



Passive Location for 5G OFDM Radiation Sources Based on Virtual Synthetic Aperture

Tong Zhang, Xin Zhang and Qiang Yang *

School of Electronics and Information Engineering, Harbin Institute of Technology, Harbin 150001, China

* Correspondence: yq@hit.edu.cn

Abstract: Passive location technology has been greatly developed because of its low power consumption, long detection distance, good concealment, and strong anti-interference ability. Orthogonal frequency-division multiplexing (OFDM) is an efficient multi-carrier transmission technology, which is an important signal form of 5G communication. Researching passive locations for OFDM signals can realize the location of base stations, which is of great significance in the military. Space-borne passive location technology has a contradiction between wide coverage and high precision. Therefore, a single-satellite passive location algorithm for OFDM radiation sources based on the virtual synthetic aperture is proposed. The algorithm introduces virtual synthetic aperture technology, using antenna movement to accumulate data coherently over a long time period and synthesizing a long azimuth virtual aperture. In addition, it utilizes fast Fourier transform (FFT) to extract phase information at a specific frequency based on the multi-carrier modulation technology of the OFDM signal. Pilot technology of the communication system is used for phase compensation and noise reduction. Thus, the azimuth linear frequency modulation (LFM) signal containing the location information of the radiation source is obtained. The radiation source location can be obtained by range searching and azimuth focusing. Simulation results verify the effectiveness of the algorithm and show that the algorithm can realize high-precision and wide-coverage location for the OFDM radiation sources using a single antenna, turning the hardware structure into software to reduce the cost and complexity of the system.

Keywords: OFDM signal; passive location; virtual synthetic aperture; data coherent accumulation



Citation: Zhang, T.; Zhang, X.; Yang, Q. Passive Location for 5G OFDM Radiation Sources Based on Virtual Synthetic Aperture. *Remote Sens.* **2023**, *15*, 1695. <https://doi.org/10.3390/rs15061695>

Academic Editor: Stefano Tebaldini

Received: 20 January 2023

Revised: 10 March 2023

Accepted: 20 March 2023

Published: 21 March 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Passive location technology has been constantly developing in the past decades [1]. Electronic reconnaissance is an important means to obtain battlefield electronic intelligence. Its main task is to monitor and intercept electromagnetic wave signals radiated by enemy military equipment (such as radar, radio communication, navigation and guidance, etc.) and obtain their technical parameters, communication content, location and other information. Thus, radiation source location by a single satellite plays an important role in electronic reconnaissance with the advantages of low power consumption, long detection distance, good concealment, and strong anti-interference ability [2].

With the development of 5G construction, the realization of satellite–Earth interconnection and the integration of communication, navigation and remote sensing is the current development hotspot. In addition, satellite communication is being vigorously developed to realize global communication without the limit of altitude and region. Therefore, realizing 5G radiation source location can not only shield, interfere and attack enemy ground base stations and satellite communication users, but can also realize the accurate location of its own satellite communication users to provide better user services, which has important military, civil and commercial value.

The methods of passive location by single satellite commonly use location parameters of direction of arrival (DOA) or change rate of Doppler frequency. DOA is usually

measured by phase interferometer or antenna array. For phase interferometer systems, the problem is that a long baseline can obtain highly accurate location information but causes phase ambiguity, which needs complex antenna structures to solve [3,4]. For antenna array systems, a long array can reach high accuracy but is limited in a moving platform [5]. Antenna array DOA estimation algorithms include conventional beamformer (CBF), multiple signal classification (MUSIC), and maximum likelihood estimator (MLE) [6]. With the development of neural networks, the DOA estimation method based on deep learning has been widely applied, which can reduce computational complexity [7]. DOA estimation with a traditional scalar sensor requires complex antenna structures, so an electromagnetic vector sensor (EMVS) array is used instead of a scalar sensor array for two-dimensional DOA estimation, which has high estimation accuracy. In addition, DOA estimation with an EMVS array is insensitive to sensor position, which makes EMVS more flexible than traditional scalar sensor arrays [8,9].

The Doppler location systems measure the Doppler change rates of the same radiation source by the satellite at different locations and obtain the radiation source location by combining the position information of the satellite platform at each moment [10–13]. Compared with the DOA method, the Doppler system has a simpler structure but needs a long time to measure the Doppler information from many positions, and the location accuracy is affected by the Doppler measurement accuracy. Long-time sampling data are needed to measure the instantaneous Doppler information, but causes the change of Doppler.

Multi-satellite passive location systems have high location accuracy. Their most widely used location methods are time difference of arrival (TDOA), frequency difference of arrival (FDOA), and the joint location method, which has high location accuracy [14–16]. Other location information can also be combined to obtain high-accuracy source location, such as combining TDOA, FDOA and differential Doppler rate (DDR) [17], or time of arrival (TOA) and TDOA [18], etc. However, issues such as time synchronization need to be considered, which result in high system complexity and cost. In contrast, although single-satellite passive location systems are not accurate enough, they are widely used because of their low cost and simple system setup.

Orthogonal frequency-division multiplexing (OFDM) is an efficient multi-carrier transmission technology, which first appeared in the field of digital communication. The OFDM multi-carrier signal has the advantages of flexibility, large bandwidth, and good orthogonal characteristics, which are an important signal form of 5G communication. In addition to the universal passive localization method, there are several passive location methods specific to OFDM signals. Reference [19] proposes a DPD method based on the MLE for OFDM signals, and Reference [20] derives the least squares estimator (LSE) algorithm. Reference [21] constructs an optimization model based on the maximum likelihood estimator and the multi-carrier technology of OFDM signals and proposes a DPD method based on the spectrum. The DPD methods for OFDM signals have the same difficulty as the DPD methods for other signals.

Article [22] introduced the long synthetic aperture technology into direct location. Article [23] analyzes the range resolution, azimuth resolution, and sensitivity of the algorithm. Compared with other passive location algorithms, the difference is that the range and azimuth distance between the radiation source and the satellite is used to replace the description of the location of the radiation source which can obtain the analytic solution of the radiation source, and the coherent accumulation of long-term data is used to obtain the high-precision location. However, the articles only introduce the algorithm for simple signal forms like the single-frequency signal or simple modulated single-frequency signal.

On this basis, this paper proposes a passive location method based on a virtual synthetic aperture for OFDM signals, which uses long-term coherent data to synthesize a large virtual antenna azimuth aperture to improve the location precision. The paper utilizes the multi-carrier modulation technology of OFDM signals and the pilot technology of the communication systems to extract carrier phase information and compensate phase, obtaining the carrier Doppler signal in the form of linear frequency modulation (LFM)

signal. The range and azimuth location of the radiation source can be obtained by range searching and azimuth focusing. In addition, a noise elimination method based on channel estimation is proposed based on the signal transmission model. The paper also derives the range and azimuth resolution, and a simple analysis on the effect of satellite vibration is discussed in this paper. Simulation results verify the effectiveness of the algorithm and show that it can realize high-precision location for the OFDM radiation sources.

This paper is organized as follows. The signal model of OFDM signals and the principle of passive location based on the virtual synthetic aperture for OFDM signals is presented in Section 2. Azimuth resolution, range resolution, the satellite vibration effect and computation complexity of the proposed method are investigated in Section 3. Simulation results are given in Section 4. Finally, the conclusion is drawn in Section 5.

The notations related to this paper are shown in Table 1.

Table 1. Notations.

Symbol	Definition	Symbol	Definition
a	Variable	$\text{rect}\{\cdot\}$	Rectangular function
\mathbf{a}	Vector	$\exp\{\cdot\}$	Exponential function
\mathbf{A}	Matrix	$\delta(\cdot)$	Impulse function
$(\cdot)^T$	Transpose	$ \cdot $	Absolute value
$(\cdot)^*$	Conjugate	\otimes	Convolution
\hat{a}	Estimated value	$O(\cdot)$	Big-oh, complexity symbol

2. Theoretical Analyses of Typical Source Localization Methods

This section briefly analyzes the typical passive source location methods: DOA, Doppler frequency of single-satellite, TDOA, and FDOA of multi-satellites.

