NAIC-ID(RS)T-0587-96

NATIONAL AIR INTELLIGENCE CENTER

SELECTED ARTICLES

Approved for public release: distribution unlimited

HUMAN TRANSLATION

NAIC-ID(RS)T-0587-96 18 February 1997

MICROFICHE NR:

SELECTED ARTICLES

English pages: 27

Source: Unknown

Country of origin: China
Translated by: Leo Kanner Associates
F33657-88-D-2188
Requester: NAIC/TAEC/Frank Scenna
Approved for public release: distribution unlimited.

PREPARED BY:

TRANSLATION SERVICES
NATIONAL AIR INTELLIGENCE CENTER
WPAFB, OHIO

TABLE OF CONTENTS

GRAPHICS DISCLAIMER

All figures, graphics, tables, equations, etc. merged into this translation were extracted from the best quality copy available.

DESIGN OF FLIGHT-PATH OF JAMMING CHECK FLIGHT

Li Jigang and Wu Wei

Air Force Deputy Room
Shanghai Bureau of Astronautics

ABSTRACT: This paper presents methods for designing the flight-path of SOJ (stand-off Jamming) check flight, practical formulas, related problems, and design examples using the SOJ equation. The burn-through distance can be optional in accordance with the selection of check flights, thus solving the problems of using high-powered jammers in low-power radar in check flight.
KEY WORDS: active jamming, radar, flight-path of jamming check flight, flight-path design.

1. Introduction

Jamming check flight, as one of the approaches in examining the anti-jamming performance of a radar, can be carried out in two ways: deliberate check flight and hostile check flight. The former is performed on the condition that the parametric indicators of a jammer and a radar are both known, while the latter is based on the principle that we (the parameter indicators of the radar) will change as the enemy (parameter indicators of the jammer) changes, or the enemy will changes as we change. Deliberate check flight is held to be more suitable

for the newly developed radars.

With respect to a radar, active jamming can be classified into two categories, namely blanket jamming and deceptive jamming, while in terms of tactical means, active jamming can be divided into long distance stand-off jamming (SOJ), escort support jamming (ESJ), and self-support jamming (SSJ). Normally, during actual battles, these two categories of jamming and the related three tactical means are used alternatively. However, only one category and one tactical means are allowed in the jamming check flight for the new radars.

This paper primarily describes the flight path design of target aircraft and jamming aircraft (jammer carrier) for a check flight intended to examine a radar's anti-jamming performance using SOJ tactical means and blanket jamming. When the parametric indicators of blanket jamming and radar performance are both determined, the design of the flight path of the check flight becomes a crucial issue and is directly related to whether or not the SOJ jamming check flight can achieve success.

2. Requirements for Flight Path of Check Flight

Generally speaking, personnel wish to observe and detect the fact that by means of only a single jamming check flight, a radar fails to discover, track, and process a target due to the blanket jamming effect, i.e.,, through the test a blanket zone can be derived. On the other hand, they also desire to see whether the radar can "burn through" the blanket jamming so that it can discover, track, and process a target, i.e.,, through the test an exposure zone be derived.

To achieve these goals, the jam-to-signal ratio (P_{st}/P_{j}) received by the radar in the check flight is required to change with the in-flight displacement of the target aircraft and

jamming aircraft relative to the radar coordinate points. For conventional radars without special jamming countermeasures, the target aircraft is located in the blanket zone when $P_{st}/P_{jr} < 1$, and the target aircraft is situated in the exposure zone when $P_{st}/P_{jr} > 1$; while $P_{st}/P_{jr}=1$, the target aircraft is located at the demarcation between the two zones.

For instance, if the detection distance of a radar is 100km, the target aircraft is required to be located in the blanket zone at the distance of 50~100km so that the effectiveness of the various jamming countermeasures of the radar can be tested; additionally, the target aircraft is required to be located in the exposure zone at the distance of 10~50km so as to test the target detection, tracking, and processing (such as TWS) capabilities of the radar under a jamming background. When the target aircraft is flying toward the radar in a radial direction, the flight path of the jamming aircraft should be designed based on the tactical means requirement and jamming power so that the foregoing requirements can be met.

3. Calculation of Blanket Zone and Exposure Zone

The typical stand-off jamming equation is as follows:

$$R_t = \frac{1}{4\pi} \cdot \frac{P_t}{P_j} \cdot \frac{G_t}{G_j} \cdot \frac{G_t}{G_j'} \cdot \frac{B_j}{B_s} \cdot \frac{1}{L_s} \cdot \frac{1}{L_j} \cdot \frac{1}{M} \cdot C \cdot \sigma \cdot R_t^2 \qquad (1)$$

where R_t is the distance between target aircraft and radar; R_j is the distance between jamming aircraft and radar; P_t and P_j are the average transmission power of radar and of the jamming aircraft; G_t and G_j are the antenna main-lobe gain of the radar and the jamming aircraft; G'_t is the gain of radar antenna along the jamming direction; B_s and B_j are the radar receiver bandwidth and the jammer bandwidth; L_s is the total loss of radar receiving and transmitting system; L_j is the polarization loss of the circularly polarized jamming signal at the linear polarized

antenna of the radar; M is the jam-to-signal ratio which is equal to P_{st}/P_{jr}; C is the anti-jamming improvement factor of radar, which is greater than 1 when the jamming countermeasures are effective, or otherwise, it is equal to 1; σ is the effective radar reflection area of the target aircraft.

