Applied Mathematics, Modeling and Computer Simulation
C.-H. Chen et al. (Eds.)

doi:10.3233/ATDE230996

Research on Critical Active Protection Performance Evaluation Methods for the Global Navigation Satellite System in Satellite Navigation Countermeasures

Yue WANG[1], Fuping SUN and Xian WANG
School of Geospatial Information, PLA Information Engineering University, Zhengzhou (450000), Henan, China

Abstract. This paper proposes an all-sided performance evaluation system including the test system with its evaluation models and detection methods for satellite navigation countermeasures to meet the manufacturers' needs for improving critical performance in production and design and satisfy the decision-makers' demands for expanding the benefit of the global navigation satellite system (GNSS) in game. GNSS are adopted as the evaluation object, and a performance test system are established around the composition of the GNSS, the properties of satellite navigation countermeasures and their performance evaluation principles, solving the one-sidedness and imperfection in current evaluation systems. Subsequently, the evaluation models for performance indices and their detection methods are proposed around the active protective capabilities including disturbing the GNSS users and destroying its ground control segment and spatial satellite segment, as the basis for realizing the performance evaluation and quantitative analysis. Finally, the impact of each performance on the corresponding ability is analyzed through case-based simulations and tests, whose obtained results can propel the decision-makers into selecting the optimal strategy and further maximizing the protective benefit of the GNSS.

Keywords. Global navigation satellite system; satellite navigation countermeasures; jamming ability, damage effect; test system; performance evaluation

1. Introduction

Any industry that uses the global navigation satellite system (GNSS) expects its information to be secure and reliable; however, the system is highly vulnerable to suffer deliberate jamming and other threats. With the full completion of GPS, American scholars [1] firstly proposed the concept of satellite navigation countermeasures to consolidate the growing advantage of GPS in the high-tech era. With the rapid development of relevant technologies, many devices of satellite navigation countermeasures have been developed; accordingly, research on the related protective performance evaluation methods for the GNSS in satellite navigation countermeasures

[1] Corresponding Author, Yue WANG, School of Geospatial Information, PLA Information Engineering University, Zhengzhou (450001), Henan, China; E-mail: wangyplaxd@163.com.

have gradually become a hot topic based on the background of GNSS secure application. Not only is this study beneficial to the improvement of GNSS protective capability, but it also can help to make an optimal decision during a dynamic game. Therefore, this topic is of great significance to GNSS secure application.

In existing studies, the evaluation can be roughly classified into two categories: Performance and efficacy evaluation. Performance evaluation focuses on a specific technology. It evaluates the inherent attributes of an object and puts forward suggestions for improvement by modeling its performance indicators and conducting simulation and testing on these models [2,3]. Efficacy evaluation focuses on a certain system. Through operational research methods, it determines the action plan of GNSS when facing deliberate threats and obtains the optimal solution to evaluate the benefit of GNSS (or the losses suffered in the antagonistic process) and expand the benefit by updating the plan [4,5]. Furthermore, performance evaluation is the foundation for the efficacy evaluation.

There have been many studies on performance evaluation of certain technologies in various abilities of satellite navigation countermeasures recently: (1) When constructing performance indicators, Heng et al. and Wang et al. respectively built performance index systems for evaluating GNSS suppressive jamming [6] and spoofing jamming [7] technologies; however, the indices involved were one-sided, the results obtained could only meet the needs of designers for improving equipment and enhancing performance, but could not meet the final demand of decision-makers (participated in the dynamic game) for expanding GNSS benefit during countermeasures. (2) For the performance evaluation, Ceccato et al. evaluated the effect of GNSS deceptive jamming [8]; and taking a GPS receiver as an example, Psiaki et al. further demonstrated the extent of the impact of spoofing techniques on user performance [9]; however, the detection methods for certain performance indices were not established, and only test results were given. Wang et al. evaluated the suppressive jamming effect on GNSS spatial signals and proposed a method to minimize its harm [10]. How to effectively use the obtained performance evaluation results in an efficacy evaluation to maximize the protective benefit for the GNSS is a key concern for decision-makers; in practice, the quantitative results obtained from the above studies were not further used for making decisions. Therefore, the abovementioned evaluation studies resulted in inevitable limitations: (1) The created performance indices were imperfect and poorly quantified. (2) Research findings were unevenly distributed, i.e., more studies were conducted on hot topics such as GNSS anti-jamming, and less studies were conducted on the system-end damage by various threats. (3) There was a lack of continuity between the performance evaluation results and the final demand of decision-makers participated in a dynamic game.

As performance evaluation is the foundation and effective transition for efficacy evaluation, in this study, we adopt the GNSS as the evaluation object and conduct the relatively complete research on their performance indices and corresponding evaluation methods. (1) We firstly sort out the active protective capability requirements for the GNSS and their performance evaluation principles based on the composition of GNSS and the properties of satellite navigation countermeasures; based on them, we build a multi-level performance test system including testing platforms and methods to compensate for the first limitation. (2) After building the test system, we propose and perfect the evaluation model and detection method of each performance indicator, in order to overcome the second limitation. (3) We analyse and obtain the performance evaluation results to use for the efficacy evaluation, which are as a data basis for realizing the final demand of decision-makers and solving the third limitation.

2. Overview of GNSS in Satellite Navigation Countermeasures and Construction of Its Performance Test System

The essence of modern high-tech countermeasures is network-electric countermeasures in the context of massive information, whose core principle is to fight for the control right of home-court information, and satellite navigation countermeasures are the key to seize information initiative. As a necessary link to promote their development, research on the performance evaluation of this confrontation gradually becomes a hot topic. Given that prior studies have limitations, it is necessary to analyze the capability requirements of satellite navigation countermeasures and construct a performance test system from the confrontational perspective, which is fundamental for the performance and efficacy evaluation.

2.1. Constitution of Satellite Navigation Countermeasures and Their Capability Requirements

GNSS mainly consist of three subsystems, namely the spatial satellite segment, the ground control segment, and the user equipment segment [11]. As the performance of three subsystems would affect the performance and efficacy evaluation of satellite navigation countermeasures, they are considered as the basis for building the performance test system. Based on the subsystems and the components of satellite navigation countermeasures in figure 1, various indices for assessing the performance of this confrontation can be grouped into four categories (including the GNSS jamming, user-end (or called client) defense, hard destruction, and system-end defense) according to ability, where the system-end defense includes three defense systems including the spatial satellite segment (space-segment defense system), airborne early warning segment (air-segment defense system), and ground control segment (ground-segment defense system).

