form a transmitting signal for users. \( D(t) \) is added to the C/A code and the P code to form the combination codes of \( C(t)D(t) \) and \( P(t)D(t) \), where C/A code and P code are denoted by \( C(t) \) and \( P(t) \) respectively. \( C(t)D(t) \) and \( P(t)D(t) \) are orthogonal on L1 carrier, so the orthogonal relationship between \( C(t)D(t) \) and \( P(t)D(t) \) can be used to construct the signal constellation on the L1 carrier.

In order to obtain an effective constellation figure, the signal must be despread to increase the signal to noise ratio (SNR). Since the C/A code is known, \( C(t)D(t) \) can be despread to obtain \( D(t) \). However, the P code is unknown, so \( P(t)D(t) \) cannot be directly despread to obtain \( D(t) \). Unfortunately, even if the P code is known, the despreaded results of C/A code and P code is the same data code \( D(t) \). Therefore, the constellation figure still cannot be constructed.

Since the constellation figure cannot be established with a single satellite signal, we consider using signals from multiple satellites to create the constellation figure. This idea is mainly based on the following two considerations. The first is that satellite receivers can usually receive multiple satellite signals at the same time and the second is that the constellation figure is established by multiple satellite signals for satellite spoofing identification, which is different from the conventional constellation figure for data decision in communication demodulation.

3. Constellation Figure

3.1. Signal Processing

Firstly, the signal \( s(t) \) emitted by the satellite is shown in equation (1):

\[
s(t) = P_s \cdot C(t - \tau) \cdot D(t - \tau) \cdot \cos(\omega_1 t + \phi_1) + n(t),
\]

where \( P_s \) is the signal power of satellite, \( C(t) \) is the C/A code, \( D(t) \) is the navigation data code, \( \tau \) is the signal transmission delay, \( \omega_1 \) is the carrier frequency of transmitting signal, \( \phi_1 \) is the initial phase of the transmitting signal and \( n(t) \) is white noise which power spectral density value is considered as a constant.

Then, the local carrier \( L(t) \) generated at the receiver is shown in equation (2):

\[
L(t) = \cos(\omega_2 t + \phi_2),
\]

where \( \omega_2 \) is local carrier frequency of receiver, \( \phi_2 \) is the initial phase of local carrier. After multiplying the received signal with the local carrier, the output signal as shown in equation (3) is obtained through the low-pass filter.

\[
s_c(t) = P_s \cdot C(t - \tau) \cdot D(t - \tau) \cdot \cos((\omega_1 - \omega_2) t + (\phi_1 - \phi_2)) + n'(t)
\]

where \( n'(t) \) is still the white noise with the bandwidth of low-pass filter, the frequency difference \( \Delta \omega = \omega_1 - \omega_2 \) and the phase difference \( \Delta \phi = \phi_1 - \phi_2 \).
Assume that the PRN code generated by the local code generator is represented as $C(t - \tau)$, where $\tau$ is the delay of local PRN code. Without considering the noise, the correlation and integration result of local PRN code and the received signal is shown as

$$s_o(\tau) = \int_0^{T_s} P_s(t) \cdot C(t - \tau) \cdot D(t - \tau) \cdot \cos(\Delta \omega t + \Delta \phi) dt,$$

where $T_s$ is the integration time. We choose $T_s < 20\text{ms}$ to make $D(t)$ a constant.

When the receiver tracks the satellite signal stably, $\Delta \omega$ is close to 0. Therefore, during the signal processing, it can be considered that $\Delta \omega = 0$. We take $\Delta \tau = \tau - \tau'$, so

$$s_o(\Delta \tau) = P_s \cdot D(t_0) \cdot \cos(\Delta \phi) \cdot \int_0^{T_s} C(t - \tau) \cdot C(t - \tau') dt.$$

Then, we make

$$R(\Delta \tau) = \int_0^{T_s} C(t - \tau) \cdot C(t - \tau') dt.$$

and get

$$s_o(\Delta \tau) = P_s \cdot D(t_0) \cdot \cos(\Delta \phi) \cdot R(\Delta \tau).$$

For the noise part,

$$N_o(\tau') = \int_0^{T_s} C(t - \tau') \cdot n(t) dt.$$

Due to the randomness of noise and the shifting cyclicity of C/A code, $N_o(\tau') = N_o$. The final output signal is shown in equation (9) as

$$s_o(\Delta \tau) = P_s \cdot D(t_0) \cdot \cos(\Delta \phi) \cdot R(\Delta \tau) + N_o.$$  

According to equation (9), the output of the integrator reaches the maximum value when the phase of local PRN code coincides with that of the input signal.

In the normal progress of satellite signal processing, subsequent process is performed after the sampling judgement of correlation results. In our proposed method, drawing the constellation figure does not require subsequent signal processing. Instead, the correlation result of each satellite signal before the judgment is used as the coordinates of the constellation figure. The correlation results before the judgment reflect the energy distribution characteristics of the satellite signals and can be represented by the constellation figure.

