IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 30, 2019, accepted January 5, 2020, date of publication January 10, 2020, date of current version January 23, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2965728

Dynamic Evaluation of GNSS Spoofing and Jamming Efficacy Based on Game Theory

YUE WANG, JIN-MING HAO, WEI-PING LIU, AND XIAN WANG
National Digital Switching System Engineering and Technological Research Center, Zhengzhou 450001, China
Corresponding author: Yue Wang (2895771372@qq.com)

ABSTRACT The evaluation of the effectiveness of global navigation satellite system (GNSS) spoofing and jamming equipment is not only an important means of enhancing the power of modern satellite navigation countermeasures, but also a dynamic decision-making problem, whose complexity manifests as the uncertainty of information used to make decisions (e.g., fuzziness, randomness, and dynamics). Previously, full consideration was given to the dynamics of decision information, as well the fuzzy, stochastic problems of quantitative and qualitative data when integrated with subjective and objective information. In this study, first, a spoofing mode index was established based on the performance analysis results of the spoofing equipment and target receivers during antagonized navigation. Second, a combined interval number eigenvalue method (IEM) algorithm with ternary association numbers, and entropy-weighting of the interval were used to combine weights, while considering the uncertainty of judged index weights and their subjectivity. Using a fuzzy comprehensive assessment of the interval and the superposition of multiple expert-derived joint scores, a profit matrix was constructed and solved using game theory to reveal the advantages of this approach in dealing with dynamic problems. Finally, the uncertainty of decision information was fully considered by applying the proposed method to practical application and dynamic analysis.

INDEX TERMS GNSS spoofing and jamming equipment, spoofing mode index, game theory, combination weighting, interval-valued fuzzy comprehensive assessment, interval number eigenvalue method.

I. INTRODUCTION

The degree to which the global navigation satellite system (GNSS) spoofing and jamming equipment can achieve the expected goals during a spoofing task can be determined by evaluating the efficacy of the equipment. The scientific and accurate evaluation of the spoofing equipment can not only enhance the countermeasure capabilities of modern satellite navigation information, but also help manufacturers improve the core performance of the equipment on demand [1]. Additionally, the evaluation process is also a complex and dynamic decision-making problem [2], which primarily manifests in the uncertainty of decision-making information, (e.g., fuzziness, randomness, and dynamical behavior). Among them, the uncertainty of decision-making information is derived from: (1) changes in target receivers and unmanned aerial vehicles (UAVs), which are hereafter referred to as ''target machine (working systems)'', (2) the indeterminacy of the spoofing modes of equipment, (3) electromagnetic environment, (4) diversity of evaluation indices, (5) lack of ''true'' data, (6) differences among ''expert'' judgments, and (7) multidimensionality of evaluations. Therefore, evaluating the effectiveness of the decision-making information of GNSS equipment poses a problem with respect to the comprehensive integration of subjective/objective information, quantitative/qualitative data, and a dynamic game problem.

In recent years, scholars across various fields have adopted different methods in a bid to reduce the uncertainty that is inherent while evaluating the GNSS efficacy. Specifically, grey correlation analyses based on interval numbers and different algorithms [3], [4] have been combined to comprehensively evaluate various machine gun design schemes and thus solve the problem of uncertain discrimination among multiple schemes. In other studies [5], [6], the interval theory has been combined with the analytic hierarchy process (AHP) and fuzzy comprehensive evaluation theory, and an evaluation method based on interval numbers has been proposed for related projects in a power grid. Moreover, subjective and objective integrations (combined weight) have been used in other studies [7], [8] to determine the relevant performance

The associate editor coordinating the review of this manuscript and approving it for publication was Mu Zhou.

of equipment. These models and methods have, to some extent, reduced the uncertainty in the process of evaluating the effectiveness of different subjects. However, it is difficult to solely employ these methods in the evaluation of GNSS spoofing and jamming equipment; this is because the objects of the above-mentioned evaluations are not in the navigation domains. Further, comprehensively considering the dynamics of decision-making information and fuzziness as well as randomness is challenging during the integration of such information.

Owing to the multidimensional and multilevel nature of GNSS evaluations, fuzzy comprehensive evaluations are the most appropriate for evaluating the effectiveness of GNSS spoofing and jamming equipment. The combined weight is an effective way of integrating quantitative and qualitative data as well as subjective and objective information. However, there are many uncertainties in these two traditional approaches. To overcome this drawback, the interval theory was first integrated with the combined weight and fuzzy comprehensive evaluation theory; this was aimed at obtaining an interval number form for all the elements involved to effectively deal with the fuzziness and randomness of decision-making factors and improve the credibility of the results. Second, game theory was introduced into the dynamic evaluation of the effectiveness of the spoofing and jamming equipment. At present, game theory is widely applied to the dynamic evaluation of jamming effects during radar antagonism [9]–[11]. Although the models and methods used for this purpose are relatively mature, these are not completely applicable for the evaluation of jamming effects in navigation antagonism. Therefore, to construct a profit matrix and to account for the uncertainty of evaluation, a weighted superposition method was employed; herein, the profit matrix was the core element of the navigation antagonism game. This approach combined an interval-valued fuzzy comprehensive evaluation and the joint scores of multiple experts. Finally, the evaluation results that were similar to the real-world situation were obtained using a linear programming algorithm.

II. ESTABLISHMENT OF A MATRIX MODEL AND INDEX SYSTEM BASED ON GAME THEORY

The relationship between spoofing and anti-spoofing is equivalent to the relationship between a spear and a shield. It is difficult to obtain a method that can deal with all the types of spoofing, and it is also challenging to produce a spoofing and jamming approach to break through all the types of detection algorithms. Moreover, the ''zero-sum law'' dictates that the one with the priority of information is more likely to take the initiative. If the spoofing party obtains the motion states of the target machine and anti-spoofing strategies as well as adopts the corresponding spoofing modes, the interference success rate will be improved significantly. In addition, the availability and reliability of anti-spoofing techniques will be improved.