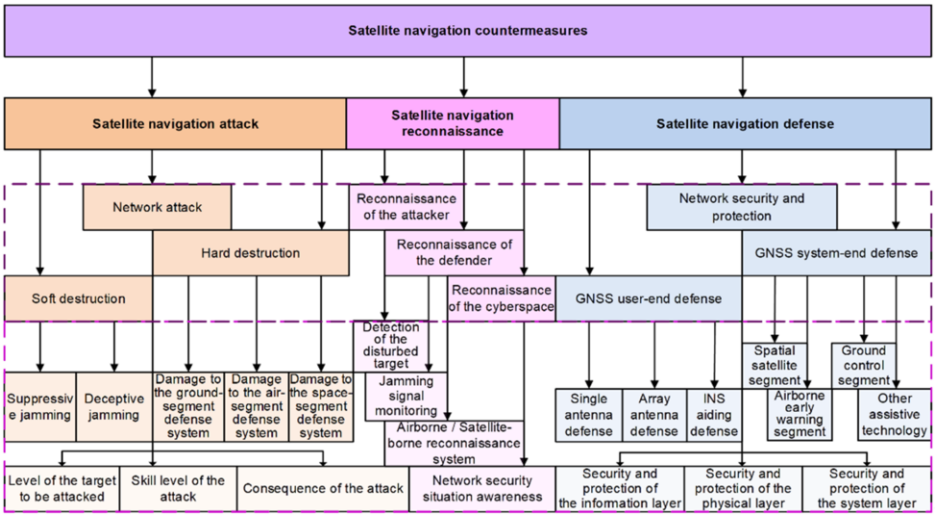

Figure 1. Basic components of satellite navigation countermeasures.

2.2. Establishment of a Performance Test System of GNSS in Satellite Navigation Countermeasures

Effective modeling and detection of bottom indices of satellite navigation countermeasures directly determine the accuracy of their performance evaluation. However, given that the abovementioned studies on the evaluation methods of bottom performance indices have problems including unspecific methods and uneven distribution, the performance testing platforms, which contribute to enhance performance, make decisions, and expand benefit, need to be established first in this paper, as the basis for perfecting relevant detection methods. Based on previous findings [12], we subsequently establish a test system, around the built testing platforms and three testing methods listed in figure 2. The purpose is to propose and perfect the evaluation models and detection methods of bottom indices corresponding to the GNSS jamming, user-end defense, hard destruction, and system-end defense and other capabilities relying on the test system.

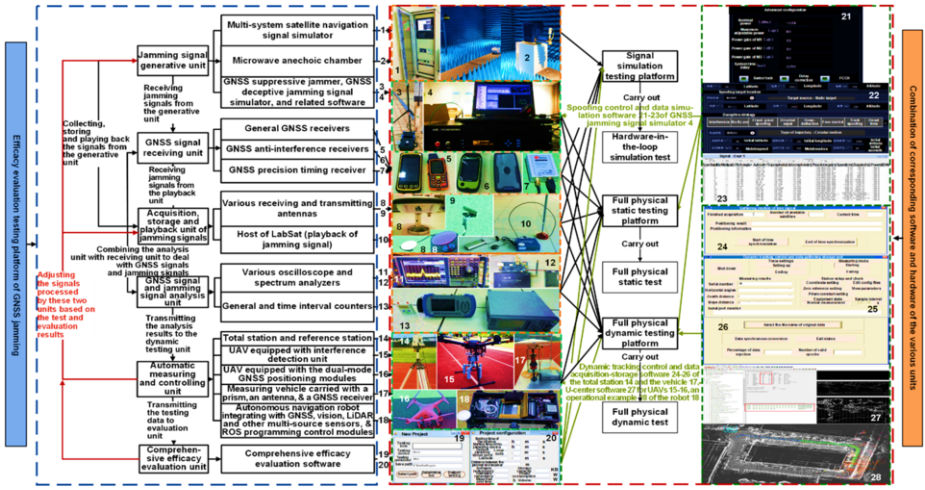

Figure 2. Components and workflow of performance test system of satellite navigation countermeasures.

3. Evaluation Methods of the Bottom Indices for Jamming Ability on the GNSS Users

GNSS jamming is a soft destruction. It mainly uses deliberate jamming, including GNSS suppressive jamming grouped into GNSS narrow-band and broadband jamming, etc., according to the bandwidth of jamming signal [13] and GNSS deceptive jamming containing the simple spoofing technique based on GNSS simulator, forwarding spoofing technique, and the complex generative spoofing technique [9], to make GNSS not work properly. Due to space limitations, we only propose the evaluation methods for the following common indices herein, whose contained parameter meanings are listed in table 1.

3.1. Common Indicators of GNSS Suppressive Jamming

GNSS suppressive jamming transmits high-power jamming signals to suppress navigation signals at the front end of a GNSS receiver, reducing the carrier-to-noise ratio (C/N) of the received navigation signals, and further making the receiver not work properly. Therefore, the signal power and jamming effect are its essential performance indices, around which can extend the following common performance indices to evaluate this jamming ability, taking the equivalent carrier-to-noise ratio and the jamming-to-signal ratio as example.

Relationship of equivalent carrier-to-noise ratio and jamming-to-signal ratio: Both the jamming-to-signal ratio threshold $(J/S)_{\min}$ and the equivalent carrier-to-noise power spectral density ratio $(C/N_0)_{\text{eq}}$ can be used to measure the jamming ability of GNSS suppressive jamming technology. Therefore, in the full digital simulation, given the calculation models of $(C/N_0)_{\text{eq}}$ (provided by existing findings [14]) and C/N_0 (denoting the C/N in a safe situation), the jamming ability respectively to a GNSS receiver and an integrated navigation receiver can be determined based on the equality relationships between $(J/S)_{\min}$, C/N_0, and $(C/N_0)_{\text{eq}}$, whose evaluation model is below.

$$\begin{cases} C/N_0 = P_{\text{R}} + G_{\text{Sa}} - 10\lg\left(k_{\text{R}} T_0\right) - N_{\text{R}} - L_{\text{R}} \\ \left(C/N_0\right)_{\text{eq}} = -10\lg\left[\dfrac{1}{10^{(C/N_0)/10}} + \dfrac{10^{(J/S)/10}}{Q_{\text{J}} f_{\text{code}}}\right] \\ \left(J/S\right)_{\min} = 10\lg\left[Q_{\text{J}} f_{\text{code}}\left(\dfrac{1}{10^{(C/N_0)_{\text{eq}}/10}} - \dfrac{1}{10^{(C/N_0)_{\min}/10}}\right)\right] \end{cases} \tag{1}$$

where f_{code} denotes the pseudocode code rate, in which $f_{\text{C/A}} = 1.023$ MHz and $f_{\text{P(Y)}} = 10.23$ MHz [11].