For the convenience in calculation, the right-hand side of Eq. (1) can be combined into a constant term K except for the term R_j^2, and Eq. (1) can be rewritten in decibel (dB) form as follows:

$$R_t = \lg^{-1}[(K+2R_t)/40] \tag{2}$$

By introducing the technical indicators of radar and jamming aircraft in Eqs. (1) or (2), an expression indicating the correlation between R_t and R_j can be derived. Based on this expression, the data regarding the correlation between R_t and R_j can be computed (see Table 1) and plotted into a curve (Fig. 1).

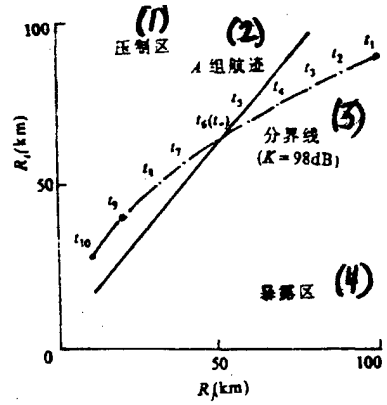

Fig. 1. Demarcation curve in transition from blanket zone to exposure zone
KEY: (1) blanket zone (2) flight path of group A (3) demarkation line (4) exposure zone

TABLE 1. Demarcation Points of Transition from Blanket Zone to Exposure Zone

$K = 98dB$										
t	t_1	t_2	t_3	t_4	t_5	$t_6(t_n)$	t_7	t_8	t_9	t_{10}
R_j(km)	100	90	80	70	60	50	40	30	20	10
R_t(km)	89	85	80	75	69	63	56	49	40	28

The data in Table 1 are demarcation points in the transition from blanket zone to exposure zone. In Fig. 1, the lower half of the curve is the exposure zone, while the upper half is the blanket zone. The demarcation line as well as the exposure zone and blanket zone will change if any of the parameters in Fig. 1 changes in value.

In the case when the radar antenna gain changes with elevation, it should be corrected each time when a demarcation point is calculated. When the jamming aircraft is located at a certain position R_j, the following scenario will occur: in the entire radar detection range, the energy of the return wave from the target is fairly low while the energy of the jamming signal is extremely high, and there is no exposure zone. Once this scenario occurs, a test should be conducted based on the energy scaling principle, i.e.,, reducing the jamming energy of the jamming aircraft so that the blanket zone and exposure zone will appear in the radar detection range. Hence, the anti-high power jamming effect of the radar can be computed owing to the positions of the demarcation points measured in the check flight, as well as the radar performance indicators and the performance indicators of the jamming aircraft after being scaled.

4. Design of Flight Path

In this paper, flight path refers to the positions of the point paths (azimuth, distance, and altitude) of the target

aircraft or jamming aircraft in order of time. Practically speaking, to design a flight path involves designing, based on the requirement for the range segments of the blanket zone and exposure zone, the positions of the point paths of the target aircraft and the jamming aircraft at the same instant, and to connect these positions in order of time to form a flight path for use in jamming check flight.

a. Selection of Elevation and Mounting Angle of Jamming Antenna

The altitude of a target aircraft is chosen from the typical target parameters given in the radar tactical display. While the altitude of a jamming aircraft is normally equal to or slightly greater than the altitude of a target aircraft so that the two aircraft can keep flying at an equal altitude within the distance range of the jamming check flight.

Generally speaking, the antenna radiation pattern of a jamming aircraft is omnidirectional in azimuth, and is directional at elevation. With change in the distance between jamming aircraft and radar, the gain of its antenna pointing toward the radar changes as well, i.e., the G_j value in Eq. (1) changes. Technically, it is desired that within the distance range of the check flight, the change of G_j value falls within a beam width range of 3dB. If it exceeds this range, the mounting angle of the jamming antenna should be re-designed and re-adjusted, which is to be considered in the design of the flight path of a jamming check flight to a radar, where the gain G_t in the vertical radiation pattern changes with elevation.

b. Selection of Azimuth

There should be no ground object clutter at the flight azimuth of the target aircraft and jamming aircraft, and the

shadowing angle should be smaller than 0.5^0. When the target aircraft is flying in a straight line toward the radar, the short-cut of the flight path should be smaller than ±1km. The following two factors should be taken into account in designing the flight direction of the jamming aircraft:

(a) Based on calculation using Eq. (2), if the blanket zone and exposure zone can be distinguished when the target aircraft and jamming aircraft located at different distances are flying toward a radar along the same azimuth level (i.e., the two aircraft are simultaneously located in the main lobe of the radar antenna), then the flight azimuth of the jamming aircraft should be selected the same as that of the target aircraft, i.e., the jamming aircraft flies toward the radar following the target aircraft, with an azimuth error not surpassing the 3dB width of the main lobe of radar antenna.