A. STRATEGIC MATRIX MODEL IN AN ANTAGONISTIC GAME

Game theory is the study of rational behavior in a situation of mutual inclusion and interdependence. Regardless of the type of game, the following three elements are always present: players, the pure strategy space of each player, and the profit matrix of the players. In navigation antagonism, spoofing equipment and target institutions become the game players At_i and Df_j, where i stands for a certain spoofing mode and j stands for an anti-spoofing measure. The spoofing mode contained in the spoofing equipment is its pure strategy space, $\boldsymbol{S}_{\mathrm{At}i} = (\mathrm{At}_1, \mathrm{At}_2, \ldots, \mathrm{At}_5)$, and the corresponding anti-spoofing measure taken by the target machine is its pure strategy space, $\boldsymbol{S}_{\mathrm{Df}j} = (\mathrm{Df}_1, \mathrm{Df}_2, \ldots, \mathrm{Df}_5)$. The two players have opposing goals and different evaluations of criteria, but their metrics are the same. Therefore, the effectiveness of spoofing and jamming is a standard measurement for both sides, and their values jointly form the profit matrix.

Combined with studies on anti-spoofing and spoofing technologies, four typical anti-spoofing measures and five spoofing modes were set in this study. Because the spoofing and jamming mode of a signal transmitted by a single antenna is easy to be detected by defenders, this condition was not included here. When the spoofing mode of the equipment is At_i and the spoofing measure adopted by the target machine is Df_j the corresponding efficacy of spoofing and jamming is represented as E_{ij}. The strategy matrix in the antagonistic game then equals the following:

$$\boldsymbol{E} = \begin{array}{c|ccccc} & \mathrm{At}_1 & \mathrm{At}_2 & \mathrm{At}_3 & \mathrm{At}_4 & \mathrm{At}_5 \\ \mathrm{Df}_1 & E_{11} & E_{12} & E_{13} & E_{14} & E_{15} \\ \mathrm{Df}_2 & E_{21} & E_{22} & E_{23} & E_{24} & E_{25} \\ \mathrm{Df}_3 & E_{31} & E_{32} & E_{33} & E_{34} & E_{35} \\ \mathrm{Df}_4 & E_{41} & E_{42} & E_{43} & E_{44} & E_{45} \end{array} \tag{1}$$

B. INDEX SYSTEM CORRESPONDING TO THE SPOOFING MODE

According to the level and order of signal processing performed by the target machine, the principles of spoofing and jamming, and their characteristic rapidity as well as concealment were selected as the six universal indices for each spoofing mode, including: (1) the time when the jamming signal was accessed by the target machine, (2) maximum jamming distance, (3) accuracy of pseudo-range rates, (4) pseudo-range measuring accuracy, (5) spoofing position accuracy, and (6) timing accuracy of synchronous clock. The specific indices applicable to each spoofing mode were then selected. Those belonging to the repeater spoofing and jamming mode included the controllability of high-precision time-delays and the power intensity of noise; however, those belonging to the generation spoofing and jamming mode were the Doppler loss, the power intensity of spoofing signals, and the success rate of spoofing. Additionally, the specific indices belonging to the spoofing mode in the capture phase were the ratio of the power levels of correlation peaks and the average capture