3.2. Common Indicators of GNSS Deceptive Jamming

GNSS deceptive jamming transmits false satellite navigation signals by means of forwarding or generating, causing a receiver to work out the wrong position information; compared with suppressive jamming, although its realization is difficult and the harm is more serious, it has better concealment and can achieve accurate control of the receiver [1]. Therefore, positioning accuracy and time synchronization are its essential performance indices, around which can extend the following common performance indices to evaluate the spoofing ability.

3.2.1. Success Rate of Spoofing

It can evaluate the spoofing effect under different power conditions for spoofing signals. In the full physical test, the spoofing distance and signal power are specified, and tests are repeated n times (10 epochs are counted as one test). If the obtained RMSE(s) does not exceed 0.50 m and the mean absolute deviation of the pseudo-range MAD(ρ) does not exceed 10 m, the deception is considered as success.

$$\begin{cases} \mathrm{RMSE}(\text{spoofing}) = \sqrt{\dfrac{1}{n}\sum_{i=1}^{n}\left[\left(x_{si}-x_{si_0}\right)^2+\left(y_{si}-y_{si_0}\right)^2+\left(h_{si}-h_{si_0}\right)^2\right]} \le 0.50\,\mathrm{m} \\ \cap \quad \mathrm{MAD}(\rho) = \dfrac{1}{n}\sum_{i=1}^{n}\left|\rho_{\mathrm{r}i}-\mathrm{mean}\left(\rho_{0i}\right)\right| \le 10\,\mathrm{m} \end{cases} \tag{2}$$

where mean(ρ_{0i}) represents a mean pseudo-range of the preset spoofing position (x_{si0}, y_{si0}, h_{si0}), and ρ_{ri} denotes a pseudo-range of the receiver's actual positioning result (x_{si}, y_{si}, h_{si}).

$$\omega = g/n \tag{3}$$

As g-th of the n-th tests are successful, the success rate of spoofing (ω) can be obtained, and its relationship with the test number can be further determined.

3.2.2. Timing Accuracy of the Synchronous Clocks

It is one of the important indices to measure the time synchronization capability of GNSS deceptive jamming technology. In the full physical static test, the test steps are as follows.

Firstly, a spoofer is opened, antennas are disconnected after being positioned for 24 h, and the output information related to the time difference is recorded for 1 hour. Then, the deviations ($\Delta t_{\hat{1}i}$) of the first 100 points in the information and the deviations (Δt_{1i}) of the last 100 points in the information are summed and averaged to obtain this indicator.

$$\Delta t = \frac{1}{100}\left|\sum_{i=1}^{100}\Delta t_{\hat{1}i}-\sum_{i=1}^{100}\Delta t_{1i}\right| \le 200\ \mathrm{ns/h} \tag{4}$$

If Δt is less than or equal to 200 ns/h, this performance under test is effective. The smaller Δt is, the better the spoofing effect of the spoofer under test is.

Table 1. Meanings of parameters contained in the evaluation models for GNSS jamming ability indices.

Index name	Equations for the index	Parameters contained in the equation	Meanings of the parameters
Relationship of equivalent carrier-to-noise ratio and jamming-to-signal ratio	Equation (1)	P_R	GNSS signal power
		G_R	Antenna gain of the receiver pointing at the satellite
		$10\lg(K_R T_0)$	Thermal noise density of the receiver
		N_R and L_R	The receiver's noise and its processor loss
		f_{code}	Pseudocode code rate
		Q_J	Spread spectrum processing factor

4. Evaluation Methods of the Bottom Indices for the Damage Effect on the GNSS System End

The effect evaluation of the hard destruction denotes the quantitative criterion of the damage effect and destructive degree to the system end. This criterion divides into the damage effect, content force, pre-test assessment, and post-test assessment according to the properties of satellite navigation countermeasures under massive information

conditions. Given space limitations and evaluation prioritization, we select the damage effect herein, and model its corresponding bottom indicators whose contained parameter meanings are listed in table 2, further perfect their detection methods to evaluate the damage effect of hard destruction on the space-, air-, and ground-segment defense systems.

4.1. Damage Effect on the Space-Segment Defense System

Most of spacecrafts adopt the double-deck structure or the improved double-deck structure, which makes fragments acting on the shielded thin plate of a spatial target to form debris clouds and further acting on its different compartments. Studying the damage effect of debris clouds on the spatial target is roughly equivalent to research on the damage effect of hard destruction on the space-segment defense system. Usually, two types of damage effect can be produced by debris clouds [15]. One is the local perforation destructive effect in the form of many perforations; the other is the tearing destructive effect in the form of dynamic pressure with large area. The penetration and tearing destructions occur simultaneously and aggravate mutually.

4.1.1. Local Perforating Destructive Probability

When a debris cloud finally reaches the compartment, its debris particles are already quite small. To form the perforating destructive effect, a certain number of perforations must be present to create a perforating area with a certain size. Therefore, it is appropriate to measure the local perforating destructive probability ($\mathrm{Prob_{LP}}$) of debris clouds by the size of the perforation area ($\mathrm{Area_{FC}}$) they cause on the compart-ment of a spatial target and its related parameters in the full digital simulation. Furthermore, referring to a previous study [16], we create the following evaluation model of $\mathrm{Prob_{LP}}$.

$$\begin{aligned}
&\mathrm{Area}_{\mathrm{FC}}^{\mathrm{th}} = L_{\mathrm{ength}}{}^{\wedge}\left(\frac{2}{R_{\mathrm{cabin}}}\right)\mathrm{Area}_{\mathrm{cabin}}^{R_{\mathrm{cabin}}},\ \mathrm{Area}_{\mathrm{FC}} = \sum_{d_{\mathrm{ebris}}=1}^{D_{\mathrm{ebris}}}\mathrm{Area}_{\mathrm{FC}}^{d_{\mathrm{ebris}}} \\
&\mathrm{Prob}_{\mathrm{LP}} = \begin{cases} 1 & \mathrm{Area}_{\mathrm{FC}} \geq \mathrm{Area}_{\mathrm{FC}}^{\mathrm{th}} \\ \mathrm{Area}_{\mathrm{FC}} \,/\, \mathrm{Area}_{\mathrm{FC}}^{\mathrm{th}} & 0 < \mathrm{Area}_{\mathrm{FC}} < \mathrm{Area}_{\mathrm{FC}}^{\mathrm{th}} \\ 0 & \mathrm{Area}_{\mathrm{FC}} = 0 \end{cases}
\end{aligned} \tag{5}$$

From Equation (5), in the process of this effect resulting in substructural failure, if the surface area of the compartment and its inside volume increase, the slower the operating temperature in the compartment falling to ambient temperature is for the same perforating area, accordingly, the larger the corresponding $\mathrm{Area_{FC}^{th}}$ becomes, the smaller the $\mathrm{Prob_{LP}}$ is.