2.1. Direction of Arrival (DOA)

DOA systems use the direction information to realize source localization. The direction information is usually from phase interferometer systems or antenna arrays in most systems.

For a phase interferometer system, the basic principle is using the phase difference generated by the signal on different receiving antennas to obtain the direction of the source, then system location combined with two-dimensional DOA estimation obtained by a two-dimensional interferometer is used to obtain the source location.

The wave path difference of two antennas Δd can lead to phase difference $\Delta\phi$:

$$\Delta\phi = \frac{2\pi}{\lambda} \Delta d, \Delta d = d \sin \theta \quad (1)$$

where d is the baseline length and θ is the incident angle. Since the phase difference measured by a phase interferometer is ranged $(-\pi, \pi)$, only when wave path $\Delta d < \lambda/2$, there is no ambiguity in direction estimation, and the direction of the source can be directly estimated by the phase difference measured by the interferometer. When $\Delta d > \lambda/2$, there is ambiguity that needs to be solved to obtain the correct direction of the source [24].

To solve phase ambiguity and ensure direction estimation accuracy, multiple antenna structures are usually designed, such as the long and short baseline method, which uses a short baseline to solve ambiguity and a long baseline to ensure high accuracy; the virtual baseline method, which can obtain the phase difference of a short baseline by subtracting the phase difference between two different baselines to resolve the ambiguity and long baseline can ensure high accuracy; or using a rotating interferometer to solve ambiguity and reduce the number of baselines [25].

For antenna array DOA localization systems, a two-dimensional array is designed to obtain two-dimensional DOA estimation, antenna array DOA estimation can be realized by CBF, MUSIC or MLE [6].

Single-satellite DOA method is not limited by signal form and can be applied to any bandwidth signal. However, to obtain high accuracy, a complex antenna structure is needed, so the location performance is relatively poor due to the limitation of the mobile platform [3].

2.2. Doppler Frequency

The Doppler frequency localization method is realized by using the instantaneous change rate of Doppler frequency caused by the movement between satellite and source. The acceleration changes of the satellite and source can be obtained by the change rates of Doppler at various times to obtain the source location [10–13].

Suppose that at time t_1, t_2, \dots, t_n , the location of the satellite is $r_o = [x_{oi}, y_{oi}, z_{oi}]^T$, the velocity of the satellite is $v_{oi} = [v_{xi}, v_{yi}, v_{zi}]^T$, the acceleration of the satellite is $a_{oi} = [a_{xi}, a_{yi}, a_{zi}]^T$, and the location of the source is $r_T = [x, y, z]^T$. The Doppler generated by relative motion is $f_d = f_0(1 - \mathbf{r}^T \mathbf{v} / (rc))$, where f_0 is the signal carrier frequency, \mathbf{r} is the relative location vector of the source and satellite, \mathbf{v} is the relative velocity vector of the source and satellite, c is the light speed. Differentiate the above equation with respect to time to obtain the Doppler rate of change $\dot{f}_d = -\frac{f_0}{c} [\frac{\mathbf{v}^T \mathbf{v} + \mathbf{r}^T \mathbf{a}}{\mathbf{r}} - \frac{(\mathbf{r}^T \mathbf{v})^2}{\mathbf{r}^3}]$, where \mathbf{a} is the relative acceleration vector of the source and satellite. The Doppler change rate at a different time can be expressed as a matrix that $\mathbf{\Omega} = \mathbf{G}f_0 + \mathbf{E}$, where $\mathbf{\Omega} = [\dot{f}_{d1}, \dot{f}_{d2}, \dots, \dot{f}_{dN}]^T$ is the change rate of Doppler at N times. $\mathbf{G} = [u_1(x, y, z), u_2(x, y, z), \dots, u_N(x, y, z)]^T$ is N expressions about the source location, $\mathbf{E} = [\delta_{f_{d1}}, \delta_{f_{d2}}, \dots, \delta_{f_{dN}}]^T$ is the error of the Doppler change rate. The source location can be obtained by solving the nonlinear equations. The solutions of nonlinear equations include Chan, Newton iteration method, grid search method, particle swarm optimization algorithm, etc. [26].

Doppler method is simple in principle and system structure, but it requires multiple times of measurement taking to obtain high location accuracy, thus a long time is required to realize localization. It is also difficult to obtain a high-accuracy measurement of the instantaneous Doppler change rate, which greatly affects the location accuracy [10].

2.3. Time Difference of Arrival (TDOA)

TDOA as a relatively mature localization technology has been applied to various radio navigation systems. The principle is that there are spatially separated base stations and by comparing the time difference of the signal arrival to each base station, a hyperbola can be made with the base station as the focus and the distance difference as the long axis, thus the intersection point of the hyperbola is the location of the signal source. The TDOA system requires high synchronization between each base station [16].

Suppose there are M base stations (satellites) to receive the same source signal, and the location of the station i is $\mathbf{p}_i = (x_i, y_i)^T$, the signal source location is $\mathbf{p}_o = (x, y)^T$. The received signal of the base station i is

$$u_i(t) = s(t - d_i) + v_i(t), \quad i = 1, 2, \dots, M \quad (2)$$

where $s(t)$ is the source signal, d_i is the time delay of source signal arrival at i th base station, $v_i(t)$ is the additive Gaussian white noise, and the signal and noise are assumed to be independent.

With the 1st base station as the reference base station, the time difference between the source signal arrival at other base stations and the reference base station is

$$\begin{aligned} d_{i1} &= d_i - d_1, \quad i = 2, 3, \dots, M \\ \mathbf{d} &= [d_{21}, d_{31}, \dots, d_{M1}]^T \in \mathbf{R}^{(M-1) \times 1} \end{aligned} \quad (3)$$

Then, set out the system of equations using time delay \mathbf{d} and the geometric relation between base stations and target source. We can solve the system of equations by the least

square iterative algorithm (e.g., Taylor) or obtain the analytical solution by linearization method (e.g., Chan, Fang) [27].

TDOA has higher location accuracy, but it is only suitable for the wideband signals and has high requirement for time synchronization.

2.4. Frequency Difference of Arrival (FDOA)

FDOA is rarely used in a location system alone and is usually used in conjunction with the TDOA method. Therefore, FDOA is only briefly described here for the complete analysis. FDOA uses the difference of Doppler frequency shift generated by the relative motion of multiple base stations and sources to obtain the location information of the source. Compared with TDOA, FDOA is more suitable for narrow-band signals, but it is more complex and difficult to solve. Additionally, time and frequency synchronization are highly required [3].

Table 2 provides a summary and comparison of the localization methods.

Table 2. Overview of the source localization methods.

Method	Advantages	Disadvantages
DOA	Performance is independent of source form, which can be applied to narrowband and wideband signals.	High antenna complexity. Limited by the moving platform. Location accuracy is relatively poor.
Doppler Frequency	The principle and system are simple.	Requires relative motion between the source and base station. Accuracy is limited by location time. Accurate instantaneous Doppler change rate measurement is difficult.
TDOA	Provides more accurate localization. The principle is relatively simple. Suitable for wideband signal.	High requirement for time synchronization. Performance depends on signal bandwidth.
FDOA	More suitable for narrowband signal.	High requirement for time and frequency synchronization. The principle is more complex.

3. The Signal Model and Principle of Virtual Synthetic Aperture Radiation Source Location Method

3.1. The Signal Model

Different from synthetic aperture radar (SAR), the moving platform (satellite) is only equipped with a receiver to obtain the signal transmitted by radiation sources. A geometric model of the virtual synthetic aperture radiation source location method is shown in Figure 1.