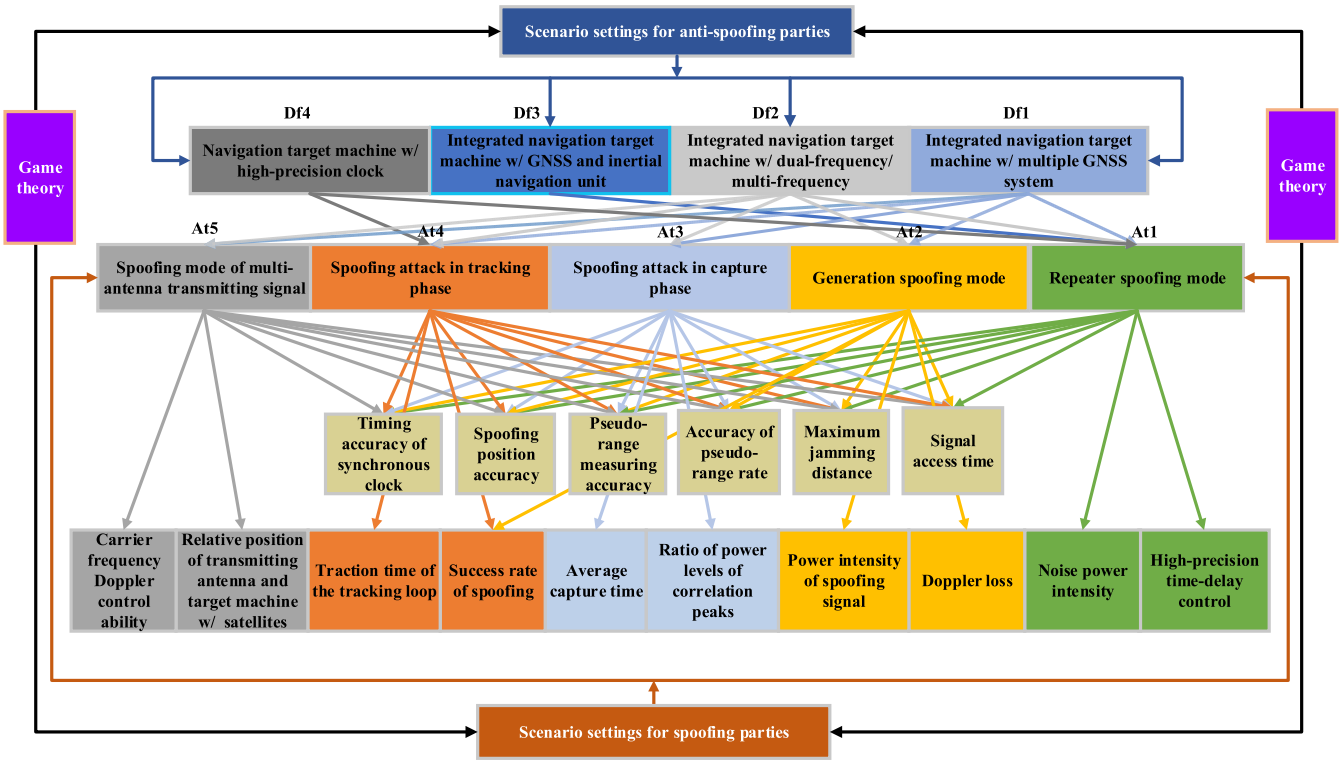


FIGURE 1. Navigation antagonism scenario and corresponding spoofing mode indices.

time. Because the prerequisites of spoofing and jamming in a synchronized code phase were too strict, spoofing and jamming in an asynchronous code phase was adopted by default during tracking; further, its specific indices represented the success rate of spoofing and the time required for the tracking loop of the target machine to gain traction. The indices that belonged to the spoofing and jamming mode of a multi-antenna transmitting signal were the relative positions of the transmitting antenna and target machine with satellites, and the ability to control the Doppler carrier frequency. Finally, Df_1 and Df_2 could deal with all jamming modes, Df_3 could emphatically resist At_1, and Df_4 could better cope with At_1 and At_4. See Figure 1 for details.

III. ESTABLISHMENT OF A PROFIT MATRIX BASED ON INTERVAL-VALUED FUZZY COMPREHENSIVE EVALUATION

A. DETERMINATION OF FACTOR AND EVALUATION SETS

The factor set determined according to the hierarchical index system of the spoofing mode, $\boldsymbol{O} = ([o_{ij}^{\mathrm{L}}, o_{ij}^{\mathrm{U}}])_{m\times n}$ (original value before standardization), of each index can be obtained. Here, i stands for a certain spoofing mode, m is the total number of spoofing modes, j is the corresponding index of a certain spoofing mode, and n is the number of indices included in a certain spoofing mode. To make the evaluation results applicable to real-world situations, the interval value of the original data must be set as the possible range of values for each index parameter in a complex electromagnetic environment (i.e., o_{ij}^{L} represents the minimum value that the index in a certain spoofing mode can obtain under any real test environment and o_{ij}^{U} represents the maximum value that the corresponding index can achieve).

An evaluation set, $\boldsymbol{V}$, was constructed according to the actual needs of the study. Five levels of evaluation were performed, $\boldsymbol{V} = (v_1, v_2, v_3, v_4, v_5)$, and the equivalent classifiers, excellent; good; medium; average; and poor were assigned. In addition, the corresponding levels were converted into values ranging from 0 to 1. This structure rendered it easier to distinguish the results; the values between 0–0.6 were equivalent to "poor," values between 0.6–0.7 were considered as "average," values between 0.7–0.8 stand were labeled "medium," and those between 0.8–0.9 and 0.9–1 were classified as "good" and "excellent," respectively. By assigning the average value to each interval (to avoid undervaluation, "poor" was assigned to the midpoint of "0.5–0.6".), the evaluation set was then quantified as:

$$\boldsymbol{V} = (0.95, 0.85, 0.75, 0.65, 0.55) \tag{2}$$

B. DETERMINATION OF A SINGLE-FACTOR COMPREHENSIVE WEIGHT

The weight of an efficacy index represents the role of each index in a systematic evaluation [12], which can be determined by subjective and objective weighting methods. Subjective weighting compares the importance of the indices according to expert preferences and experiences. A judgment matrix is obtained and then the weights of the indices

are obtained using the AHP. During objective weighting, a corresponding mathematical model is used to calculate the weights of indices for known real data, including entropy-weighting methods. The combined weighting method used here involved the combination of subjective and objective weighting methods, which has the capacity to make full use of their advantages and avoid their disadvantages, thereby obtaining a more accurate algorithm [13].

Because of the uncertainty in expert evaluation processes, the determination of index weights was based on the interval number eigenvalue method (IEM), which is one of the algorithms for obtaining the weights of judgment matrices in the uncertain type of the AHP. The resultant interval number was relatively greater according to experts. Compared with the traditional AHP, the IEM combined the randomness and fuzziness of interval numbers with the subjectivity of the AHP, enhancing the reliability of index weights. The steps in the IEM used in this study were as follows:

(1) A judgment matrix of interval numbers was constructed. The interval number included the upper and lower limits of the interval. The importance of the indices was identified according to the 1–9 scaling method proposed by Saaty [14] and the interval number judgment matrix was obtained. Taking the repeater spoofing and jamming mode as an example, the values shown in Table 1 were obtained.

(2) The index weight interval was calculated using interval eigenvalues in which the judgment matrix $\boldsymbol{A} = ([a_{ij}^{\mathrm{L}}, a_{ij}^{\mathrm{U}}])_{n\times n}$ was decomposed into two matrices $\boldsymbol{A}^{\mathrm{L}} = (a_{ij}^{\mathrm{L}})_{n\times n}$ and $\boldsymbol{A}^{\mathrm{U}} = (a_{ij}^{\mathrm{U}})_{n\times n}$, and the eigenvectors $w^{\mathrm{L}} = (w_1^{\mathrm{L}}, w_2^{\mathrm{L}}, \cdots, w_n^{\mathrm{L}})$ and $w^{\mathrm{U}} = (w_1^{\mathrm{U}}, w_2^{\mathrm{U}}, \cdots, w_n^{\mathrm{U}})$ corresponding to the maximum eigenvalues were solved. The eigenvector of the maximum eigenvalue corresponding to $\boldsymbol{A}$ was [15]