4.1.2. Tearing Destructive Probability

Debris clouds cause strong dynamic pressure on the compartment, resulting in a series of shockwaves inside its material; they are then superimposed and propagated; eventually the compartment is torn apart and destroyed. Therefore, the specific impulse per unit area I_{SP} (MA) generated by debris clouds can be taken as a measure of the tearing destructive probability ($\mathrm{Prob_{TF}}$). In the full digital simulation, it is assumed that the large-area tearing destructive effect of debris clouds is like its strong shockwave

effect; accordingly, we can create the following evaluation model of $\mathrm{Prob}_{\mathrm{TF}}$ by referring to the strong shockwave destructive criterion [16].

$$I_{\mathrm{SP}}(\mathrm{DY}) = \frac{(\sigma_{\mathrm{DY}}\sigma_{\mathrm{US}}\mathrm{Thick}_{\mathrm{FP}})}{c\sigma_{\mathrm{US}}^{\mathrm{Al}}},\quad I_{\mathrm{SP}}(\mathrm{US}) = \frac{(\sigma_{\mathrm{US}}^{2}\mathrm{Thick}_{\mathrm{FP}})}{c\sigma_{\mathrm{US}}^{\mathrm{Al}}}$$
$$\mathrm{Prob}_{\mathrm{TF}} = \begin{cases} 0 & I_{\mathrm{SP}}(\mathrm{MA}) \le I_{\mathrm{SP}}(\mathrm{DY}) \\ \dfrac{I_{\mathrm{SP}}(\mathrm{MA}) - I_{\mathrm{SP}}(\mathrm{DY})}{I_{\mathrm{SP}}(\mathrm{US}) - I_{\mathrm{SP}}(\mathrm{DY})} & I_{\mathrm{SP}}(\mathrm{DY}) < I_{\mathrm{SP}}(\mathrm{MA}) < I_{\mathrm{SP}}(\mathrm{US}) \\ 1 & I_{\mathrm{SP}}(\mathrm{MA}) \ge I_{\mathrm{SP}}(\mathrm{US}) \end{cases} \tag{6}$$

During satellite navigation countermeasures, as $I_{\mathrm{SP}}(\mathrm{MA})$ increases, $\mathrm{Prob}_{\mathrm{TF}}$ also increases, the damage effect on the space-segment defense system is stronger.

4.2. Damage Effect on the Air-Segment Defense System

As the principle of damaging to different components of an aircraft is different, its vital components need to be grouped into three categories, including flammable (e.g., fuel tanks), explosive (e.g., various ammunition boxes carried), and functional/systematic components (e.g., engines, instrumentation, and fire control systems, etc.). Thus, based on the distributive nature of fragments (shown in figure 3) and the feature information of vital components, the following specific indicator of the damage effect can be created to evaluate the damage effect of hard destruction on the air-segment defense system.

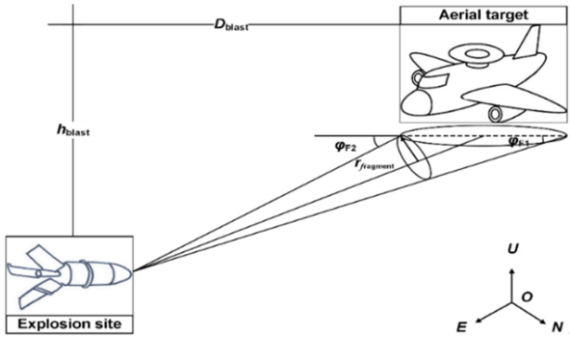

Figure 3. Diagram of intersecting information of the projectile explosion site and the aerial target.

In the full digital simulation, based on the calculation models of the destructive probability P_{HI} for flammable/explosive components and P_{HD} for functional/systematic components given in previous findings [17], if the fragment dispersion of the projectile exploding in close proximity is uniform distribution, and setting the damage area that fragments hit the three types of vital components of the aircraft as S_{D1}, S_{D2}, S_{D3}, we can develop the following evaluation models for the destructive probability $P_{\mathrm{AD}}(p_{\mathrm{ellet}})$ and destruction error $\mathrm{Error}_{\mathrm{AD}}$ of fragments (generated by the p_{ellet}-th near-blast projectile) to the vital components.

$$P_{\mathrm{AD}}\left(p_{\mathrm{ellet}}\right)=1-\left\{1-\frac{\left[\frac{\left(S_{\mathrm{D1}}+S_{\mathrm{D2}}\right)P_{\mathrm{HI}}\left(p_{\mathrm{ellet}}\right)+S_{\mathrm{D3}}P_{\mathrm{HD}}\left(p_{\mathrm{ellet}}\right)}{\sum_{f_{\mathrm{ragment}}=1}^{F_{\mathrm{ragment}}\left(p_{\mathrm{ellet}}\right)}\left(0.25\pi r_{f_{\mathrm{ragment}}}^{2}\cos\phi_{f_{\mathrm{ragment}}}\right)}\right]^{F_{\mathrm{ragment}}\left(p_{\mathrm{ellet}}\right)}}{\left[\frac{1}{N_{\mathrm{test}}}\sum_{n_{\mathrm{test}}=1}^{N_{\mathrm{test}}}P_{\mathrm{ellet}}\left(n_{\mathrm{test}}\right)\right]}\right\} \tag{7}$$

If the fragments are spherical, columnar, or rod-shaped, etc., the piercing diameter and impact angle of the f_{ragment}-th fragment are $r_{f_{\mathrm{ragment}}}$ and $\phi_{f_{\mathrm{ragment}}}$, where $\phi_{f_{\mathrm{ragment}}} \in (\varphi_{\mathrm{F1}}, \varphi_{\mathrm{F2}})$.

$$\mathrm{Error}_{\mathrm{AD}}=\sqrt{\frac{1}{N_{\mathrm{test}}}\sum_{n_{\mathrm{test}}=1}^{N_{\mathrm{test}}}\left\{\frac{1}{P_{\mathrm{ellet}}\left(n_{\mathrm{test}}\right)}\sum_{p_{\mathrm{ellet}}=1}^{P_{\mathrm{ellet}}\left(n_{\mathrm{test}}\right)}\left[P_{\mathrm{AD}}\left(p_{\mathrm{ellet}}\right)-\max\begin{pmatrix}P_{\mathrm{AD}}(1),\\P_{\mathrm{AD}}(2),\cdots,\\P_{\mathrm{AD}}\left(p_{\mathrm{ellet}}\right),\cdots,\\P_{\mathrm{AD}}\left(P_{\mathrm{ellet}}\left(n_{\mathrm{test}}\right)\right)\end{pmatrix}\right]^{2}\right\}} \tag{8}$$

During satellite navigation countermeasures, an increase in $P_{\mathrm{AD}}(p_{\mathrm{ellet}})$ indicates better the damage effect on the air-segment defense system; otherwise, the damage effect is worse; a smaller $\mathrm{Error}_{\mathrm{AD}}$ suggests higher the continuous success rate in damaging the air-segment defense system; otherwise, the continuous success rate decrease.