(b) If the blanket zone and exposure zone cannot be distinguished as mentioned above, then the flight azimuth of the jamming aircraft should be selected as the azimuth of the first parasitic lobe or some other parasitic lobe of the radar antenna [depending on the calculations of the demarcation point in Eq. (1)], i.e., the target aircraft is in the main lobe of the radar antenna and the jamming aircraft is in its parasitic lobe at the same instant. This kind of flight path is designed to check the radar anti-jamming performance in the case when jamming enters through the parasitic lobe of the radar antenna, which often occurs with SOJ.

c. Selection of Range

Through calculations based on Eq. (1) the elevation and azimuth of the point path, i.e., the antenna gain $G_t G'_t G_j$, as well as other parameters in Eq. (1), the result as shown in Fig. 1 can be obtained. Then, from Fig. 1, various ranges of the target

aircraft and jamming aircraft at the same instant are selected so that the target aircraft is located in the blanket zone at the far distance of the range of the check flight, and it is located in the exposure zone at the near distance of the range segment of the check flight.

The length of the flight range of the target aircraft in the exposure zone is required to basically ensure that the TWS system of the radar has enough time to build up a target flight path and generate the batch number. This requirement can be met with several flight paths, of which one path can be selected for a trial design in consideration of other requirements.

The point paths of the target aircraft and jamming aircraft at different instants, respectively, are connected in order of time and, respectively, are timed, which, in fact, concludes the theoretical design of the flight path of the check flight. These theoretical flight paths are marked in a military-oriented map with an appropriate scale in which the geographical coordinates of the radar have already been determined. When this is done, the flight velocity of the two aircraft can be derived through the time sequence and their positions relative to the radar.

The next step is to check whether or not a particular aircraft can satisfy the requirement from the theoretical flight path. After correction, the flight path available for actual manned flight, or unmanned remote controlled flight can be derived. Additionally, this flight path must basically satisfy all the above-mentioned requirements. Only in this way can the design of the flight path of check flight be considered to be finalized. Evidently, this kind of design needs repeated correction and iteration and therefore, can hardly be accomplished at one time.

5. Design Example

The concept and methodology of the foregoing design can be further detailed in one example.

5.1. Goal and Requirements

a. Goal: The goal of the design is to verify the anti-jamming capabilities of a radar when its parasitic lobe is subject to blanket jamming.

b. Requirements: The distance range of the flight check should be 10~100km, of which the exposure zone and blanket zone, respectively, account for approximately 1/2.

5.2. Given Conditions

a. A constant K=98dB can be derived through merging of the related parametric values of the radar and the jamming aircraft as shown in Eq. (2);

b. The included angle between the main lobe and the first parasitic lobe of radar antenna should be 8^0;

c. The azimuth of the radar position is 90^0~120^0, in which there is no ground object, and the shadowing angle is less than 0.5^0;

d. The beam width in elevation of the jamming aircraft antenna is no less than 50^0;

e. The altitude of the target aircraft is 8000m.

5.3. Assumptions

To illustrate the major steps, it is assumed that:

a. With the very wide beam of the jamming aircraft antenna, the mounting angle can meet the requirement for the range segment of the check flight;

b. The vertical beam gain change of the radar antenna can be ignored;

c. The effect of the short-cut of the flight path and its error on the demarcation point calculation can be ignored.

5.4. Initial Design

a. Based on one of the given conditions, calculating the data corresponding to R_t and R_j using Eq. (2) and inserting them in Table 1.

b. Plotting the demarcation curve between the blanket zone and exposure zone in accordance with the data listed in Table 1 (see Fig. 1).

c. Based on the conditions that the blanket zone and exposure zone, respectively, account for 1/2 of the range of the check flight, select R_j as equal to 50km, find the corresponding demarcation point (t_n) on the demarcation curve, and draw at random straight line A with positive slope, which passes through the demarcation point. Then all the points at line A can satisfy the requirement (Fig. 1). If t_n:R_j=90km, and R_t=108km, the target aircraft is located in the blanket zone, while T_g:R_j=30km, and R_t=39km, the target is in the exposure zone. Set up Table 2 indicating the correlation between R_j and R_t, represented by the straight line A, in order to finalize the initial design of the flight path of group A of the jamming aircraft check flight. In this case, the flight path of the jamming aircraft is referred to as flight path A_1, while the flight path of the target aircraft is called flight path A_2. Similarly, another segmented line B can be drawn, from which a group of new data corresponding to R_j and R_t can be derived to design the flight path of group B.