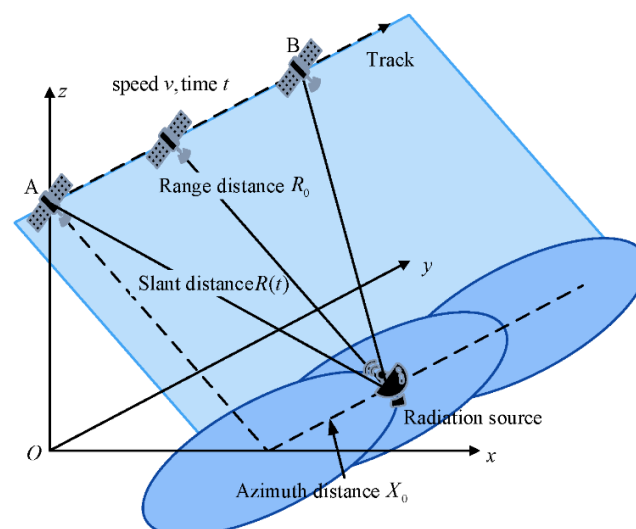


Figure 1. Geometric model of the virtual synthetic aperture radiation source location method.

The y-axis is parallel to the flight track of the receiver, the z-axis is the direction from the center of the earth to the receiver, and the x-axis direction is determined by the right-hand rule. The receiver flies over the source radiation at speed v and the flight time of the satellite is t . R_0 and X_0 denote the range and azimuth distance of the radiation source, respectively. The range direction is perpendicular to the flight track and the azimuth direction is parallel to the flight track. The receiver can receive a signal from the radiation source for the first time at starting point A and can just miss the signal at point B. Thus, the slant distance from the satellite to the radiation source $R(t)$ is

$$R(t) = \sqrt{R_0^2 + (vt - X_0)^2} \approx R_0 + \frac{(vt - X_0)^2}{2R_0} \quad (4)$$

The radiation source of this research is the 5G base station, and the signal form of the 5G radiation source is the OFDM signal. The principle of generating the OFDM signal is shown in Figure 2. After PSK/QAM modulation, the input data stream is loaded onto the single frequency subcarriers and then the modulated subcarriers are added with fixed spacing frequencies together. This process is equivalent to reconstruction of the time domain signal from the frequency domain, so the OFDM signal is generated by inverse fast Fourier transform (IFFT).

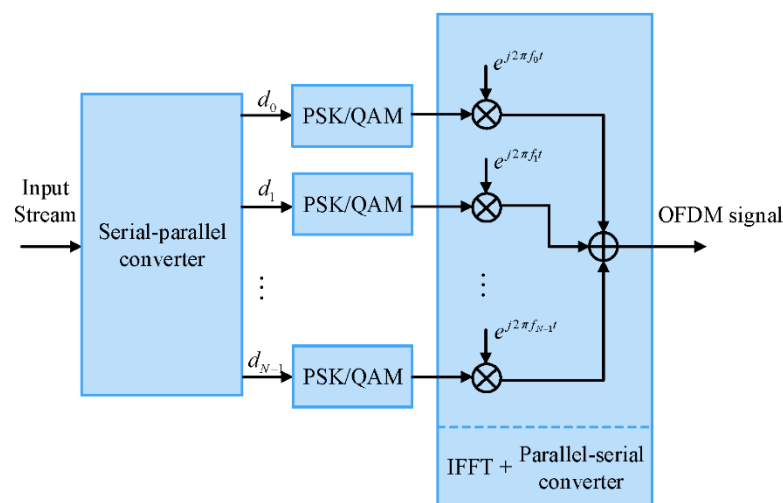


Figure 2. The principle of generating the OFDM signal.

Unlike LTE/4G, 5G has a more flexible frame structure. According to 3GPP, the downlink transmission is organized into frames with $T_f = 10\text{ms}$ duration, each consisting of ten subframes of 1 ms duration. The subframe is divided into slots, which is the minimum unit of data scheduling and the slot duration is decided by the subcarrier spacing (SCS) Δf . In addition, to remove the influence of the multipath effect, the OFDM system adopts the cyclic prefix (CP). There are two modes of 5G cyclic prefix, “Normal” and “Extended”. However, the “Extended” mode is only applicable to a specific subcarrier spacing 60 kHz, which is not considered in this paper.

The subcarrier spacing available for 5G and its corresponding parameters are shown in Table 3. The parameter μ is the subcarrier spacing configuration, $\Delta f = 2^\mu \cdot 15\text{kHz}$. The slot duration is $T_{\text{slot}} = \frac{1}{2^\mu}\text{ms}$. Because of the orthogonality of OFDM signal, the OFDM symbol duration without CP is $T_u = \frac{1}{\Delta f}$. For “Normal” mode CP, number of symbols per slot is set as 14, so the OFDM symbol duration is $T_{\text{sym}} = \frac{T_{\text{slot}}}{14}$. The difference between T_{sym} and T_u is the CP duration T_c . Thus, the transmitted signal is given by

$$s(t) = \sum_{m=0}^{\infty} \sum_{l=0}^{L-1} \sum_{k=0}^{K-1} c_{mlk} \exp\{j2\pi f_k t\} \text{rect}\{t - lT_s - mLT_s\} \quad (5)$$

where

m denotes the frame number,

l denotes the OFDM symbol number,

k denotes the subcarrier number,

c_{mlk} denotes the modulation symbols,

K denotes the number of subcarriers, which is 4096 for 5G,

L denotes the number of symbols per slot, which is 14,

f_k denotes the subcarrier frequency, $f_k = f_0 + k\Delta f$,

$\text{rect}\{\cdot\}$ denotes a rectangular function representing the duration of signal.

Thus, the received signal is expressed as follows:

$$s_r(t) = s(t - \tau(t)) = s\left(t - \frac{R(t)}{c}\right) \quad (6)$$

Table 3. The parameters of 5G frame structure.

Parameter μ	0	1	2	3	4
Subcarrier spacing (kHz)	15	30	60	120	240
Slot duration T_{slot} (μ s)	1000	500	250	125	62.5
OFDM symbol duration (without CP) T_u (μ s)	66.67	33.33	16.67	8.33	4.17
OFDM symbol duration T_s (μ s)	71.35	35.68	17.84	8.92	4.46
CP duration T_c (μ s)	4.69	2.34	1.17	0.57	0.29

3.2. The Principle of the Proposed Localization Algorithm

According to the virtual synthetic aperture technology in SAR, the data utilization mode is the “go-stop-go” mode. Take a period of the received data with duration T_p at an interval T and rearrange the data into two domains. $T_s = L_s/v$ is the synthetic aperture time, where $L_s = \theta R_0 = kcR_0/(f_0D)$, D is the antenna aperture and k is the beam width factor. Using $t_m = mT$ represents the azimuth time of the m th pulse. Thus, the slant distance (instantaneous range) at t_m is $R(t_m)$:

$$R(t_m) = \sqrt{R_0^2 + (vt_m - X_0)^2} \approx R_0 + \frac{(vt_m - X_0)^2}{2R_0} \quad (7)$$

Thus, the received signal is expressed as follows:

$$s_r(t_r, t_m) = s(t_r - \tau(t_m)) = s\left(t_r - \frac{R(t_m)}{c}\right) \quad (8)$$

Convert the signal down to the baseband and discretize it into a two-dimensional matrix \mathbf{H} with a size of $M \times N$, where M is the number of slots and N is the sampling points of one OFDM symbol. The m th row of the matrix is

$$\mathbf{H}(m, n) = \sum_{l=0}^{L-1} \sum_{k=0}^{K-1} c_{mlk} \exp\left\{j \frac{2\pi kn}{N}\right\} \exp\left\{-j \frac{2\pi f_k R(t_m)}{c}\right\} \quad (9)$$

Discrete Fourier transform (DFT) is performed along the row of the matrix \mathbf{H} , and the result is

$$\mathbf{H}_r(m, k) = \sum_{l=0}^{L-1} c_{mlk} \exp\left\{-j \frac{2\pi f_k R(t_m)}{c}\right\} \quad (10)$$

Then, we take a particular frequency $k = 0$, the signal is a LFM signal in the azimuth domain and can be written as

$$\begin{aligned} \mathbf{m}(t_m) &= \mathbf{H}_r(m) = C_m \exp\left\{-j\frac{2\pi f_0 R(t_m)}{c}\right\} \\ &= C_m \exp\left\{-j\frac{2\pi f_0 R_0}{c}\right\} \exp\left\{-j\frac{\pi f_0 (vt_m - X_0)^2}{cR_0}\right\} \end{aligned} \quad (11)$$

where $C_m = \sum_{l=0}^{L-1} c_{ml0}$.