4.3. Damage Effect on the Ground-Segment Defense System

The main types of hard destructive weapons against the ground-segment defense system are various types of carrier-based aircrafts, including reconnaissance, fighter, and jammer [18]. Based on this, the corresponding specific performance indicators can be created to evaluate the damage effect of hard destruction on the ground-segment defense system. Due to the limitation of space, only the performance indicator, namely damage ability against a ground target ($\mathrm{Ability}_{\mathrm{TD}}$), is created here as a standard to measure the ability of relevant equipment in damage to this defense system.

$\mathrm{Ability}_{\mathrm{TD}}$ is defined as the ability of a carrier-based aircraft or a missile to damage the important solid target, such as monitoring stations, upload stations, and master control station in the ground-segment defense system, through the penetration effect P_{PE} and the detonation effect P_{DA}, without considering the secondary damage effect [19]. In the full digital simulation, if the distance between the ground target and the detonation point is set to D_{TBP}, the following model for evaluating the damage ability of the weapons against the ground target can be built.

$$\begin{cases} P_{\mathrm{PE}} = 1 - \left[1/\left(\sqrt{2\pi}\sigma_{\mathrm{PE}}\right)\right]\int_0^{(D_{\mathrm{TBP}})_{\max}} \exp\left[-\left(D_{\mathrm{TBP}} - R_{\mathrm{PE}}\right)^2/\left(2\sigma_{\mathrm{PE}}^2\right)\right]\mathrm{d}D_{\mathrm{TBP}} \\ = 1 - \dfrac{\int_0^{(D_{\mathrm{TBP}})_{\max}} \exp\left[-\left(D_{\mathrm{TBP}} - 2.080B_{\mathrm{reak}}\sqrt[3]{W_{\mathrm{powder}}}\right)^2/\left(0.4599B_{\mathrm{reak}}\sqrt{2}\sqrt[3]{W_{\mathrm{powder}}}\right)^2\right]\mathrm{d}D_{\mathrm{TBP}}}{\sqrt{2\pi}\left(0.4599B_{\mathrm{reak}}\sqrt[3]{W_{\mathrm{powder}}}\right)} \\ P_{\mathrm{DA}} = 1 - \left[1/\left(\sqrt{2\pi}\sigma_{\mathrm{DA}}\right)\right]\int_0^{(D_{\mathrm{TBP}})_{\max}} \exp\left[-\left(D_{\mathrm{TBP}} - R_{\mathrm{DA}}\right)^2/\left(2\sigma_{\mathrm{DA}}^2\right)\right]\mathrm{d}D_{\mathrm{TBP}} \\ = 1 - \dfrac{\int_0^{(D_{\mathrm{TBP}})_{\max}} \exp\left[-\left(D_{\mathrm{TBP}} - 1.664B_{\mathrm{reak}}\sqrt[3]{W_{\mathrm{powder}}}\right)^2/\left(0.3679B_{\mathrm{reak}}\sqrt{2}\sqrt[3]{W_{\mathrm{powder}}}\right)^2\right]\mathrm{d}D_{\mathrm{TBP}}}{\sqrt{2\pi}\left(0.3679B_{\mathrm{reak}}\sqrt[3]{W_{\mathrm{powder}}}\right)} \end{cases} \tag{9}$$

$$\mathrm{Ability}_{\mathrm{TD}} = 1 - (1 - P_{\mathrm{PE}})(1 - P_{\mathrm{DA}}) \tag{10}$$

According to the conclusions given in the existing study [19], R_{PE} and R_{DA} are functions of the TNT equivalent (W_{powder}) of the weapon's charge and the fragmentation coefficient (B_{reak}) related to the properties of the medium and the explosive, respectively; σ_{PE} and σ_{DA} are functions of their corresponding effective damage radius (R_{PE} and R_{DA}). Larger P_{PE} and P_{DA} values suggest $\mathrm{Ability}_{\mathrm{TD}}$ is larger and the related weapon is more likely to have the ability to destroy the ground target.

Table 2. Meanings of parameters contained in the evaluation models for the system-end damage effect indices.

Index name	Equations corresponding to the index	Parameters contained in the equation	Meanings of the parameters
Local perforating destructive probability	Equation (5)	$\mathrm{Area}_{\mathrm{FC}}^{\mathrm{th}}$	Critical perforation area
		$\mathrm{Area}_{\mathrm{cabin}}$	Surface area of a compartment facing threats
		L_{ength}	Dimension of a unit of length
		D_{ebris}	Total number of debris clouds
		$\mathrm{Area}_{\mathrm{FC}}^{d_{\mathrm{ebris}}}$	The parameter related to the total number of debris clouds and the perforation area of individual debris
		R_{cabin}	The experimental constant associated with the geometrical characteristics of the compartment and the ambient temperature, which is dimensionless and less than 1
Tearing destructive probability	Equation (6)	$I_{\mathrm{SP}}(\mathrm{DY})$, $I_{\mathrm{SP}}(\mathrm{US})$	Specific impulse exerted by debris clouds on this material when the compartment material respectively reaches the dynamic yield and the ultimate strength
		$\mathrm{Thick}_{\mathrm{FP}}$, $\mathrm{Thick}_{\mathrm{ED}}$	Front plate thickness of the compartment and its equivalent duralumin thickness
		σ_{DY}, σ_{US}	Dynamic yield and ultimate strength of compartment material
		$\sigma_{\mathrm{US}}^{\mathrm{Al}}$	Ultimate strength of the compartment duralumin
Destructive probability of fragments on the vital components	Equations (7) and (8)	$P_{\mathrm{ellet}}(n_{\mathrm{test}})$	Number of hits required for damaging the vital components in the n_{test}-th test
		$F_{\mathrm{ragment}}(p_{\mathrm{ellet}})$	Number of fragments generated by the p_{ellet}-th near-blast projectile
Damage ability against the ground target	Equation (9)	R_{PE} and σ_{PE}	Effective damage radius and damage mean square error of the penetration effect
		R_{DA} and σ_{DA}	Effective damage radius and damage mean square error of the detonation effect

5. Analysis of Performance Evaluation Results for the GNSS in Satellite Navigation Countermeasures

To meet the final demand of decision-makers, depending on the test system and the performance evaluation methods proposed around the capability requirements of satellite navigation countermeasures, we perform the simulation and experimental studies of various performance indicators changing with diverse parameters such as signal power herein. The evaluation results obtained will serve as a complete theoretical and data basis for realizing the efficacy evaluation.