TABLE 2. Correlation Between R_j and R_t

(1) 分界点t_6(R_p = 50km, R_m = 71km)												
(2) 时序			t_1	t_2	t_3	t_4	t_5	$t_6(t_n)$	t_7	t_8	t_9	t_{10}
(3) A组航迹	A_1	β_j	100	100	100	100	100	100	100	100	100	100
		R_j	100	90	80	70	60	50	40	30	20	10
	A_2	β_t	108	108	108	108	108	108	108	108	108	108
		R_t	120	108	97	86	74	63	51	39	27	16

KEY: (1) demarcation point (2) time sequence
(3) flight path of group A

5.5. Plotting of Flight Path Diagram

After the position of the radar is marked, in accordance with the included angle between the main lobe and parasitic lobe of the radar antenna as well as the required azimuth angle, β_j=100° is selected as the jamming aircraft entry azimuth angle, and also, β_t=108° is selected as the target aircraft entry azimuth angle. Based on Table 2, the initial point of flight path A_1 (β_j=100°, R_j=100km) and the initial point of flight path A_2 (β_t=108°, R_t=120km) at time t_1 can be marked. Similarly, all the flight paths during the range of the jamming check flight can be marked in order of time with the same procedure (diagrams are omitted).

Acknowledgement: Thanks are due to Meng Wei and Wang Zheli for their assistance in this research project.

This paper was received on March 17, 1996.

JAMMING OF GLOBAL POSITIONING SYSTEM

Liang Baichuan

Xi'dian University

ABSTRACT: This paper introduces signal intercepting and measuring methods for the Global Positioning System (GPS), discusses basic ways of implementing electronic jamming of GPS receivers, and analyzes the modes and effects of electronic jamming of GPS. The analysis results show that applying individual jamming to GPS can obtain good jamming effects.
KEY WORDS: global positioning system, personal jamming, jamming mode, jamming effect, direct array spread-spectrum.

1. Introduction

A complete global positioning system (GPS) is primarily composed of three parts: satellites for transmitting navigation positioning information, a ground control designed for normal and reliable operation of the system, and the user receiver[1].

At present, GPS is partially open to the public. Technically speaking, this system, by using a direct array spread-frequency modulation technique as well as pseudo-random codes with two rates: 10.23 and 1.023MHz, can modulate and

transmit 50B/s of navigation positioning information at two frequencies L_1 and L_2.

In peacetime, frequencies L_1 and L_2 are open to public: L_1=1575.42MHz and L_2=1227.6MHz. The signal at L_1 is the non-balance QPSK modulated as shown in Fig. 1. The pseudo-code array at channel I is the Gold code (i.e., C/A code) with length 1023bits and rate 1.023MHz. Transmission and reception among various satellites are identified through the code division identification process. The pseudo-code array at channel Q is a nonlinear code with rate 10.23MHz, called P code. The L_2 frequency can only be used to transmit the P code through P-code spread-frequency BPSK modulation.

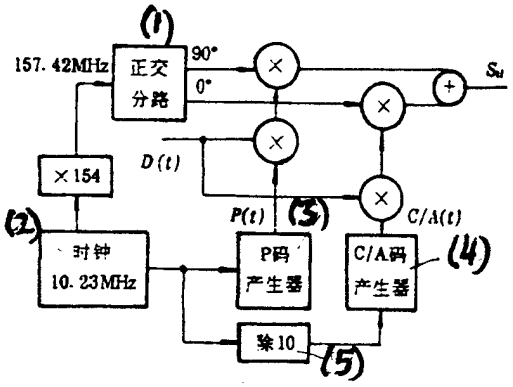

Fig. 1. Structure of GPS L_1 frequency signal modulation
KEY: (1) orthogonal shunt circuit (2) clock
(3) P code generator (4) C/A code generator
(5) divided by 10

Therefore, the navigation positioning signal transmitted by the satellite can be expressed as

$$\begin{cases} S_{L1} = A_P D(t) P(t) \cos 2\pi f_1 t \\ \quad + A_C D(t) C/A(t) \sin 2\pi f_1 t \\ S_{L2} = B_P D(t) P(t) \cos 2\pi f_2 t \end{cases} \tag{1}$$

where A_P, B_P and A_C are the relative amplitudes; f_1=1575.42MHz,

f_2=1277.60MHz; and D(t) is modulated signal.

By encrypting the P-code signal, a Y code can be generated, which has anti-deception capabilities. The U.S. Department of Defense decided to implement selective availability (SA) and anti-electronic deception (A-S) policies once GPS is brought into practical use.

So-called selective availability refers to a process of introducing errors in unapproved user pseudo-range measurements through manually changing the navigation message data or making the in-satellite clock frequency dither during signal transmission, as well as transmitting the encrypted coded calibration parameters, while allowing approved users to avoid the SA-introduced errors with special software or hardware.