The Doppler centroid frequency and Doppler chip rate are shown as follows, which contains the location information of the radiation source.

$$\begin{aligned} f_{dc} &= \frac{vX_0 f_0}{cR_0} \\ f_{dr} &= -\frac{v^2 f_0}{cR_0} \end{aligned} \quad (12)$$

According to the theory of matched filtering, construct a series of matched filters $\mathbf{h}(t_m, K_i)$ with different chirp rates K_i .

$$\mathbf{h}(t_m, K_i) = \exp\left\{j\pi K_i t_m^2\right\} \quad (13)$$

where $K_i = f_0 v^2 / (cR_i)$ is the chirp rate with the range R_i , and the interval is ΔR .

Take the signal $\mathbf{m}(t_m)$ through the series of matched filters, the location of the radiation source can be obtained when the output is the maximum. The output of the matched filters is:

$$\begin{aligned} \mathbf{w}(t_m) &= \mathbf{m}(t_m) \otimes \mathbf{h}(t_m, K_i) \\ &= \text{IFFT}\{\text{FFT}\{\mathbf{m}(t_m)\} \cdot \text{FFT}\{\mathbf{h}(t_m, K_i)\}\} \\ &= C'_m \text{IFFT}\left\{\exp\left\{-j\pi\left(\frac{f_m^2}{f_{dr}} + \frac{f_m^2}{K_i}\right)\right\}\right\} \otimes \delta(t_m - \frac{X_0}{v}) \end{aligned} \quad (14)$$

where $C'_m = C_m \exp\left\{-j\frac{2\pi f_0 R_0}{c}\right\}$. When $K_i = -f_{dr}$, the output is the maximum. Suppose that the peak coordinate is (\hat{R}, \hat{t}_p) . Thus, the corresponding range and azimuth location is the estimation of the radiation source location:

$$\begin{aligned} \hat{R}_0 &= \frac{f_0 v^2}{c\hat{K}} \\ \hat{X}_0 &= v\hat{t}_p \end{aligned} \quad (15)$$

3.3. Phase Compensation

The premise of the above conclusion is that the influence of C_m is ignored; however, C_m is an unknown variable whose phase will affect the location result. To solve the problem, we use the reference signals (or pilot subcarriers) for channel estimation to obtain the information carried on the modulation symbols c_{mlk} .

The reference signals (or pilot subcarriers) are specific signals in OFDM systems for channel estimation. Technical specifications for 5G NR include several different types of reference signals, which are configured and transmitted in different ways for different purposes of the receiving device. The main application of DM-RS (demodulation reference signal) in NR is to estimate the channel coefficients of physical channel coherence detection, and it can be argued that the transmitter precoding is transparent to the receiver and treated as part of the whole channel. To reduce the interpolation error and implementation complexity under the condition of a stationary channel, it is recommended to use uniform DM-RS assignment in both frequency and time domains. Since DM-RS does not transmit user data, it needs to be allocated at an appropriate density to maximize throughput. DM-RS adopts the front-loading mode, and the data is loaded after it. After estimating the channel based on the front-loaded DM-RS, the receiver can conduct coherent demodulation in the data region.

As the signal model in this paper, the time delay is considered constant in the same slot. Therefore, the channel property is time-invariant in the same slot, and different types of DM-RS can be unified into the model shown in Figure 3. The modulation symbols of the reference signal are discrete in the frequency domain and the interval is Δl . After DFT, the reference signal in a slot is processed as

$$P(k) = d_k \exp\{-j2\pi f_k \tau\} + W_p(k) = d_k H_p(k) + W_p(k) \quad (16)$$

where d_k denotes the modulation symbols of DM-RS, which are considered known to the receiver. $H_p(k)$ is the channel property at the frequency f_k . Therefore, the channel can be estimated at the reference signal as

$$\hat{H}_p(k) = \frac{P(k)}{d_k} = H_p(k) + \frac{W_p(k)}{d_k} (d_k \neq 0) \quad (17)$$

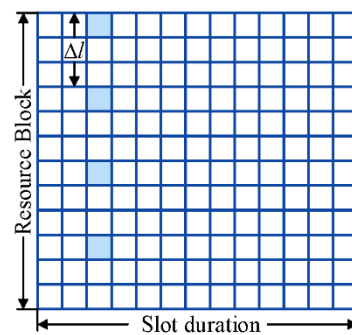


Figure 3. The unified time–frequency resource grid of virtual synthetic aperture radiation source location method.

Since $H_p(k) = \exp\{-j2\pi f_k \tau\}$ is a single-frequency signal of f_k and the interval is uniform, we adopt the transform domain interpolation method to estimate the channel property without the reference signal. The basic idea of transform domain interpolation is that adding zero in the time domain is equivalent to interpolating in the frequency domain. In addition, in the time domain, the energy of the channel is concentrated at a certain delay of the channel, while the noise exists in the whole time domain, so the noise can be removed if only the maximum point is retained. Then the channel estimation on all subcarriers in the frequency domain can be obtained by performing DFT with zero-padding in the time domain.

$$H_p(k, t_m) = \exp\{-j2\pi f_k \tau(t_m)\} \quad (18)$$

According to the estimation of the channel, we can obtain C_m in the same slot.

$$\hat{C}_m = \frac{m(t_m)}{H_p(0, t_m)} \quad (19)$$

Thus, the phase of C_m can be compensated by:

$$\begin{aligned} m'(t_m) &= \hat{C}_m^* \cdot m(t_m) \\ &= |C_m|_2 \exp\left\{-j \frac{2\pi f_0 R(t_m)}{c}\right\} \end{aligned} \quad (20)$$

where \hat{C}_m^* is the conjugate of \hat{C}_m .

In conclusion, the principle of the algorithm is shown in Figure 4. First, the received baseband signal is preprocessed to remove the CP and the preprocessed signal is rearranged into range and azimuth domain. Then FFT is performed along the range domain to extract the signal at a particular frequency. Next, to compensate for the phase of the data symbol, we use the least square method and transform domain interpolation method to estimate the channel based on the known DM-RS and use the channel characteristics for denoising.

Then we extract the compensated signal at a particular frequency in the range domain, obtaining an LFM signal in the azimuth domain with a particular centroid frequency and chirp rate which contain the location information. Finally, we construct a series of matched filters at different distances and perform pulse compression. By reorganizing the results by distance, the range and azimuth location can be obtained by focusing and searching.

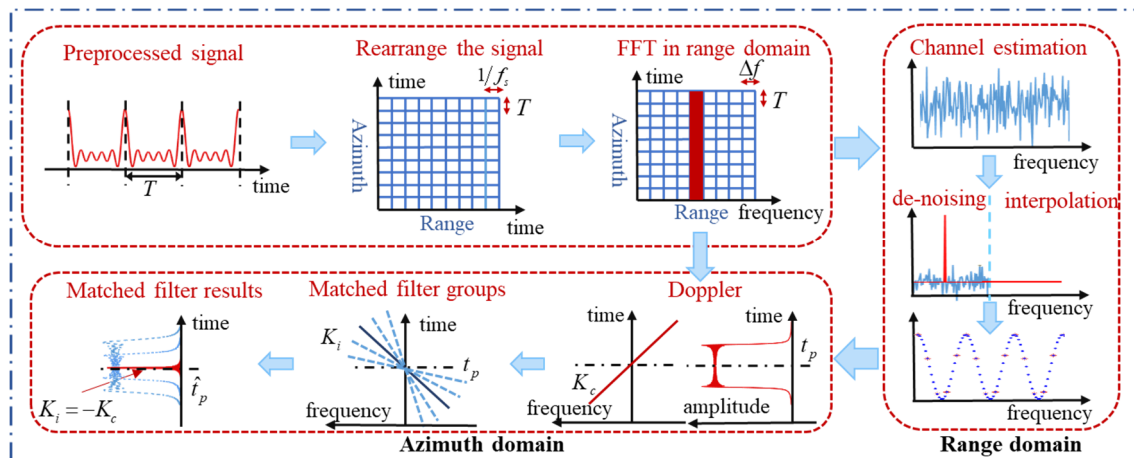


Figure 4. The principle of virtual synthetic aperture radiation source location method.