5.1. Full Digital Simulation Tests and Related Results Analysis

5.1.1. Performance evaluation of GNSS jamming

Figure 4 shows that: (1) For the same jamming equipment, taking GPS signals as an example, the jamming-to-signal ratio threshold $(J/S)_{min}$ for C/A code is much smaller than that for P(Y) code; $(J/S)_{min}$ for a normal GPS receiver is much smaller than that for an GPS receiver assisted by INS. Therefore, it is easier for the jamming equipment to disturb a civil receiver without INS aiding. (2) As the spread spectrum processing factor Q_J is proportional to $(J/S)_{min}$, the jamming ability decreases from GNSS narrow-band jamming, broadband spread spectrum jamming, to broadband jamming.

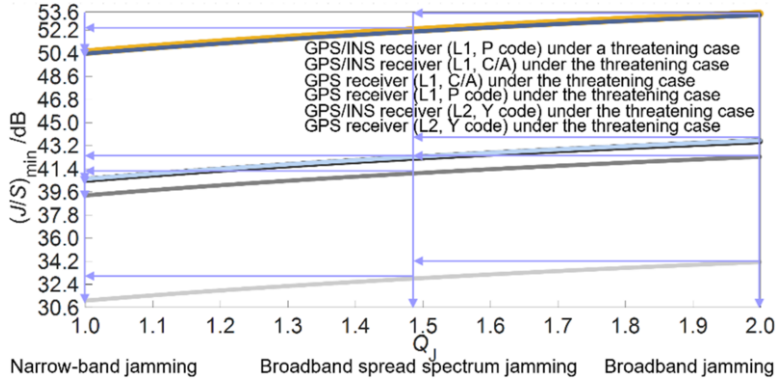

Figure 4. Simulation of the relationship between Q_J and $(J/S)_{min}$ based on different GPS users.

5.1.2. Evaluation of the Damage Effect on the Space-Segment Defense System

From figure 5, the total number of debris clouds D_{ebris} is proportional to its local perforating destructive probability $Prob_{LP}$ until $Prob_{LP} = 1$. When D_{ebris} and their formed perforation shape are fixed, the stronger the perforation capacity of debris clouds is, the larger $Prob_{LP}$ is. When the perforation capacity is fixed, if the perforation shape arranges according to foursquare, regular triangle and strip-groove, its corresponding $Prob_{LP}$ increases in sequence, and the D_{ebris} required for full piercing decreases in turn. From figure 6, the specific impulse per unit area I_{SP}(MA) generated by debris clouds is proportional to its tearing destructive probability $Prob_{TF}$ until $Prob_{TF} = 1$. When I_{SP} (MA) is fixed, the lower the ultimate strength of the compartment material of the space-segment defense system (σ_{US}) is, the weaker its defense capability is; accordingly, the larger the $Prob_{TF}$ caused by debris clouds is, further the smaller the I_{SP} (MA) required for full tearing is.

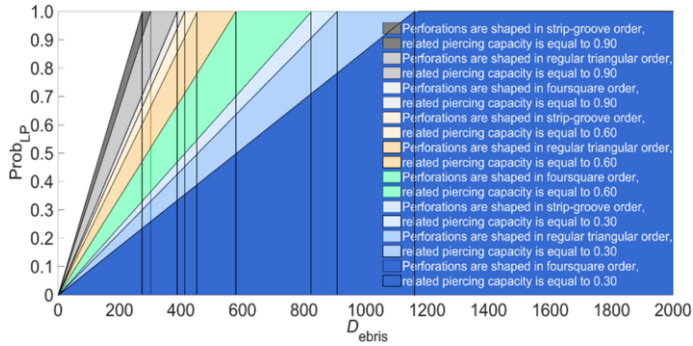

Figure 5. Simulation graph of the relationship between $Prob_{LP}$ and D_{ebris} based on debris clouds with different properties.

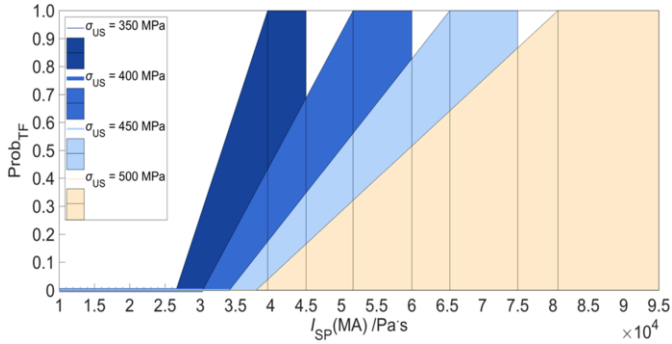

Figure 6. Simulation of the relationship between $Prob_{TF}$ and I_{SP}(MA) based on spatial targets with different properties.

5.1.3. Evaluation of the Damage Effect on the Air-Segment Defense System

From figure 7, it is clear that: (1) When the fragment shape is fixed, if the number of hit projectiles P_{ellet} required for damaging the critical components of the aircraft in a single test decreases, and the number of fragments $F_{ragment}(p_{ellet})$ generated by the p_{ellet}-th projectile (exploded in close proximity) increases, and then the destructive probability $P_{AD}(p_{ellet})$ of the $F_{ragment}(p_{ellet})$ increases until $P_{AD}(p_{ellet}) = 1$. (2) When $F_{ragment}(p_{ellet})$ (> 1) and P_{ellet} (> 1) are fixed, $P_{AD}(p_{ellet})$ becomes larger in sequence for spherical, columnar, or rod-shaped fragments, and its corresponding damage ability becomes larger in turn. Fig. 8 shows that: No matter what the shape of fragments, when single P_{ellet} reaches a certain value, $P_{AD}(p_{ellet})$ fluctuates continuously with the change of the impact angle $\phi_{fragment}$; then, $P_{AD}(p_{ellet})$ gradually stabilizes as P_{ellet} becomes larger. Specifically, (1) the overall variation trend of $P_{AD}(p_{ellet})$ corresponding to spherical fragments decreases as P_{ellet} (> 17) increases, and the maximum value (= 1) of $P_{AD}(p_{ellet})$ is achieved when P_{ellet} = 17; (2) the overall variation trend of $P_{AD}(p_{ellet})$ corresponding to rod-shaped fragments increases as P_{ellet} (> 56) increases, and the maximum value (= 1) of $P_{AD}(p_{ellet})$ is achieved when P_{ellet} = 67; (3) the overall variation trend of $P_{AD}(p_{ellet})$ corresponding to columnar fragments increases as P_{ellet} (> 109) increases, and the maximum value (= 0.61) of $P_{AD}(p_{ellet})$ is achieved when P_{ellet} = 120. Thus, when $F_{ragment}(p_{ellet})$ is greater than 40, spherical fragments are a better choice of hard destructive weapons in terms of the damage effect and damage cost.