$$\begin{aligned}\boldsymbol{w}^* &= \left(w_1{}^*, w_2{}^*, \cdots, w_n{}^*\right)\\ &= \left(\left[cw_1^{\mathrm{L}*}, dw_1^{\mathrm{U}*}\right], \left[cw_2^{\mathrm{L}*}, dw_2^{\mathrm{U}*}\right],\right.\\ &\quad \left.\cdots, \left[cw_n^{\mathrm{L}*}, dw_n^{\mathrm{U}*}\right]\right)\end{aligned} \tag{3}$$

in the formula [16], [17]

$$\begin{aligned}c &= \left[\sum_{j=1}^{n}\left(1\Big/\sum_{i=1}^{n}a_{ij}^{\mathrm{U}}\right)\right]^{\frac{1}{2}},\\ d &= \left[\sum_{j=1}^{n}\left(1\Big/\sum_{i=1}^{n}a_{ij}^{\mathrm{L}}\right)\right]^{\frac{1}{2}}\end{aligned} \tag{4}$$

(3) A definite value transformation of the weight interval was performed. The index weights obtained by the IEM were expressed using interval numbers, which could not directly be applied to numerical calculations. Therefore, it was necessary to convert the weight intervals into definite values. For this purpose, a three-unit connection number during set-paired analysis was used to transform the weight intervals into definite values, following the methods detailed in a previous study [17]. Finally, the obtained subjective weights of the indices of each spoofing mode were

$$\begin{aligned}\boldsymbol{w}_1{}^* &= (0.0796, 0.0471, 0.1341, 0.2754, 0.0302,\\ &\quad 0.0777, 0.1491, 0.2068)\\ \boldsymbol{w}_2{}^* &= (0.0398, 0.0289, 0.0795, 0.2166, 0.0219,\\ &\quad 0.1127, 0.2868, 0.1579, 0.0560)\\ \boldsymbol{w}_3{}^* &= (0.2126, 0.0337, 0.0463, 0.0683, 0.0999,\\ &\quad 0.1447, 0.2946, 0.0999)\\ \boldsymbol{w}_4{}^* &= (0.0302, 0.0811, 0.1625, 0.3031,\\ &\quad 0.0237, 0.0585, 0.1149, 0.2259)\\ \boldsymbol{w}_5{}^* &= (0.0427, 0.0319, 0.0855, 0.2279,\\ &\quad 0.0244, 0.1181, 0.3044, 0.1651)\end{aligned} \tag{5}$$

TABLE 1. Interval number judgment matrix of each index in the repeater spoofing and jamming mode.

Mode	A	B	C	D	E	F	G	H
a	[1,1]	[2,3]	[1/3,1/2]	[1/5,1/4]	[4,5]	[1,1]	[1/3,1/2]	[1/4,1/2]
b	[1/3,1/2]	[1,1]	[1/4,1/3]	[1/7,1/6]	[2,3]	[1/3,1/2]	[1/5,1/4]	[1/6,1/5]
c	[2,3]	[3,4]	[1,1]	[1/3,1/2]	[5,6]	[2,3]	[1,1]	[1/3,1/2]
d	[4,5]	[6,7]	[2,3]	[1,1]	[8,9]	[4,5]	[2,3]	[1,2]
e	[1/5,1/4]	[1/3,1/2]	[1/6,1/5]	[1/9,1/8]	[1,1]	[1/5,1/4]	[1/7,1/6]	[1/8,1/7]
f	[1,1]	[2,3]	[1/3,1/2]	[1/5,1/4]	[4,5]	[1,1]	[1/3,1/2]	[1/4,1/3]
g	[2,3]	[4,5]	[1,1]	[1/3,1/2]	[6,7]	[2,3]	[1,1]	[1/2,1]
h	[2,4]	[5,6]	[2,3]	[1/2,1]	[7,8]	[3,4]	[1,2]	[1,1]

a = signal access time; b = maximum jamming distance; c = pseudo-range rate accuracy; d = pseudo-range measuring accuracy; e = spoofing position accuracy; f = timing accuracy of the synchronous clock; g = high-precision time-delay control; h = noise power intensity.

The basic idea of an entropy-weighting method is to use the information contained in each index to calculate the weight. The smaller the index information entropy, the more information it can provide, and the greater the weight assigned [18]. However, to reduce the uncertainty of the evaluation; and because the quantified value of the index is an interval number; interval theory was introduced into the entropy-weighting method for weighting and obtaining the weight of each index, $w_{ij}^{\#}$. The steps in the entropy-weighting method used in this study were as follows:

(1) First, each index in the index set matrix, $\boldsymbol{O}$, of spoofing the modes was de-dimensioned to obtain the normalized index set, $\boldsymbol{X}$, illustrated as

$$\begin{aligned}x_{ij}^{\mathrm{L}} &= o_{ij}^{\mathrm{L}}\Big/\left[\left(o_{ij}^{\mathrm{L}} + o_{ij}^{\mathrm{U}}\right)\Big/2\right],\\ x_{ij}^{\mathrm{U}} &= o_{ij}^{\mathrm{U}}\Big/\left[\left(o_{ij}^{\mathrm{L}} + o_{ij}^{\mathrm{U}}\right)\Big/2\right]\end{aligned} \tag{6}$$

(2) Second, $\boldsymbol{X} = ([x_{ij}^{\mathrm{L}}, x_{ij}^{\mathrm{U}}])_{m\times n}$ was normalized to obtain the matrix $\boldsymbol{Y} = ([y_{ij}^{\mathrm{L}}, y_{ij}^{\mathrm{U}}])_{m\times n}$, as shown in Table 2.

TABLE 2. Index values and corresponding membership parameters of spoofing modes.