The A-S technique is employed for anti-electronic deception jamming countermeasures by encrypting the P code so as to form the Y code. As long as the P code user receiver is equipped with an additional Y code output chip, it can be prevented from being deceived by the enemy's false P code designed to reduce the reception accuracy. The A-S can be connected or disconnected depending on the needs of the Defense Department.

2. Interception and Detection of GPS Signals

To effectively jam the GPS, it is necessary to understand the change of GPS signal parameters, and to discover and identify whether this system is present.

With the direct array spread-spectrum modulation technique, the GPS system can transmit signals with a low acquisition probability, which are virtually drowned in noise and therefore can hardly be detected with conventional detection means. Hence, the detection of GPS signals becomes an extremely complex issue,

for which an effective approach is yet to be created thus far. Here, we discuss only several GPS signal detection methods which are based on modern spectrum estimation techniques[2-4].

Suppose the signal at the receiving end of GPS reconnaissance equipment is:

$$x(t)=\sqrt{2S}P(t)D(t)\cos[2\pi f(t)t+\varphi(t)]+n(t) \tag{2}$$

where S is signal power;

P(t) is spread-frequency modulated random code;

D(t) is data code;

n(t) is Gaussian white noise with a single sideband power spectrum density N_0

f(t) is carrier wave frequency;

φ(t) is initial phase.

2.1. Energy Detection Method

At present, this is the classical method for energy detection. The fundamental concept of this method lies in the fact that when the energy of signal plus noise is higher than the noise energy, it indicates the presence of a signal. Fig. 2 shows a typical energy detector.

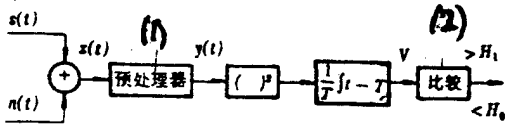

Fig. 2 Principle of energy detector
KEY: (1) preprocessor (2) comparison

When n(t) is Gaussian white noise, the output of the detector can be approximated with the square sum of a limited number of samples within observation interval T. When the detected value U is smaller than the threshold, H_0 is selected,

while when it is larger than the threshold, H_1 is selected. Analysis suggests that the mean value of this set of samples at H_0 is zero, their variance is equal, and they are statistically independent.

The detected value V derived on this basis is in central X^2 distribution. Under H_1, V obeys non-central X^2 distribution so that the detection probability and false-alarm probability of the detected energy value can be solved. This method is rarely used directly because its detection threshold cannot be determined.

2.2. Correlation Spectrum Estimation Method

With the self-correlation spectrum estimation method, the number of random sample values N of the spread-frequency signal S(t) can be calculated using a high speed FFT technique. This method features fast operation, fairly simple algorithm, and ideal spectrum estimation property in the case when the signal-noise ratio is greater than zero decibel. A shortcoming of this method is that its frequency spectrum estimation property deteriorates under signal-noise ratio α (<0dB).

2.3. Mutual Correlation Orthogonal Shunt Circuit Detection

This detection method, based on code domain correlation theory and the time domain shunt circuit correlation detection mechanism, can effectively reduce the detection threshold of the direct array spread-spectrum signal to below a signal-noise ratio below -20dB.

The basic concept of the mutual correlation orthogonal shunt circuit detection suggests that the pseudo-random code with a limited length has a cluster of correlated code groups, which, with a mutual correlation side lobe being higher than the mutual correlation peak value of the optimal array, are favorable for

enhancing the signal energy. This feature, coupled with the independence of noise and correlativity of signals in shunt circuit correlation detection, can lead to a greater detection gain and thus can effectively reduce the detection threshold.

2.4. Cepstrum Detection Method

The cepstrum detection method takes advantage of the periodicity of pseudo-code components in frequency domain as well as the pseudo-code periodicity in the direct array spread-spectrum signal. With this method, when the discrete component is drowned in a continuous quantity, the discrete component can be increased using logarithmic operations. The structure of the cepstrum detector is shown in Fig. 3.

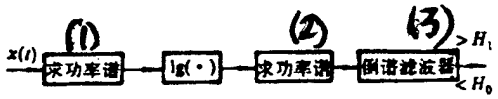

Fig. 3 Structure of cepstrum detector
KEY: (1) solve power spectrum (2) solve power spectrum (3) cepstrum filter

Analysis indicates that when the noise is Gaussian white noise, the output of the cepstrum detector is composed of the following four signals: noise at 0; pulse reflecting the signal power amplitude; a low-frequency pulse reflecting the signal power spectrum envelope characteristics; and a high-frequency pulse reflecting the signal pseudo-code periodic frequency. With a cepstrum filter, signal detection can be realized.

2.5. Automatic Regression Moving-Average (AKMA) Detection

The AKMA simulation method is a signal modeling method, or pole and zero modeling method, integrating the automatic regression (AR) method and the moving-average (MA) method. The AKMA model, even closer to a spread-spectrum signal model, has

fairly ideal spectrum estimation capabilities, i.e., it can provide not only a high estimation accuracy at a small signal to noise ratio, but also a higher spectrum resolution. The simulation result suggests that the AKMA algorithm can distinguish two spread-spectrum signals.