4. Resolutions and Satellite Vibration

4.1. Azimuth Resolution

The 3 dB width of the matched filtering output is $\tau_a = 1/B_a$, where B_a is the azimuth bandwidth of the signal. The virtual aperture time is T_s , so the bandwidth $B_a = KT_s = kv/D$. Thus, the azimuth resolution is:

$$\rho_a = v\tau_a = \frac{v}{B_a} = \frac{D}{k}. \quad (21)$$

As a result, the azimuth resolution is constant. However, if we process only part of the received data, the azimuth resolution will change. Suppose that the length of the captured data is t_s , the azimuth resolution is:

$$\rho_a(t_s) = \frac{v}{Kt_s} = \frac{v}{t_s} \frac{cR_0}{v^2 f_0} = \frac{cR_0}{vf_0 t_s}. \quad (22)$$

Therefore, the longer the virtual aperture is, the better the azimuth resolution will be.

4.2. Range Resolution

Chirp rates are utilized to estimate range distance. Suppose that the range distance of target 1 is R_1 with chirp rate K_1 and the range distance of target 2 is R_2 with chirp rate K_2 .

$$K_1 = \frac{f_0 v^2}{cR_1}, K_2 = \frac{f_0 v^2}{cR_2}. \quad (23)$$

The envelope of range-matched filtering for chirp rates is a Fresnel function. The bandwidth of 3 dB is $\rho = 3.4743/T_s^2$. The range resolution $\rho_r = |R_1 - R_2|$ can be calculated as follows:

$$\frac{K_1}{2} - \frac{K_2}{2} = \frac{f_0 v^2}{2cR_1} - \frac{f_0 v^2}{2cR_2} = \frac{3.4743}{T_s^2}, \quad (24)$$

$$\rho_r = |R_1 - R_2| \approx \frac{6.9486cR_0^2}{f_0 v^2 T_s^2} = \frac{6.9486f_0 D^2}{k^2 c}.$$

As a result, the range resolution is constant for the same antenna and source signal. For different sources with the same antenna, the higher center frequency causes worse range resolution. However, if we process only part of the received data, the range resolution will change. Suppose that the length of the captured data is t_s , and the range resolution is

$$\rho_r(t_s) = \frac{6.9486cR_0^2}{f_0 v^2 t_s^2}. \quad (25)$$

Therefore, the longer the virtual aperture is, the better the range resolution will be.

4.3. Computation Complexity

According to the principle of the proposed method, the received signal is first transformed into a two-dimensional matrix, whose size is $M \times N$, and FFT is performed along the row of the matrix. Since the complexity of N-points FFT is $O(N \log_2 N)$, the complexity of this process is $O(MN \log_2 N)$.

Next, for the process of compensating the phase, if the number of DM-RS symbols is K for a slot, the complexity of the least square method is $O(K)$, and the complexity of transform domain interpolation method is $O(N \log_2 N)$. Therefore, the complexity of the process is $O(MN \log_2 N)$.

Then, extract the compensated signal at a particular frequency in the range domain, obtaining an M-points LFM signal in the azimuth domain. Construct a set of N matched filters, and the matched filtering process is equivalent to the convolution process, so the complexity is $O(M^2)$, and the complexity of this process is $O(NM^2)$.

Finally, the computation complexity is $O(MN \log_2 N + NM^2)$.

4.4. Effect of Satellite Vibration

During satellite orbit, due to the influence of gravity and other factors in the universe, a small-amplitude tremor effect will be produced, leading to satellite attitude jitter. The satellite attitude jitter will cause antenna pointing stability error, which will influence the location result.

The satellite's attitude mainly changes in pitch, yaw and roll. Assuming that the attitude jitter error angles of pitch, yaw and roll directions are $\xi_\theta, \xi_\psi, \xi_\varphi$, respectively, the jitter in the range and azimuth direction are

$$\begin{aligned} \Delta\theta_a &= \xi_\psi \cos \theta_0 \sin \varphi_0 + \xi_\theta \cos \theta_0 \cos \varphi_0 \\ \Delta\theta_r &= \xi_\varphi - \xi_\psi \tan \theta_0 / \cos \varphi_0 \end{aligned} \quad (26)$$

where φ_0 is the range angle (angle of view) of the antenna and θ_0 is the azimuth angle (squint angle). The antenna azimuth jitter is mainly caused by the jitter of yaw and pitch angle, while the jitter of range direction is related to the roll and yaw angle.

When the satellite works in the strip mode and is side-looking ($\theta_0 = 0^\circ$), the relationship between the antenna azimuth and range errors and the attitude error becomes

$$\begin{aligned} \Delta\theta_a &= \xi_\psi \sin \varphi_0 + \xi_\theta \cos \varphi_0 \\ \Delta\theta_r &= \xi_\varphi \end{aligned} \quad (27)$$

Assuming that the yaw, pitch and roll attitude jitters are of a single frequency and are not coupled to each other, the mathematical model of the jitter of the antenna in the azimuth and range directions is

$$\begin{aligned} \Delta\theta_a(t) &= \theta_{am} \sin(\omega_a t + \varphi_a), \omega_a = 2\pi f_a \\ \Delta\theta_r(t) &= \theta_{rm} \sin(\omega_r t + \varphi_r), \omega_r = 2\pi f_r \end{aligned} \quad (28)$$

where $\Delta\theta_a(t)$ is the antenna jitter in the azimuth direction, $\theta_{am}, \omega_a, f_a$, and φ_a are amplitude, angular frequency, frequency and initial phase of azimuth jitter, while $\Delta\theta_r(t)$ is the antenna jitter in the range direction, $\theta_{rm}, \omega_r, f_r$, and φ_r are amplitude, angular frequency, frequency

and initial phase of range jitter. Additionally, the jitter will influence the antenna gain in the azimuth and range direction.

Thus, the effect of satellite vibration on location error can be analyzed by using the jitter model of the antenna in azimuth and range direction. Since the algorithm in this paper only needs to perform matched filtering in the azimuth direction, the influence of satellite vibration on location is mainly caused by the antenna azimuth jitter, so we can ignore the effect of the antenna range jitter and only consider the effect of the antenna azimuth jitter on the location error. The simulation results of the effect of satellite vibration are presented in Section 5.

5. Simulations and Results

The parameters of the simulation are shown in Table 4. Since the spectrum of the 5G signal is divided into two regions, 450 MHz to 6 GHz and 24 GHz to 52 GHz, the frequency of the signal is set as 29 GHz.

Table 4. Simulation parameters.

Parameters	Values
Center frequency f_0	29 GHz
Subcarrier interval Δf	30 kHz
Bandwidth	50 MHz
Sampling frequency f_s	122.88 MHz
Modulation	16 QAM
Antenna aperture D	5 m
Platform velocity v	7313 m/s
SNR	5 dB
Radiation source location	(0 km, 600 km)

According to the parameters, the virtual aperture time $T_s = kcR_c/(vf_0D) \approx 0.17$ s (generally, $k = 1$). The Doppler spectrum with a certain width after range FFT to extract signal at a particular frequency is shown in Figure 5a. After the phase compensation, the processed signal will be a linear frequency modulation signal in the azimuth domain, as shown in Figure 5b. Thus, after matched filtering, the location result is shown in Figure 6. The location error is around 10 m. The theoretical value of the azimuth resolution is $\rho_a \approx 5$ m, which is approximately equal to the simulation result. The theoretical value of the range resolution is $\rho_r \approx 16.703$ km, simulation result. Since the center frequency of the simulation signal is high, the virtual aperture is short, which leads to a poor range resolution. To improve the resolution, it is considered to use high-order spectrum instead of amplitude spectrum to analyze the location result. For 4th-order spectrum, the range resolution is $\rho_r \approx 8.498$ km, and the azimuth is $\rho_a \approx 2.5$ m.