Index	Original index		Standard normalized index		Membership parameters				
	O^{L}	O^{U}	Y^{L}	Y^{U}	o_1	o_2	o_3	o_4	o_5
Signal access time (s)	0.1	10.0	0.0099	0.9901	0.0	2.8	5.6	8.4	11.2
Maximum jamming distance (km)	100	800	0.1111	0.8889	50	250	450	650	850
Pseudo-range rate accuracy (m/s)	0.0001	0.0050	0.0196	0.9804	0.0001	0.0002	0.0006	0.0021	0.0075
Pseudo-range measuring accuracy (m)	0.01	20.00	0.0005	0.9995	0.0050	0.0500	0.5000	5.0000	50.0000
Spoofing position accuracy (m)	0.01	0.20	0.0476	0.9524	0.0050	0.0130	0.0338	0.0879	0.2285
Timing accuracy of synchronous clock (ns/h)	1	200	0.0050	0.9950	0	50	100	150	200
High-precision time-delay control/chip	0.1	1.0	0.0909	0.9091	0.0500	0.1150	0.2645	0.6084	1.3992
Noise power intensity (dB)	10	22	0.3125	0.6875	1	7	13	19	25
Doppler loss	1	10	0.0909	0.9091	0	2	4	8	16
Power intensity of spoofing signal (dB)	4	25	0.1379	0.8621	1	8	15	22	29
Success rate of spoofing (%)	0.05	100.00	0.0005	0.9995	0.01	0.10	1.00	10.00	100.00
Ratio of power levels of correlation peaks (dB)	0.01	31.00	0.0003	0.9997	0.005	0.050	0.500	5.000	50.000
Average capture time (s)	12	70	0.1463	0.8537	10	25	40	55	70
Traction time of the tracking loop (s)	7	3069	0.0023	0.9977	5	25	125	625	3125
Relative positions of transmitting antenna, target machine with satellites	1	9	0.1000	0.9000	0	2	4	8	16
Carrier frequency Doppler control	1	9	0.1000	0.9000	0	2	4	8	16

(3) The calculated entropy, S_{ij}, is

$$S_{ij} = -\frac{1}{\ln 2}\left(y_{ij}^{L}\ln y_{ij}^{L} + y_{ij}^{U}\ln y_{ij}^{U}\right) \tag{7}$$

(4) The entropy-weighted value, $w_{ij}^{\#}$, of each index was calculated from

$$w_{ij}^{\#} = \left(1 - S_{ij}\right) \Big/ \sum_{j=1}^{n}\left(1 - S_{ij}\right) \tag{8}$$

To highlight the subjective opinions of experts and to consider the objectivity of the evaluation, the aforementioned calculated weights were superimposed and $\delta = 0.65$ [19], which allowed for the effective combination of weights. Here, δ represents weight coefficient. The following equation could then be obtained.

$$\boldsymbol{w}_i = \delta \boldsymbol{w}_i * + (1-\delta)\,\boldsymbol{w}_i^{\#} = 0.65\boldsymbol{w}_i * + 0.35\boldsymbol{w}_i^{\#} \tag{9}$$

Through (9), the final weight of the corresponding index of each spoofing mode was obtained as

$$\begin{aligned}
\boldsymbol{w}_1 &= (0.1091, 0.0616, 0.1408, 0.2410, 0.0648,\\
&\quad 0.1100, 0.1318, 0.1409)\\
\boldsymbol{w}_2 &= (0.0724, 0.0439, 0.0952, 0.1910, 0.0508,\\
&\quad 0.1215, 0.2147, 0.1239, 0.0867)\\
\boldsymbol{w}_3 &= (0.1890, 0.0493, 0.0776, 0.0992, 0.1049,\\
&\quad 0.1467, 0.2464, 0.0870)\\
\boldsymbol{w}_4 &= (0.0662, 0.0778, 0.1492, 0.2473, 0.0520,\\
&\quad 0.0863, 0.1250, 0.1962)\\
\boldsymbol{w}_5 &= (0.0813, 0.0496, 0.1057, 0.2060,\\
&\quad 0.0580, 0.1323, 0.2288, 0.1382)
\end{aligned} \tag{10}$$

C. DETERMINATION OF TRIANGULAR MEMBERSHIP

Compared with the two traditional membership functions (shown in Fig. 2) [20], the weight of the triangular with trapezoidal membership function (Fig. 2b) was more proportional to the evaluation set, whose evaluation results were expected to be better. Therefore, a triangular with trapezoidal membership function was deemed to be the most suitable approach towards evaluating the effectiveness of GNSS spoofing and jamming equipment. The formulae for calculating the triangular with trapezoidal membership function were expressed in (12), and the definition of each variable was summarized in Table 2. The membership of single factors corresponding to the five levels of the evaluation set were determined as:

$$\begin{aligned}
\left[\boldsymbol{R}_{ij}^{L}, \boldsymbol{R}_{ij}^{U}\right] = \Big(&\left[r_{ij1}^{U}, r_{ij1}^{L}\right], \left[r_{ij2}^{U}, r_{ij2}^{L}\right],\\
&\left[r_{ij3}^{U}, r_{ij3}^{L}\right], \left[r_{ij4}^{L}, r_{ij4}^{U}\right], \left[r_{ij5}^{L}, r_{ij5}^{U}\right]\Big)
\end{aligned} \tag{11}$$

$$r_1 = \begin{cases} 1, & o < o_1 \\ \dfrac{o_2 - o}{o_2 - o_1}, & o_1 \le o < o_2 \\ 0, & o \ge o_2, \end{cases}$$

$$r_2 = \begin{cases} 0, & o < o_1, \quad o \ge o_3 \\ \dfrac{o - o_1}{o_2 - o_1}, & o_1 \le o < o_2 \\ \dfrac{o_3 - o}{o_3 - o_2}, & o_2 \le o < o_3, \end{cases}$$

$$r_3 = \begin{cases} 0, & o < o_2, \quad o \ge o_4 \\ \dfrac{o - o_2}{o_3 - o_2}, & o_2 \le o < o_3 \\ \dfrac{o_4 - o}{o_4 - o_3}, & o_3 \le o < o_4 \end{cases}$$

$$r_4 = \begin{cases} 0, & o < o_3, \quad o \ge o_5 \\ \dfrac{o - o_3}{o_4 - o_3}, & o_3 \le o < o_4 \\ \dfrac{o_5 - o}{o_5 - o_4}, & o_4 \le o < o_5, \end{cases}$$

$$r_5 = \begin{cases} 0, & o < o_4 \\ \dfrac{o - o_4}{o_5 - o_4}, & o_4 \le o < o_5 \\ 1, & o \ge o_5 \end{cases} \tag{12}$$