### 3.2. Acquisition of Constellation Figure

In digital communication, the receiver obtains the baseband signal with the same frequency and phase as the transmitter and then the sample point for decision is obtained through time synchronization. The above processed digital signals are drawn on the complex plane as a constellation figure which is a kind of map for linear modulation and can represent the relationship between signals visually. The constellation figure provides a convenient way for studying the performance of receivers in digital communication system and the relationship between I/Q signals. Without considering the noise, we set up the constellation figure with two different satellite data codes, as shown in Figure 1.
Figure 1. Constellation figure of satellite signals.

The purpose of acquiring the constellation figure is usually to study the performance of demodulation, the bit error rate, etc., so only the sampling points for decision are drawn generally. As mentioned above, in order to study the constellation figure of satellite signals, unlike the traditional way of obtaining constellation points, we use signals from multiple satellites to build constellation figure.

We use MATLAB to produce 7 satellite signals denoted by $s_i (i = 1, \ldots, 7)$. The correlation results of $s_i$ are taken as the x axis coordinate of the constellation figure and those of the other 6 satellite signals $s_j (i = 2, \ldots, 7)$ are taken as the y axis coordinate of the constellation figure. The data are processed according to the algorithm flow of Section 3.1 to obtain the constellation figure of satellite signals, which is shown in Figure 2.

Figure 2. Constellation figure of simulated signals.
4. Experimental Results and Analysis

4.1. Experimental Setup
The experimental system consists of the Universal Software Radio Platform (USRP) [10], the front-end RF module and the computer. Due to the insufficient receiving gain of USRP, a customized front-end RF module is used to increase the received signal strength and it outputs a intermediate frequency (IF) of 46.42MHz. The computer is equipped with Intel Core i7-4790 processor and its operating system is Ubuntu 14.04 with open source software of radio platform and Matlab. The satellite signals are collected and processed through the front-end receiving module and USRP and then sent to the computer by ethernet to extract spatial RF fingerprint feature and recognize the spoofing signal. The front-end equipment of experimental system is shown in Figure 3.

![Figure 3](image)

Figure 3. The front-end equipment of experimental system.

We firstly use Motorola's M12M platform [11] to determine the quantity and numbering of satellites in current space. In our observation, there are 7 satellites that can actually be tracked and their numbering is shown in Figure 4.

![Figure 4](image)

Figure 4. The tracked satellite data.

4.2. Spatial RF Feature Extraction
The spatial RF feature of satellite signals can not only be directly obtained by the correlation calculation among different constellation figures to obtain the differences among the various distributions of constellation points, but also be obtained through the visible processing. In comparison,
visible processing is more convenient and intuitive than direct correlation calculation, and the image obtained through visible processing of the constellation figure is shown in Figure 5.

![Figure 5. Visible processed constellation figure.](image)

As shown in Figure 5, the intensity distribution of the constellation points can be expressed by the change of colors. The red regions indicate that the distribution of constellation points is dense. The distribution can be considered as a unique spatial RF feature formed by the satellite signals. After the receiving of normal signals for a period of time, a stable spatial RF fingerprint will be formed. As long as the continuous receiving of normal signals is guaranteed, there will be differences in spatial RF fingerprint upon the appearance of spoofing signals. Visible processing and pattern recognition can be applied to feature extraction to determine whether there are spoofing signals. A method of visible processing for constellation figures and the spoofing signal recognition will be introduced next.

4.3. Clustering

Features of constellation figure in Figure 5 can be found by clustering the densely distributed points and the K-means algorithm [12] is chosen as the clustering algorithm to cluster the densely distributed points to form different cluster centers. Due to the differences of signal strength, several different cluster centers will be obtained, reflecting the spatial RF fingerprint characteristics. By analyzing the changes of the coordinates of the cluster centers in different time periods, it can be determined whether there is a spoofing signal. The specific method for feature extraction and spoofing recognition based on the constellation figure is as follows.

Firstly, the constellation figure is divided into \( N \times N \) regions to generate a matrix of \( N \times N \). Then, the density of constellation points is calculated by counting the number of points in each region. When the density is greater than the preset threshold \( \alpha \), the corresponding element of the matrix is set to 1 and otherwise 0. After all the constellation points are counted, the K-means clustering method is performed on the element with value 1 in the matrix to get \( P \) cluster centers \( C_p \), where \( p = 1, 2, \ldots, P \) and \( j \) denotes the counting time period. Then, the Euclidean distances between \( C_p \) and \( C_p' \), the cluster centers for the new time period \( j \) is calculated as shown in equation (10).

\[
D_j = \sum_{p=1}^{P} d(C_p, C_p'),
\]

where \( d \) is the calculation of Euclidean distance.