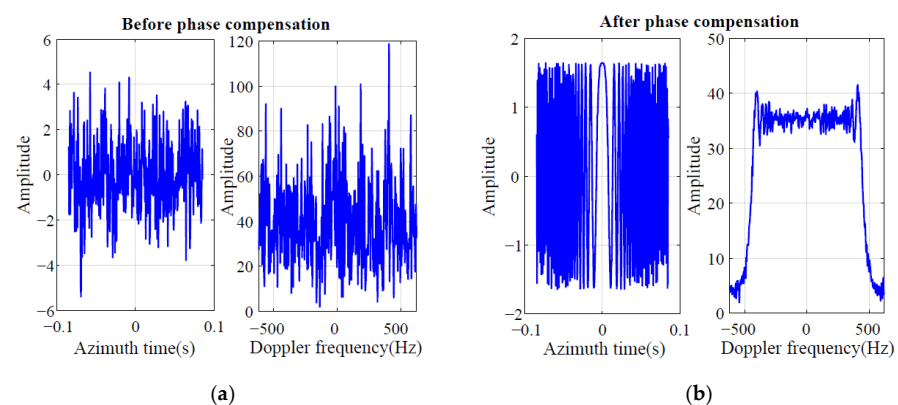


Figure 5. The Doppler spectrum before and after phase compensation. (a) The Doppler spectrum before phase compensation. (b) The Doppler spectrum before phase compensation.

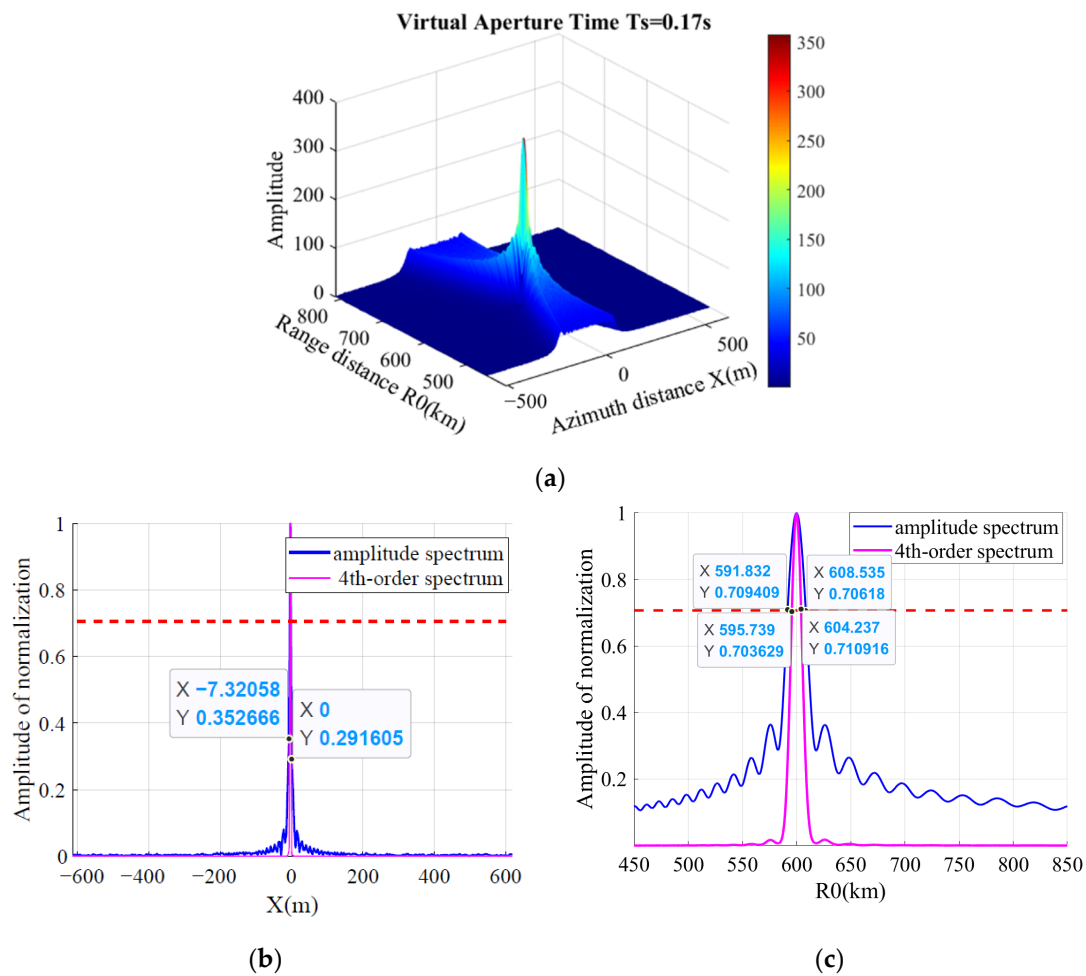


Figure 6. The passive location result. (a) The 2-D location result. (b) The azimuth location result. (c) The range location result.

After Monte Carlo simulations, the azimuth and range resolution curves of the amplitude spectrum and 4th-order spectrum are shown in Figure 7. The result shows that the azimuth and range resolution will be better with the longer virtual aperture. In addition, the simulation result is basically consistent with the theoretical result as Equations (22) and (24).

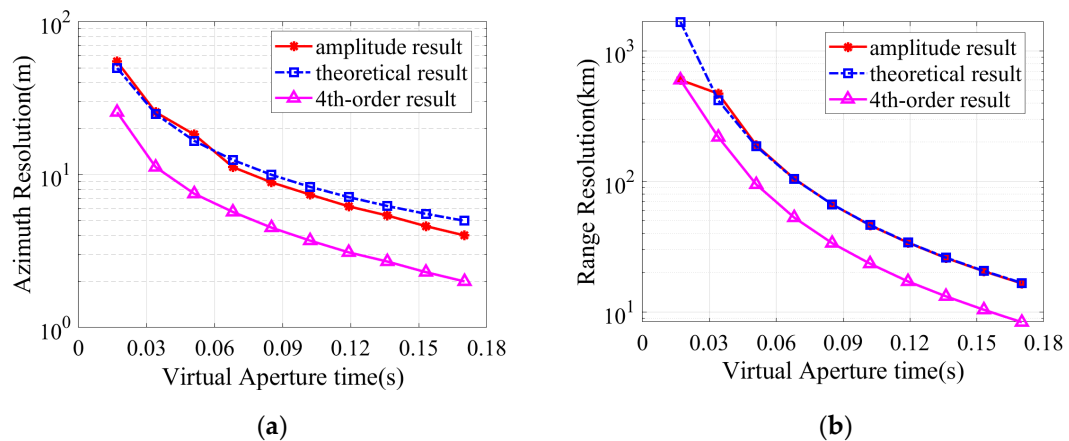


Figure 7. The resolution curves. (a) The azimuth resolution. (b) The range resolution.

Monte Carlo simulations (100 times) under different SNR are carried out, and the location error curve variation with the virtual aperture is shown in Figure 8, which was compared with the traditional DOA and TDOA methods. The DOA method is using phase interferometer for direction finding, the baseline is 5 m, and the phase ambiguity is solved by a shorter baseline with a length of 0.5 m. TDOA method uses Chan to solve the radiation source location with seven satellites. Both methods are simulated at 20 dB SNR. Compared with the DOA method, the accuracy of the virtual aperture passive location method is significantly improved, and Figure 8 shows that the longer virtual aperture leads to higher location accuracy. When SNR = 5 dB and virtual aperture time $t_s \approx 30$ ms, the location error is approximately the same as the DOA method. Under the condition of higher SNR and longer virtual aperture, the location accuracy can reach tens of meters, which is similar to that of the TDOA method, but the system complexity and cost are greatly reduced because only a single satellite and antenna are used. The configuration of satellites is shown in Figure 9. The distance between the satellites is about 100 km.