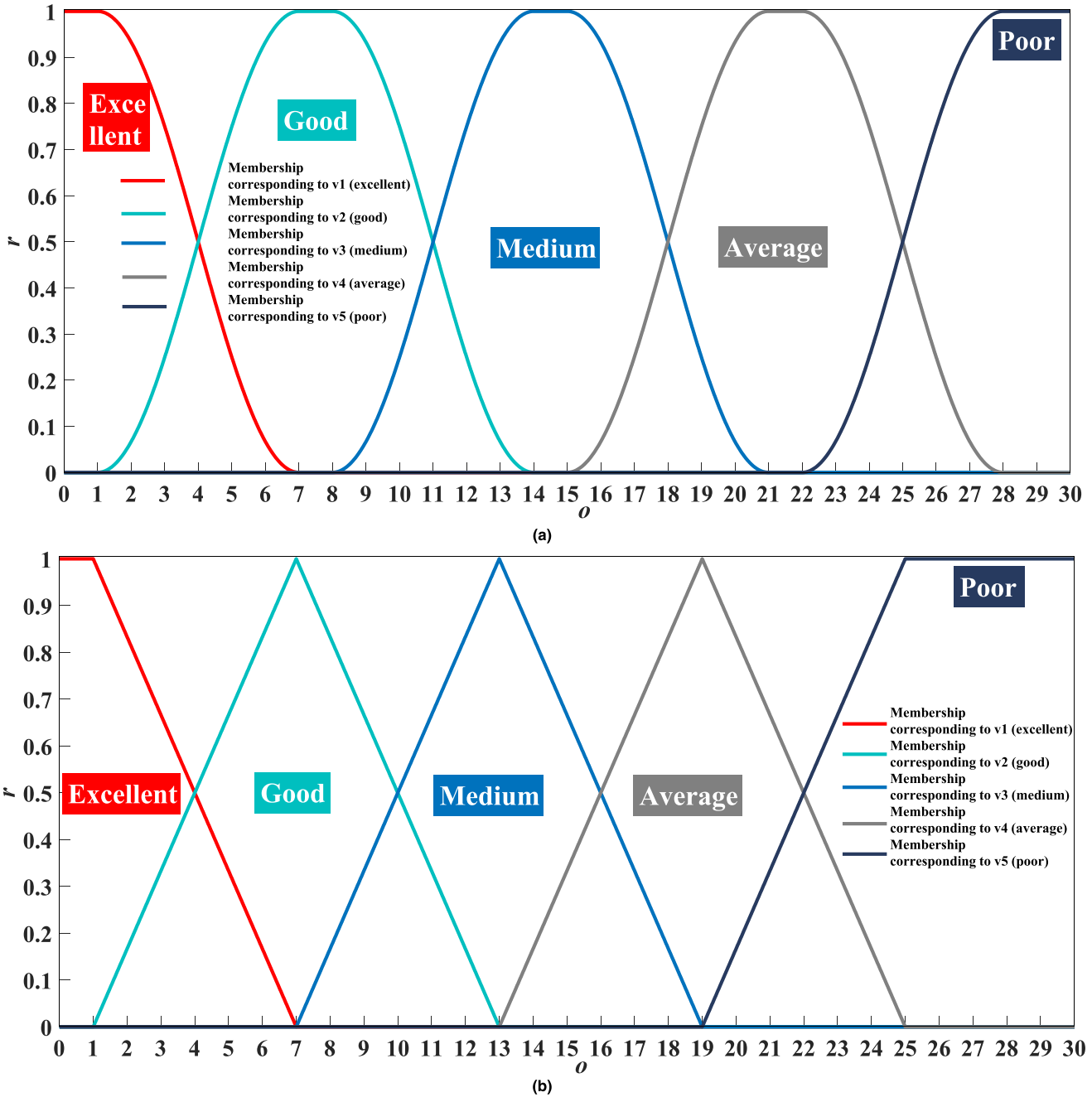


FIGURE 2. Simulated charts of (a) ridge membership function and (b) triangular w/ trapezoidal membership function, corresponding to noise power intensity.

Taking the repeater spoofing mode as an example, this membership may be further expressed as (13), shown at the bottom of the next page.

D. DETERMINATION OF A COMPREHENSIVE EVALUATION VALUE

Considering the single-factor membership values and evaluation set, the fuzzy evaluation values of single factors, which are interval vectors, were obtained as

$$f_{ij} = \left[\sum_{k=1}^{5} \left(r_{ijk}^{\mathrm{L}} v_k \right), \sum_{k=1}^{5} \left(r_{ijk}^{\mathrm{U}} v_k \right) \right] \tag{14}$$

By using single-factor evaluation values and the final weight value, the comprehensive evaluation interval value for the spoofing party could be obtained as (15), shown at the bottom of the next page.

E. DETERMINATION OF THE JAMMING PROFIT MATRIX

The expert scoring method was used in this study to determine the horizontal and vertical weights (i.e., five spoofing modes were scored according to their jamming ability considering each anti-spoofing measure and a score of 10 represented the strongest jamming ability; Table 3). Additionally, four anti-spoofing measures were scored according to their

TABLE 3. Standard interval numbers of evaluation levels.