Finally, the system can determine whether there is a spoofing signal by analyzing the result of \( D_j \) and the determination threshold will be determined by the training data in practical applications,
After visible processing and clustering of the normal signals, 6 clusters are obtained through the constellation figure and the clustering results are shown in Figure 6.

![Figure 6. Clustering results of normal signals.](image)

As shown in the figure, the dense points in the constellation figure are divided into 6 clusters successfully. Firstly, the normal satellite signals in the current space are trained for a period of time to acquire the corresponding spatial RF fingerprint features and then another USRP with the github's open source GPS emulation code gps-sdr-sim [13] is started to generate the spoofing signals. After a period of running and signal acquisition, the results of the clusters are shown in Figure 7. As seen from the figure, the right-side cluster marked with black dot in Figure 7 is clearly different from the clusters in Figure 6 and it's a new cluster due to the spoofing signal. Therefore, it is easy to find the abnormal signals from the comparison of the clustering results. Furthermore, the Euclidean distance between the two figures can be calculated by equation (10). By comparing with the spatial RF fingerprint feature of normal state, we can determine whether there is a spoofing signal. From the experimental results, we can see that the RF fingerprint feature extraction method based on the constellation figure can identify the spoofing satellite signal efficiently.

![Figure 7. Clustering results of spoofing signals.](image)
5. Conclusion
This paper introduces a spatial RF fingerprint extraction method based on constellation figure, which belongs to the signal feature detection technology. The method of generating constellation figure and getting intuitive spatial RF fingerprint features is described in detail. Based on the obtained constellation figure, a method of spatial RF feature extraction and spoofing satellite signal recognition by K-means clustering is proposed. Through the experiments of feature extraction and spoofing recognition of satellite signals tracked in real space, the validity and practicability of the proposed method based on constellation figure are verified. The following work will mainly focus on how to design a classifier based on visible processing methods to extract and recognize signal feature.

6. Acknowledgments
This work was supported in part by a grant from National Natural Science Foundation of China (Grant No. 61601114, No. 61602113, No. 61571110) and State Key Laboratory of Satellite Navigation System and Equipment Technology Open Fund Project of China under Project No. EX166840046.

7. References
[1] Wang, F., Li, H., & Lu, M. (2017). GNSS Spoofing Detection and Mitigation Based on Maximum Likelihood Estimation. Sensors, 17(7), 1532.
[2] Broumandan, A., Jafarnia-Jahromi, A., Dehghanian, V., Nielsen, J., & Lachapelle, G. (2012, April). GNSS spoofing detection in handheld receivers based on signal spatial correlation. In Position Location and Navigation Symposium (PLANS), 2012 IEEE/ION (pp. 479-487). IEEE.
[3] Caparra, G., Ceccato, S., Sturaro, S., & Laurenti, N. (2017, May). A key management architecture for GNSS open service Navigation Message Authentication. In Navigation Conference (ENC), 2017 European (pp. 287-297). IEEE.
[4] Margaria, D., Motella, B., Anghileri, M., Floch, J. J., Fernandez-Hernandez, I., & Paonni, M. (2017). Signal Structure-Based Authentication for Civil GNSSs: Recent Solutions and Perspectives. IEEE Signal Processing Magazine, 34(5), 27-37.
[5] Dehghanian, V., Nielsen, J., & Lachapelle, G. (2012). GNSS spoofing detection based on signal power measurements: statistical analysis. International Journal of Navigation and Observation, 2012, 313527.
[6] Jafarnia-Jahromi, A., Daneshmand, S., Broumandan, A., Nielsen, J., & Lachapelle, G. (2013, April). PVT solution authentication based on monitoring the clock state for a moving GNSS receiver. In European navigation conference (ENC) (pp. 11).
[7] Psiaki, M. L., Powell, S. P., & O’Hanlon, B. W. (2013). GNSS spoofing detection: Correlating carrier phase with rapid antenna motion. GPS World, 24(6), 53-58.
[8] Lim, S., Lim, D. W., Chun, S., Heo, M. B., Choi, Y. S., Lee, J. H., & Lee, S. J. (2015). Design and Performance Evaluation of GPS Spoofing Signal Detection Algorithm at RF Spoofing Simulation Environment. Journal of Positioning, Navigation, and Timing, 4(4), 173-180.
[9] Lee, J. H., Kwon, K. C., An, D. S., & Shim, D. S. (2015). GPS spoofing detection using accelerometers and performance analysis with probability of detection. International Journal of Control, Automation and Systems, 13(4), 951-959.
[10] http://www.ettus.com/, online available 2018-3-1.
[11] http://www.ilotus.com.sg/m12m_timing_oncore/, online available 2018-3-1.
[12] Ripley, B. D. (2007). Pattern recognition and neural networks. Cambridge university press.
[13] https://github.com/osqzss/gps-sdr-sim, online available 2018-3-1.