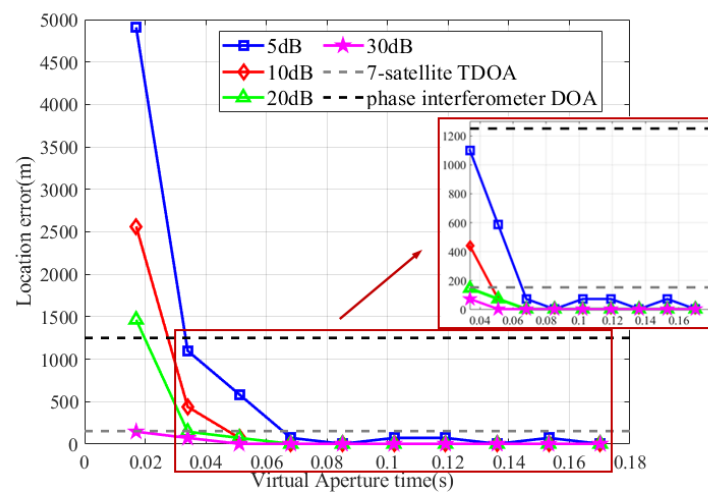


Figure 8. The location error curve variation with the virtual aperture time.

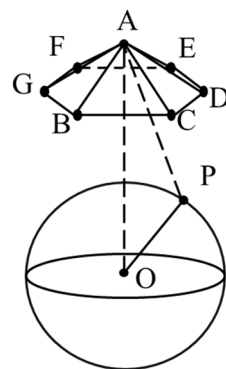


Figure 9. The configuration of satellites for the TDOA method.

The Monte Carlo simulations of the satellite vibration effect are shown in Figure 10. Since the virtual aperture time is $T_s \approx 0.17$ s, we consider the two cases that the azimuth jitter frequency $f_a < 1/T_s$ (5 Hz) and $f_a > 1/T_s$ (10 Hz, 15 Hz). The range jitter amplitude is 0.05° , and the frequency is 2 kHz; the azimuth jitter amplitude and frequency are set as shown in Figure 9, and the initial phase is random.

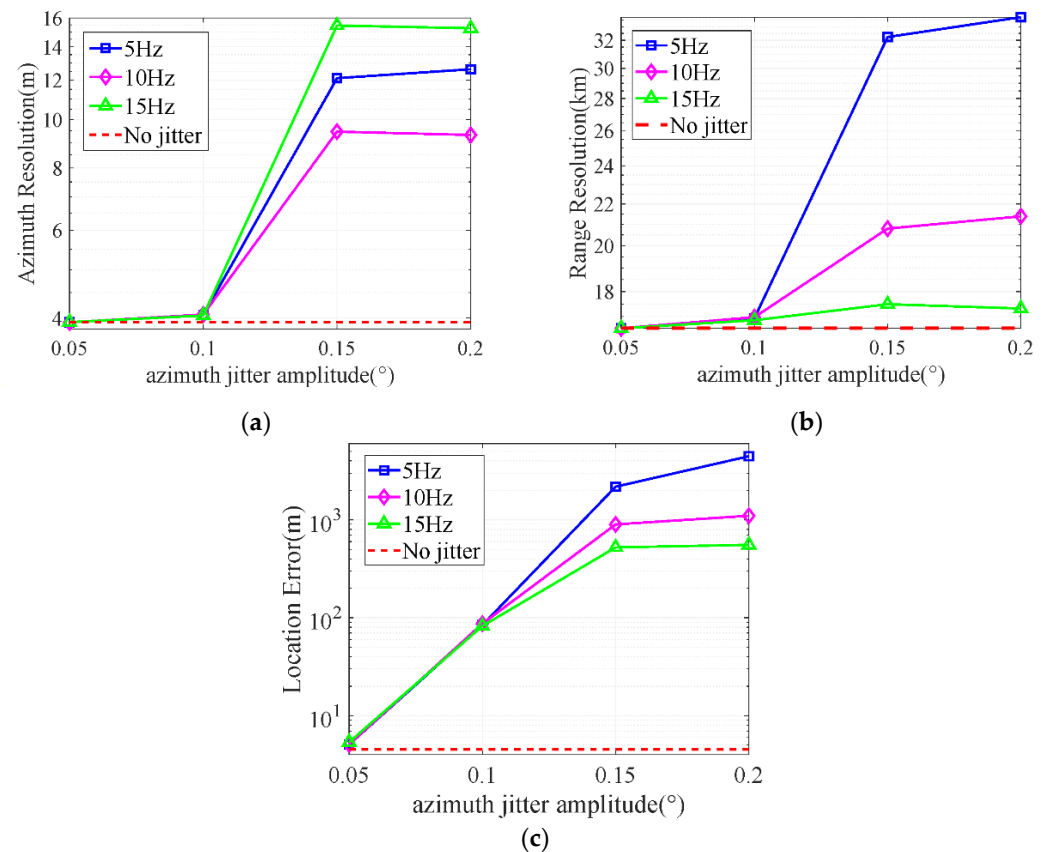


Figure 10. The effect of satellite vibration. (a) The effect on azimuth resolution. (b) The effect on range resolution. (c) The effect on location error.

The satellite vibration will cause a serious effect on the location when the azimuth jitter amplitude is greater than 0.15° , and the error will even be two orders of magnitude higher. The range and azimuth resolution will also become worse. Therefore, it is necessary to compensate for the effect caused by satellite vibration. Our subsequent research will combine the simulation results and quantitative analysis to compensate for the effect of satellite vibration.

6. Conclusions

The paper proposes a passive location for the OFDM radiation source based on the virtual synthetic aperture. The algorithm utilizes the characteristics of the moving platform and the principle of virtual aperture forming, using the coherent data to achieve the high-precision location. According to the multi-carrier modulation technology of the OFDM signal, phase information at a specific frequency can be extracted by FFT, which contains the location information of the radiation source. The reference signal of the 5G communication system is used for phase compensation and noise reduction. The processed signal is equivalent to an LFM signal in the azimuth domain, thus the azimuth location can be completed by pulse compression, while the range location can be completed by range searching. The algorithm achieves high-precision location by a single antenna, which can realize large-area coverage and turn the hardware structure into software signal processing to reduce system complexity and cost. In addition, the paper deduces the azimuth resolution and range resolution and verifies them by Monte Carlo simulations. Simulations were conducted to verify the effectiveness of the algorithm and analyze the effect of satellite vibration on resolution and location error. In subsequent studies, the effects caused by satellite vibration will be compensated according to the simulation results.

We will further analyze the performance of the proposed location algorithm, especially in the more complex scenarios such as multi-target or moving target, and improve the performance in a follow-up study.

Author Contributions: Q.Y. and X.Z. provided the core idea for this study. T.Z. and Q.Y. implemented the method and carried out the experimental evaluation. T.Z. wrote the main manuscript. T.Z., X.Z. and Q.Y. provided comments and suggestions for this paper. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China under grant 62031014 and the Key R&D Program of Hainan Province under grant ZDYF2019195.

Conflicts of Interest: The authors declare no conflict of interest.