Level	10	9	8	7	6	5	4	3	2	1
Interval	[91,100]	[81–90]	[71–80]	[61–70]	[51–60]	[41–50]	[31–40]	[21–30]	[11–20]	[1–10]

TABLE 4. Jamming ability scored by experts in the anti-spoofing party.

Mode	Spoofing party`				
	Repeater	Generation	In capture phase	In tracking phase	Multi-antenna signal
Integrated target machine with multiple GNSS systems	8	2	8	4	5
Integrated target machine with dual-frequency/multi-frequency	8	4	8	4	5
Integrated target machine with GNSS and inertial navigation unit	2	3	3	2	3
Target machine with high-precision clock	8	8	8	7	4

defensive abilities. In this method, five experts were asked to assign scores. Among them, the third expert scored the measures according to the scenario of a single system with a single generated spoofing signal, which was representative. So, to save space, only score results of the third expert were listed and indicated in Tables 4 and 5. In this case, i represented a certain spoofing mode, p was the total number of spoofing modes, j represented a certain anti-spoofing measure, q was the total number of anti-spoofing measures, and b_{ij} and b_{ji} represented the scores off a certain anti-spoofing measure and spoofing mode, respectively. The weight of each antagonistic mode was obtained from

$$J_{ij} = \left(1 \Big/ \sum_{i=1}^{p} b_{ij}b_{ji} + 1 \Big/ \sum_{j=1}^{q} b_{ij}b_{ji}\right)^{1/2} \tag{16}$$

The scoring weight set of each expert was

$$\boldsymbol{J}_4 = \begin{bmatrix} 0.7600 & 0.4866 & 0.8756 & 0.6830 & 0.6927 \\ 0.7083 & 0.4892 & 0.6974 & 0.9091 & 0.6972 \\ 0.5370 & 0.7168 & 0.5590 & 0.4146 & 0.7643 \\ 0.6812 & 0.8369 & 0.6331 & 0.4337 & 0.5557 \end{bmatrix} \tag{17}$$

TABLE 5. Defensive ability scored by experts in the spoofing party.

Mode	Anti-spoofing party			
	Integrated w/ multiple GNSS	Integrated w/ dual-frequency/multi-frequency	Integrated w/ GNSS and inertial navigation	Target machine w/ high-precision clock
Repeater	1	1	9	1
Generation	9	9	9	5
In capture phase	7	5	8	4
In tracking phase	8	6	9	5
Multi-antenna signal	7	7	9	8

Different percentages can be assigned to the scoring weights based on the results of the previous study in [21], to derive a comprehensive scoring weight set. The formula for assigning these percentages is

$$\boldsymbol{J} = 40\%\boldsymbol{J}_1 + 10\%\boldsymbol{J}_2 + 25\%\boldsymbol{J}_3 + 10\%\boldsymbol{J}_4 + 15\%\boldsymbol{J}_5 \tag{18}$$

By weighting the comprehensive scoring weight set, $\boldsymbol{J}$, relative to the comprehensive evaluation value, $\boldsymbol{F}$, the effectiveness of spoofing and jamming, $E_{ij} = [E_{ij}^{\mathrm{L}}, E_{ij}^{\mathrm{U}}]$, can be determined. Thus, the profit matrix, $\boldsymbol{E}$, composed of all values of jamming efficacy may be defined as (19), shown at the bottom of the next page.

IV. MIXED-STRATEGY GAME BASED ON BLIND INFORMATION

A blind information condition refers to a scenario in which spoofing equipment cannot judge all anti-spoofing measures of the other party, and the selection of the spoofing mode is completely based on the relevant knowledge from game theory. In general, the optimal pure strategy and jamming effectiveness of spoofing equipment under blind information conditions can be obtained using the minimax and maximin principles of game theory. However, if $\min_{1\le j\le q}(\max_{1\le i\le p} E_{ij}) \neq \max_{1\le i\le p}(\min_{1\le j\le q} E_{ij})$, there is no optimal pure strategy for spoofing equipment, but an optimal mixed strategy

$$\boldsymbol{X}^* = \left(x_1^*, x_2^*, \cdots, x_p^*\right), \quad \boldsymbol{Y}^* = \left(y_1^*, y_2^*, \cdots, y_q^*\right) \tag{20}$$

$$\left[\boldsymbol{R}_1^{\mathrm{L}}, \boldsymbol{R}_1^{\mathrm{U}}\right] = \begin{pmatrix} [0.0000, 0.9643] & [0.0000, 0.0357] & [0.0000, 0.0000] & [0.0000, 0.4286] & [0.0000, 0.5714] \\ [0.0000, 0.7500] & [0.0000, 0.2500] & [0.0000, 0.0000] & [0.0000, 0.2500] & [0.0000, 0.7500] \\ [0.0000, 0.6000] & [0.0000, 0.4000] & [0.0000, 0.0000] & [0.0000, 0.4671] & [0.0000, 0.5329] \\ [0.0000, 0.8889] & [0.0000, 0.1111] & [0.0000, 0.0000] & [0.0000, 0.6667] & [0.0000, 0.3333] \\ [0.0000, 0.3750] & [0.0000, 0.6250] & [0.0000, 0.0000] & [0.0000, 0.2026] & [0.0000, 0.7974] \\ [0.0000, 0.9800] & [0.0000, 0.0200] & [0.0000, 0.0000] & [0.0000, 0.0000] & [0.0000, 1.0000] \\ [0.0000, 0.2308] & [0.0000, 0.7692] & [0.0000, 0.0000] & [0.0000, 0.5048] & [0.0000, 0.4952] \\ [0.0000, 0.0000] & [0.0000, 0.5000] & [0.0000, 0.5000] & [0.0000, 0.5000] & [0.0000, 0.5000] \end{pmatrix} \tag{13}$$

$$\boldsymbol{F} = \sum_{j=1}^{n} w_{ij}f_{ij} = \begin{pmatrix} [0.5958, 0.9061] & [0.5806, 0.9017] & [0.5669, 0.9179] & [0.5718, 0.9203] & [0.5803, 0.8933] \\ [0.5958, 0.9061] & [0.5806, 0.9017] & [0.5669, 0.9179] & [0.5718, 0.9203] & [0.5803, 0.8933] \\ [0.5958, 0.9061] & [0.5806, 0.9017] & [0.5669, 0.9179] & [0.5718, 0.9203] & [0.5803, 0.8933] \\ [0.5958, 0.9061] & [0.5806, 0.9017] & [0.5669, 0.9179] & [0.5718, 0.9203] & [0.5803, 0.8933] \end{pmatrix} \tag{15}$$