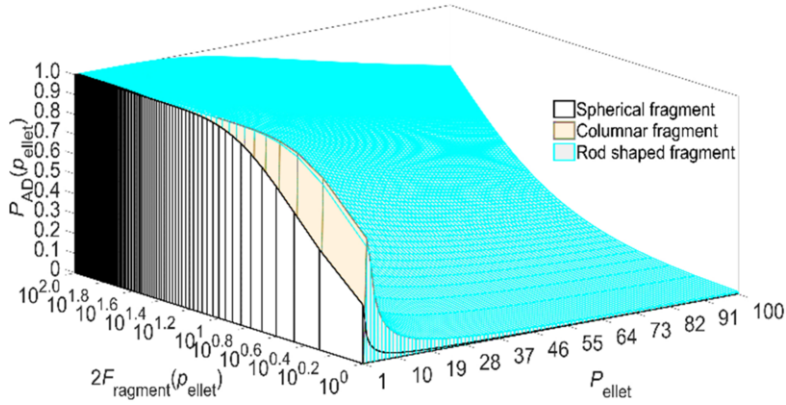

Figure 7. Simulation diagram of the relationship between three variables P_{AD}, P_{ellet}, and $F_{ragment}$ based on different shapes of fragments.

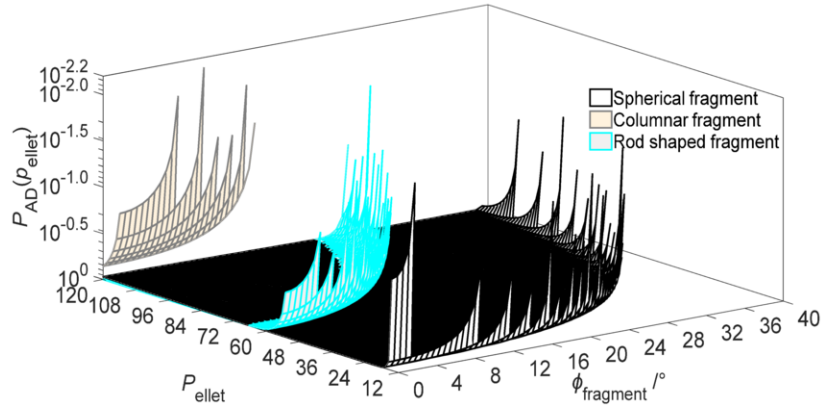

Figure 8. Simulation diagram of the relationship between three variables P_{AD}, $\phi_{f_{ragment}}$, and P_{ellet} based on different shapes of fragments.

5.1.4. Evaluation of the Damage Effect on the Ground-Segment Defense System

Figure 9 shows that: (1) The larger the breaking coefficient B_{reak} related to medium and explosive properties is, the smaller the distance between the ground target and the detonation point D_{TBP} is, and the better the penetration effect P_{PE} and detonation effect P_{DA} on the ground target is. Meanwhile, the damage ability of hard destructive weapons against the ground target, $Ability_{TD}$, becomes stronger until its maximum value (0.97). Subsequently, by increasing B_{reak} and decreasing D_{TBP}, $Ability_{TD}$ first decreases slightly and then quickly levels off. (2) If P_{DA} and P_{PE} are greater than 0, the effective intervals of B_{reak} and D_{TBP} corresponding to P_{PE} are [0.8, 2.0] and [0, 5], respectively, which are greater than the two corresponding to P_{DA}, i.e., [1.13, 2.09] and [0, 1]. Therefore, the penetration effect not only has a relatively better damage effect on the ground target but also contributes more to the corresponding damage ability. In sum, if we properly increase B_{reak} and decrease D_{TBP}, increase the weight of the penetration effect in simulation, and increase the input of such firepower in real measurement, the obtained $Ability_{TD}$ will be greater.

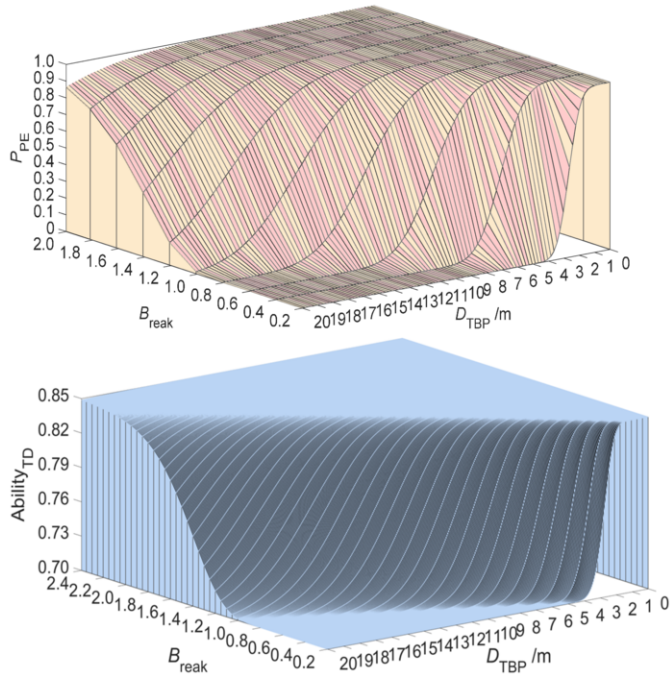

Figure 9. Simulation diagrams of damage ability to a ground target: which includes three simulating surfaces of the relationship between P_{PE} (top), P_{DA} (middle), and $Ability_{TD}$ (bottom) respectively and D_{TBP} and $B_{reak.}$

5.2. Full Physical Tests and Related Results Analysis

In the process of performance detection, the full physical test mainly relies on two types of platforms: One is the full physical static testing platform, which is mainly used for the detection of indicators corresponding to GNSS jamming ability; the other is the full physical dynamic testing platform, which is mainly used for the detection of indicators corresponding to GNSS jamming and user-end defense capability, such as the spoofing success rate. Owing to limitations in the test conditions, the spoofing success rate is taken as an example. Through the full physical dynamic testing platform, we conduct a total of seven tests, and obtain the spoofing positioning accuracy, spoofing success rate, and their average values of each test.

Figure 10 shows that: The average spoofing success rate corresponding to the three directions of the 7th test is the largest, and that corresponding to the three directions of other tests are all stable at approximately 96%. Thus, the spoofing success rate of each test is generally larger because the spoofing device was placed near the targeted receiver during tests. In sum, it is necessary to increase the number of experiments while ensuring that a certain number of tests are included in a single experiment, in order to obtain more objective evaluation results and improve the anti-jamming ability of the targeted receiver.