Glossary

Acronym	Definition	Acronym	Definition
OFDM	Orthogonal Frequency Division Multiplexing	MLE	Maximum Likelihood Estimator
FFT	Fast Fourier Transform	LSE	Least Squares Estimator
LFM	Linear Frequency Modulation	DPD	Direct Position Determination
DOA	Direction of Arrival	SAR	Synthetic Aperture Radar
CBF	Conventional Beamformer	IFFT	Inverse Fast Fourier Transform
MUSIC	Multiple Signal Classification	SCS	Subcarrier Spacing
EMVS	Electromagnetic Vector Sensor	CP	Cyclic Prefix
TDOA	Time Difference of Arrival	DFT	Discrete Fourier Transform
FDOA	Frequency Difference of Arrival	DM-RS	Demodulation Reference Signal
TOA	Time of Arrival		

References

- Huang, J.H.; Barr, M.N.; Garry, J.L.; Smith, G.E.; IEEE. Subarray Processing for Passive Radar Localization. In Proceedings of the IEEE Radar Conference (RadarConf), Seattle, WA, USA, 8–12 May 2017; pp. 248–252.
- Zhu, Y.F.; Zhang, S.S.; IEEE. Passive Location Based on an Accurate Doppler Measurement by Single Satellite. In Proceedings of the IEEE Radar Conference (RadarConf), Seattle, WA, USA, 8–12 May 2017; pp. 1424–1427.
- Dempster, A.G.; Cetin, E. Interference localization for satellite navigation systems. *Proc. IEEE* **2016**, *104*, 1318–1326. [\[CrossRef\]](#)
- Kawase, S. Radio interferometer for geosynchronous-satellite direction finding. *IEEE Trans. Aerosp. Electron. Syst.* **2007**, *43*, 443–449. [\[CrossRef\]](#)
- Yuan, Q.W.; Chen, Q.; Sawaya, K. Accurate DOA estimation using array antenna with arbitrary geometry. *IEEE Trans. Antennas Propag.* **2005**, *53*, 1352–1357. [\[CrossRef\]](#)
- Eranti, P.K.; Barkana, B.D. An Overview of Direction-of-Arrival Estimation Methods Using Adaptive Directional Time-Frequency Distributions. *Electronics* **2022**, *11*, 1321. [\[CrossRef\]](#)
- Chen, T.; Shen, M.Y.; Guo, L.M.; Hu, X.J. A gridless DOA estimation algorithm based on unsupervised deep learning. *Digit. Signal Process.* **2023**, *133*, 103823. [\[CrossRef\]](#)
- Cai, C.X.; Huang, G.J.; Wen, F.Q.; Wang, X.H.; Wang, L. 2D-DOA Estimation for EMVS Array with Nonuniform Noise. *Int. J. Antennas Propag.* **2021**, *2021*, 9053864. [\[CrossRef\]](#)
- Wen, F.Q.; Shi, J.P.; Gui, G.; Gacanin, H.; Dobre, O.A. 3-D Positioning Method for Anonymous UAV Based on Bistatic Polarized MIMO Radar. *IEEE Internet Things J.* **2023**, *10*, 815–827. [\[CrossRef\]](#)
- Lopez, R.; Malarde, J.P.; Royer, F.; Gaspar, P. Improving Argos Doppler Location Using Multiple-Model Kalman Filtering. *IEEE Trans. Geosci. Remote Sens.* **2014**, *52*, 4744–4755. [\[CrossRef\]](#)
- Li, H.; Zhang, M.; Guo, F.C.; IEEE. A Novel Single Satellite Passive Location Method Based on One-Dimensional Cosine Angle and Doppler Rate of Changing. In Proceedings of the IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), Qingdao, China, 14–16 September 2018.
- Park, J.W.; Won, J.S. An Efficient Method of Doppler Parameter Estimation in the Time-Frequency Domain for a Moving Object from TerraSAR-X Data. *IEEE Trans. Geosci. Remote Sens.* **2011**, *49*, 4771–4787. [\[CrossRef\]](#)
- Zhou, T.Y.; Cheng, Y. Research on High-precision Extraction of Phase Difference Change Rate in Single Observer Passive Location. In Proceedings of the 4th International Conference on Information Science and Control Engineering (ICISCE), Changsha, China, 21–23 July 2017; pp. 1652–1655.
- Liu, C.F.; Yun, J.W.; Su, J. Direct solution for fixed source location using well-posed TDOA and FDOA measurements. *J. Syst. Eng. Electron.* **2020**, *31*, 666–673. [\[CrossRef\]](#)

15. Liu, Z.X.; Wang, R.; Zhao, J. Computationally efficient TDOA and FDOA estimation algorithm in passive emitter localisation. *LET Radar Sonar Navig.* **2019**, *13*, 1731–1740. [\[CrossRef\]](#)
16. Shu, F.; Yang, S.; Lu, J.; Li, J. On Impact of Earth Constraint on TDOA-Based Localization Performance in Passive Multisatellite Localization Systems. *IEEE Syst. J.* **2018**, *12*, 3861–3864. [\[CrossRef\]](#)
17. Wang, H.; Li, L.P. An effective localization algorithm for moving sources. *Eurasip J. Adv. Signal Process.* **2021**, *2021*, 32. [\[CrossRef\]](#)
18. Ma, G.N.; Huang, Z.J.; Wang, M.; Ji, Z.Y.; Li, X.L.; Shen, B.; Tian, J. Performance Analysis and Sensor-Target Geometry Optimization for TOA and TDOA-Based Hybrid Source Localization Method. *Appl. Sci.* **2022**, *12*, 12977. [\[CrossRef\]](#)
19. Bar-Shalom, O.; Weiss, A.J.; IEEE. Direct position determination of OFDM signals. In Proceedings of the 8th IEEE Workshop on Signal Processing Advances in Wireless Communications, Helsinki, Finland, 17–20 June 2007; pp. 1–5.
20. Bar-Shalom, O.; Weiss, A.J. Efficient direct position determination of orthogonal frequency division multiplexing signals. *LET Radar Sonar Navig.* **2009**, *3*, 101–111. [\[CrossRef\]](#)
21. Lu, Z.Y.; Wang, J.H.; Ba, B.; Wang, D.M. A Novel Direct Position Determination Algorithm for Orthogonal Frequency Division Multiplexing Signals Based on the Time and Angle of Arrival. *IEEE Access* **2017**, *5*, 25312–25321. [\[CrossRef\]](#)
22. Wang, Y.; Sun, G.C.; Xiang, J.; Xing, M.; Guo, L.; Yang, J. A Imaging Passive Localization Method for Wideband Signal Based on SAR. In Proceedings of the 2019 6th Asia-Pacific Conference on Synthetic Aperture Radar (APSAR), Xiamen, China, 26–29 November 2019; pp. 1–4.
23. Li, A.; Huan, H.; Tao, R.; Zhang, L.T. Passive Synthetic Aperture High-Precision Radiation Source Location by Single Satellite. *IEEE Geosci. Remote Sens. Lett.* **2022**, *19*, 1–5. [\[CrossRef\]](#)
24. Van Doan, S.; Vesely, J.; Janu, P.; Hubacek, P.; Tran, X.L. Optimized Algorithm for Solving Phase Interferometer Ambiguity. In Proceedings of the 17th International Radar Symposium (IRS), Krakow, Poland, 10–12 May 2016.
25. Jiang, K.C.; Wu, Y.C.; Wu, X.J.; Cai, Y.; Zhou, J.L.; Du, L.H.; IEEE. A Novel Ambiguity Resolution Method of Rolling Interferometer Based on Differential Reduction. In Proceedings of the 11th Asian Control Conference (ASCC), Gold Coast, Australia, 17–20 December 2017; pp. 2511–2515.
26. Yang, M.H.; Bao, Y.C.; Wu, C.L. Single Satellite Positioning Error Analysis and Performance Simulation Based on LEO Constellation. In Proceedings of the 13th China Satellite Navigation Conference (CSNC)—Digital Economy and Intelligent Navigation, Beijing, China, 25–27 May 2022; pp. 119–128.
27. Stefanski, J. Hyperbolic Position Location Estimation in the Multipath Propagation Environment. In Proceedings of the 2nd Joint Conference on Wireless and Mobile Networking, Gdansk, Poland, 9–11 September 2009; pp. 232–239.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.