2.6. Pre-filtering Delay Multiplication Detection

A direct spread-spectrum signal features a pseudo-continuous spectrum at a particular pseudo-code array, i.e., its frequency spectrum consists of two parts: continuous spectrum and discrete spectrum. Once the discrete spectrum is detected, the presence of a signal can be determined.

However, it is difficult to detect the discrete spectrum directly from the received signal spectrum. In this case, through delay multiplication correlation, the discrete component from the output signal--the pseudo-code rate and its component at its harmonic wave can be output.

By taking advantage of the output of the pre-filtering delay multiplication (PFDM) detection, the ratio between the square value of the Fourier series K-level coefficient amplitude at the pseudo-code rate and the power spectrum density amplitude at its K-times fundamental frequency neighborhood (called the performance factor) can be detected, by which we find out whether or not a signal can be determined.

3. Basic Modes and Approaches in Implementing Electronic Jamming

At present, GPS as an advanced navigation system for both military and civilian applications is shifting toward the practical-use stage. With the SA technique, this system makes it difficult for the enemy to derive high- precision positioning parameters. And at the same time, the A-S technique is adopted

for deceptive jamming countermeasures.

With the wide application of GPS, some new SA and A-S techniques are likely to emerge in the future. Furthermore, through an analysis of GPS working principle and features, it can be seen that implementing electronic jamming to its receiver can be possible[1]. The following lists several GPS features that are, in fact, its disadvantages in taking jamming countermeasures:

a. Use of fixed frequency. Since the satellite transmits data at dot frequency with high stability, the power can be concentrated in the narrow band while jamming is being performed.

b. Unchanged data format. Data transferred on the basis of synchronous code are easy to be intercepted and identified. Additionally, jamming can be implemented by guiding the GPS receiver.

c. In order for the receiver to track several satellites above the horizon, the radiation pattern of the receiving antenna is made in a hemispherical form, and besides, the parasitic lobe level of a miniature antenna at that waveband is fairly high (approximately -3~15dB). In this case, a large air domain is vulnerable to jamming.

d. To receive weak signals, the sensitivity of the GPS receiver ranges from -115 to 135dB. Hence, a not-so-large jamming power is sufficient for signal processing to reach a required jamming-signal ratio.

e. Jamming still can be implemented to the receiving processor even after the A-S technique is analyzed and deciphered.

4. Jamming Tolerance of GPS Signal

The so-called jamming tolerance of GPS signal refers to its working ability in a jamming environment. Since GPS employs the direct array spread-frequency technique, its jamming tolerance

can be expressed with a corresponding formula as follows:

$$M_j = G_p - [L_s + (S/N)_0] \quad (3)$$

where G_p is the processing gain of GPS receiver;

L_s is the correlator loss of receiver;

$(S/N)_0$ is the output signal-noise ratio of correlator.

The processing gain of the C/A code GPS receiver is approximately 43dB, while the typical correlator loss of receiver is normally within the range 1.5~2.5dB. And to ensure phase tracking of the loop so as to demodulate the 50B/s navigation positioning information, $(S/N)_0$ is required to be approximately 16dB. Thus, the jamming tolerance of the GPS receiver is around 25dB. This tolerance is the only tolerance required before the receiver captures and tracks signals; once the carrier wave ring and code ring of the receiver are in a lock-in state, its processing gain may reach 50 or even 53dB with the decrease in the bandwidth of the loop. Therefore, in the state of tracking, the jamming tolerance will be 32 or even 35dB. With the jamming tolerance M_j, it will be easy to calculate the anti-jamming threshold of GPS signal M_{AJ}, given the input level of GPS receiver.

$$M_{AJ} = P_r + M_j \quad (4)$$

where P_r is the signal level at the input end of the GPS receiver.

The anti-jamming threshold M_{AJ} shows that the GPS receiver can no longer operate in normal conditions once it reaches M_{AJ} in receiving jamming signal. Obviously, the jamming level at the input end of GPS receiver P_{jr} should be:

$$P_{jr} > M_{AJ} \quad (5)$$

5. Analysis of Jamming of GPS

By taking advantage of the ideal self-correlation and mutual correlation properties of the pseudo-code and using code-

division-multiple access mode, GPS can refuse to receive unnecessary signals from the satellite, and can separate the signals received simultaneously from different satellites. The way this is done is to assign C/A code and P code with different structures to different satellites. Suppose P_s is the power of the satellite signal to be received; G_s is the gain of the satellite transmitting antenna; P_j is the personal jamming power; G_j is the gain of jamming transmitting antenna, then the signal-jamming-power ratio output by the related receiving circuit can be approximated as:

$$(\frac{S}{N_j})\approx\frac{P_sG_s}{P_jG_j}\frac{\Delta f}{\Delta F} \qquad (6)$$

where Δf is pseudo-code signal bandwidth;
ΔF is coding pulse signal bandwidth;
$\Delta f/\Delta F$ is spread-frequency gain, and $\Delta f/\Delta F=G_p$.