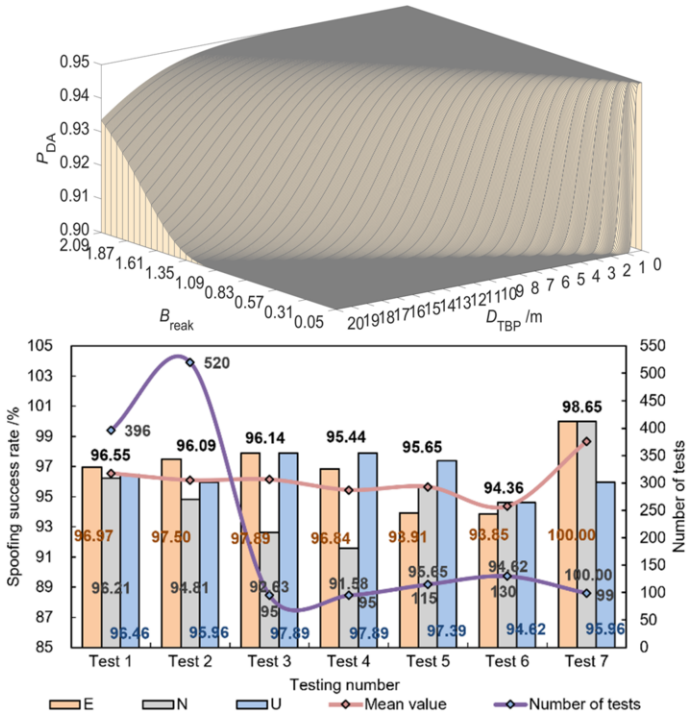

Figure 10. Variation $_{curves}$ of success rate of spoofing corresponding to seven tests.

6. Conclusions and Future Work

In this study, we have proposed and perfected the evaluation models and detection methods of performance indicators based on previous findings; we have performed simulation and tests based on the established test system to analyze the influence law of each performance on the evaluation object executing antagonistic tasks. Relevant results and future work are below.

(1) Decreasing the jamming-to-signal ratio threshold received by the user end, properly increasing the jamming signal wavelength of a jamming source and its transmitting power and transmitting antenna gain, increasing the number of jamming sources, improving the spoofing success rate, and preferentially adopting the GNSS narrow-band jamming can improve GNSS jamming ability.

(2) Increasing the average number of fragments and debris clouds, improving their perforation capacity and specific impulse per unit area, preferably controlling the material ultimate strength of a spatial target, reducing the distance between the detonation point and the ground stations, prioritizing weapons that can produce more spherical fragment and whose generated perforation shape can be arranged in a strip-groove pattern, and preferring to the attack strategy with more penetration effect all can improve the damage effect on the GNSS.

(3) The next-phase research will focus on the efficacy evaluation for GNSS

jamming and anti-jamming, based on the results obtained by this study. By improving the fixed weight model of operational research methods and the optimal algorithms of the game theory, we will analyze the optimal defense measure that decision-makers choose under different antagonistic situations, and then dynamically adjust the defense measure with the change of threatening conditions, in order to expand GNSS benefit.

References

[1] Humphreys T E. Detection strategy for cryptographic GNSS anti-spoofing [J]. IEEE Transactions on Aerospace and Electronic Systems, 2013, 49(2): 1073-1090.
[2] Borio D, Dovis F, Kuusniemi H, Presti L L. Impact and detection of GNSS jammers on consumer grade satellite navigation receivers [J]. Proceedings of the IEEE, 2018, 104(6): 1233-1245.
[3] Shepard D P, Humphreys T E. Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks [J]. International Journal of Critical Infrastructure Protection, 2012, 5(3-4): 146-153.
[4] Wang Y, Sun F P, Hao J M, Zhang L D, Wang X. Reduction research on performance index system of satellite navigation system spoofing [J]. GPS Solutions, 2022, 26(43): 1-21.
[5] Wang Y. Optimal decision for the satellite navigation system under navigation countermeasures based on spoofing effect evaluation results [J]. IET Control Theory & Applications, 2023, 17(11): 1522-1542.
[6] Heng L, Walter T. GNSS multipath and jamming mitigation using high-mask-angle antennas and multiple constellations [J]. IEEE Transactions on Intelligent Transportation Systems, 2015, 16(2): 741-750.
[7] Wang Y, Sun F P, Wang X. Full-domain Collaborative Deployment Method of Multiple Interference Sources and Evaluation of Its Deployment Effect [J]. Defence Technology, 2023, in press.
[8] Ceccato M, Formaggio F, Tomasin S. Spatial GNSS spoofing against drone swarms with multiple antennas and wiener filte [J]. IEEE Transactions on Signal Processing, 2020, 68: 5782-5794.
[9] Psiaki M L, Humphreys T E. GNSS spoofing and detection [J]. Proceedings of the IEEE, 2016, 104(6): 1258-1270.
[10] Wang P, Wang Y Q, Cetin E. GNSS jamming mitigation using adaptive-partitioned subspace projection technique [J]. IEEE Transactions on Aerospace and Electronic Systems, 2019, 55(1): 343-355.
[11] Ioannides R T, Pany T, Gibbons G. Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques [J]. Proceedings of the IEEE, 2016, 104(6): 1174-1194.
[12] Wang Y, Sun F P, Wang X. Construction of the performance index system of navigation confrontation and research on its related evaluation methods [J]. IEEE Transactions on Instrumentation and Measurement, 2022, 71: 3515316.
[13] Chen L W. Research on interference suppression technique in the GNSS receiver under high-dynamic circumstances. Ph.D Thesis: Department of Geomatics Engineering, Wuhan University, 2016.
[14] Jafarnia-Jahromi A. GNSS signal authenticity verification in the presence of structural interference. Ph.D Thesis: Department of Geomatics Engineering, University of Calgary, 2013.
[15] Li H S, Li Y. Target damage distribution probability calculation arithmetic based on space tangential differential unit area [J]. IEEE Sensors Journal, 2015, 15(4): 2274-2279.
[16] Esa M, Amin M S, Hassan A. Relative performance of novel blast wave mitigation system to conventional system based on mitigation percent criteria [J]. Defence Technology, 2021, 17(3): 912-922.
[17] Lomazzi L, Cadini F, Giglio M, Manes A. Vulnerability assessment to projectiles: Approach definition and application to helicopter platforms [J]. Defence Technology, 2022, 18(9): 1523-1537.
[18] Tugnait K J. Pilot spoofing attack detection and countermeasure [J]. IEEE Transactions on Communications, 2018, 66(5): 2093-2106.
[19] Li H S, Zhang X Q, Zhang X W. Calculation model and method of target damage efficiency assessment based on warhead fragment dispersion [J]. IEEE Transactions on Instrumentation and Measurement, 2020, 70: 1001308.