For P(t) code, its code rate is f_1=10.23MHz, its symbol width is $T_p=1/(10.23\times10^6)$s, and its bandwidth is $\Delta f=1/Tp=10.23$MHz.

For C/A code, its code rate is f_2=1.023MHz, its symbol width is $T_b=1/(1.023\times10^6)$s, and its bandwidth is $\Delta f=1/Tp=1.023$MHz.

For coding pulse D(t), its code rate is 50Hz, its symbol width is T_b=20ms, and the coding pulse signal bandwidth is $\Delta F=1/T_b=50$Hz.

Thus, the $\Delta f/\Delta F$ value for P code and C/A code, respectively, is 2.046×10^5 and 2.04×10^4.

The following is an estimation of the correlation between GPS jamming range and jamming power, based on GPS receivers of the ground vehicle-born or ship-born jammer and jamming early warning aircraft:

$$\left(\frac{R_s}{R_j}\right)^2=\left(\frac{\Delta f}{\Delta F}-M_j\right)\left[\frac{P_sG_s}{P_jG_j}\right] \tag{7}$$

where R_s=20000km; R_j=200km; P_s=300W; G_s=20dB; G_j=5dB; spread-frequency gain $\Delta f/\Delta F$, respectively, is 53dB and 43dB for P code and C/A code; M_j is jamming tolerance. To reflect the requirement for the output signal-noise ratio of the spread-frequency receiver and to consider the signal-noise ratio loss inside the system (including radio frequency filter loss, correlation processor fixed frequency loss, signal-noise ratio loss of the amplifier, etc.), M_j is generally evaluated as equal to 13dB, i.e., $(\Delta f/\Delta F-M_j)$ is 40dB for P code and 30dB for C/A code.

The jamming power is calculated as

$$P_j=\left(\frac{\Delta f}{\Delta F}-M_j\right)\frac{P_sG_s}{G_j}\left[\frac{R_j}{R_s}\right]^2 \tag{8}$$

for P code

$$P_j=10^4\times\frac{30\times100}{3.16}\times\left[\frac{200}{2\times10^4}\right]^2$$
$$\approx950(\mathrm{W})$$

and for C/A code

$$P_j\approx10^3\times\frac{30\times100}{3.16}\times\left[\frac{2\times10^2}{2\times10^4}\right]^2$$
$$\approx95(\mathrm{W})$$

6. Analysis of Jamming Modes to GPS

To jam direct spread-frequency modulated signals, aiming-mode jamming, and interception mode jamming are generally accepted. Western countries started to work on new jamming techniques while developing new-generation spread-frequency and jump-frequency modulation techniques, such as high-speed response jamming, partial-frequency-band noise jamming, continuous multitone-filtering jamming, as well as retransmission jamming based on the focal variation filter and the mode-direction filter group technique.

The GPS P code signal is a long pseudo-code array direct-spread signal, while its C/A code signal is a short pseudo-code array direct-spread signal. The transmission of navigation data is realized through sampling and conversion to the corresponding symbol characters. Hence, jamming can be successfully implemented as long as a particular jamming technique is used to increase the error rate at the receiving end of GPS system causing the articulation of the de-spread data to worsen[2].

6.1. Correlation Jamming

Correlation jamming is achieved through the pseudo-code modulation jamming system. To make the optimal correlation jamming possible, it is needed to study the pseudo-code array of jamming, which can generate the maximum correlation value with the pseudo-code array of the signal. If the array has a higher mutual correlativity, then through correlation reception, the average-phase jump frequency of its output signal will slow down, and the jamming energy will concentrate at the central frequency, while the jamming energy passing through the narrow-band filter of the receiver will enhance, resulting in a better jamming effect.

For effective jamming, the jamming power required can be reduced. From an analysis of the concept of the optimal jamming, the optimal jamming parameters are as follows:

a. Jamming carrier frequency and signal carrier frequency are aiming at each other;

b. Pseudo-code rate of the jamming signal should be close to the pseudo-code rate of the signal;

c. Pseudo-code array of the jamming signal should be correlated to the pseudo-code array of the signal, and the correlation is required to reach its maximum value.

6.2. Single-frequency (Narrow Band) Jamming

When the single-frequency jamming or narrow-band jamming, transmitted from the GPS jammer, enter the GPS receiver, the local fast pseudo-code array is modulated into a wide-band jamming signal through frequency mixing. Fig. 4 shows the correlation between the jamming parameter b and jamming/signal bandwidth ratio, while Fig. 5 shows the correlation between the jamming parameter b and jamming-signal carrier frequency deviation coefficient.

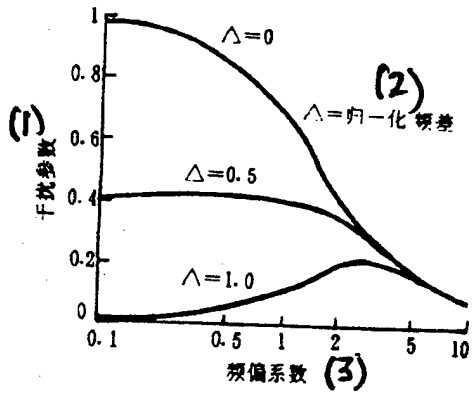

Fig. 4 Correlation curves between jamming parameter and jamming-signal frequency deviation coefficient
KEY: (1) jamming parameter (2) normalized frequency difference (3) frequency deviation coefficient

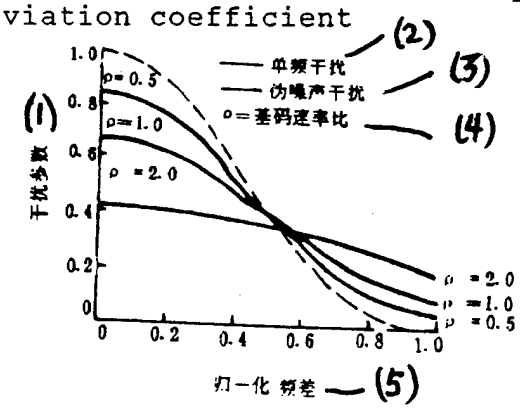

Fig. 5 Correlation curves between jamming parameter and jamming-signal bandwidth ratio
KEY: (1) jamming parameter (2) single-frequency jamming (3) pseudo-noise jamming (4) fundamental code rate ratio (5) normalized frequency difference

It can be seen from the figures that for the direct array spread-frequency signal system, the single tone jamming aiming at central frequency (or its vicinity), multitone jamming, narrow-band noise frequency modulation jamming, and narrow-band noise phase modulation jamming can all achieve a larger jamming parameter b. While the error rate of the direct array spread-spectrum receiver in a single tone jamming environment is

$$P_e=\frac{1}{2}\mathrm{erfc}\left[\frac{bP_j}{G_pP_s}+\frac{N_0}{E_b}\right]^{-\frac{1}{2}} \tag{9}$$

where G_p is processing gain, and $G_p=T_b/T_p=W/B=\Delta f/\Delta F$;

W is pseudo-code bandwidth;

B is data code bandwidth;

$N_0/2$ is power spectrum density of thermal noise;

E_b is energy received in each bit, and $E_b=A^2T_b/2$;

erfc(x) is Gaussian error integration, and

$$\mathrm{erfc}(x)=\frac{2}{\sqrt{\pi}}\int_0^{\infty}\exp(-y^2)\,dy$$

Through calculations, the related curves of jamming parameter b can be derived as shown in Fig. 5, where Δ is jamming carrier frequency and signal carrier frequency deviation coefficient; ρ is the ratio between jamming bandwidth and spread-frequency bandwidth.

6.3. Blocking Jamming

Blocking jamming can be applied when the pseudo-code array cannot be understood. With a sawtooth wave wide-band frequency modulation and noise narrow-band frequency modulation jamming system, each blocking jammer can transmit a wide-band and uniform jamming frequency spectrum. Owing to its unique features, the blocking jamming is capable of jamming all the signals within this jamming frequency band, and implementing jamming to all the satellite signals simultaneously that can be received in this region.

6.4. Jamming Effects

The following jamming effects can be generated to the GPS receiver:

a. The GPS receiver completely fails to receive satellite navigation signals, and even is damaged or paralyzed permanently.

b. The GPS receiver is wrongly locked at a jamming signal and cannot execute positioning because "false" satellites occur.

c. GPS flight path displays interruption, and the target data memorized are the data recorded before the jamming, and errors occur in the target indicating data.

d. GPS data processing becomes confusing. Even if the jammer is closed, the GPS receiver still cannot restore to normal condition in a fairly long time and cannot receive any signal.

7. Conclusions

The foregoing analysis indicates that with the manual jamming method implemented to the GPS system, better jamming effects can be derived, i.e., GPS fails to perform positioning and navigation assignments. However, it is to be noted that considering the possibility of the combined service of GPS and GLONASS (Commonwealth of Independent States) in the future, it is needed to implement overall and effective jamming not only for GPS, but also for GLONASS. Under such circumstances, the jamming of navigation and positioning systems will be facing an even greater challenge.

REFERENCES

1 徐穆洵. 导航星全球定位系统的电子对抗. 电子对抗, 1993;3

2 Torrieri Don J. Principles of military communication systems. Artech House, Inc. 1981

3 Kuehls J F, Geraniots E. Presence detection of binary phase-shift keyed and direct-sequency speread-spectrum signals using a prefilter-delay and multiply device. IEEE Journal ON SAC, 1990;18(5)

4 马宝宝, 戴庆源. 对扩频通信系统侦察干扰的新方法. 航天电子对抗, 1994;3

This paper was received on March 17, 1996.