The spoofing mode selected according to this mixed strategy can ensure that the profit of the spoofing equipment is not less than $E(\boldsymbol{X}^*, \boldsymbol{Y}^*)$, and the loss of the target machine is not greater than $E(\boldsymbol{X}^*, \boldsymbol{Y}^*)$, thus causing the game to reach equilibrium.

A. JAMMING PROFIT MATRIX SOLUTION

To obtain the optimal mixed strategy, the profit matrix must be solved. Potential solution methods include linear programming and iterating Brownian algorithm. A linear programming algorithm can solve a profit matrix of any order and is more convenient and faster than the iterative method. Therefore, a linear programming algorithm was adopted in this study. The steps for solving the profit matrix were as follows:

(1) For spoofing equipment, if $\boldsymbol{X}^*$ meets the requirements: $\sum_{i=1}^{p} E_{ij} x_i^* \geq v, j = 1, 2, \cdots, q$ and $\sum_{i=1}^{p} x_i^* = 1, x_i^* \geq 0$, then $v > 0$ and $x_i * /v = x_i$, and the jamming profit of the spoofing equipment is not less than v. This can be expressed as

$$\begin{aligned} &\min v = \sum_{i=1}^{p} x_i \\ &\begin{cases} \sum_{i=1}^{p} E_{ij} x_i \geq 1, & j = 1, 2, \cdots, q \\ x_i \geq 0, & i = 1, 2, \cdots, p \end{cases} \end{aligned} \tag{21}$$

The optimal solution, x_i, and the optimal mixed strategy, $x_i^* = v x_i$, can be obtained by solving this linear function.

(2) For a target machine, if $\boldsymbol{Y}*$ meets the requirements: $\sum_{j=1}^{q} E_{ij} y_j^* \leq \omega, i = 1, 2, \cdots, p$ and $\sum_{j=1}^{q} y_j^* = 1$, $y_j^* \geq 0$, then $\omega > 0$ and $y_j^*/\omega = y_j$, and the loss of the target machine is no greater than ω. This can be expressed as

$$\begin{aligned} &\max \omega = \sum_{j=1}^{q} y_j \\ &\begin{cases} \sum_{j=1}^{q} E_{ij} y_j \leq 1, & i = 1, 2, \cdots, p \\ y_j \geq 0, & j = 1, 2, \cdots, q \end{cases} \end{aligned} \tag{22}$$

The optimal solution, y_j, and the optimal mixed strategy, $y_j^* = \omega y_j$, can be obtained by solving this linear function

B. DETERMINATION OF THE OPTIMAL MIXED STRATEGY

By using linear programming, the obtained profit matrix, $\boldsymbol{E}^{\mathrm{L}}$, may be converted into two dual-linear programming problems, the solutions of which are

$$\begin{cases} v = \min (x_1 + x_2 + x_3 + x_4 + x_5) \\ 0.3980x_1 + 0.3002x_2 + 0.4726x_3 \\ +0.3941x_4 + 0.4032x_5 \geq 1 \\ 0.3767x_1 + 0.3515x_2 + 0.3984x_3 \\ +0.4305x_4 + 0.4097x_5 \geq 1 \\ 0.3732x_1 + 0.4051x_2 + 0.3400x_3 \\ +0.3074x_4 + 0.4144x_5 \geq 1 \\ 0.3478x_1 + 0.4667x_2 + 0.3657x_3 \\ +0.3379x_4 + 0.3612x_5 \geq 1, \end{cases}$$

$$\begin{cases} \omega = \max (y_1 + y_2 + y_3 + y_4) \\ 0.3980y_1 + 0.3767y_2 + 0.3732y_3 + 0.3478y_4 \leq 1 \\ 0.3002y_1 + 0.3515y_2 + 0.4051y_3 + 0.4667y_4 \leq 1 \\ 0.4726y_1 + 0.3984y_2 + 0.3400y_3 + 0.3657y_4 \leq 1 \\ 0.3941y_1 + 0.4305y_2 + 0.3074y_3 + 0.3379y_4 \leq 1 \\ 0.4032y_1 + 0.4097y_2 + 0.4144y_3 + 0.3612y_4 \leq 1 \end{cases} \tag{23}$$

where v and ω are the winning expectation values of both sides. The optimal mixed strategy of $\boldsymbol{E}^{\mathrm{L}}$ obtained by solving (23) is

$$\begin{cases} v = \omega = 0.3912 \\ \boldsymbol{X}^* = (0.0291, 0.0006, 0.1168, 0.0717, 0.7817) \\ \boldsymbol{Y}^* = (0.0793, 0.5325, 0.0156, 0.3726) \end{cases} \tag{24}$$

The optimal mixed strategy of $\boldsymbol{E}^{\mathrm{U}}$ can be obtained in the same manner. Thus, the minimum jamming profit range suitable for any test scenario is

$$E = \boldsymbol{X}^{*T} \mathbf{E} \boldsymbol{Y}^* = [0.3905, 0.6114] \tag{25}$$

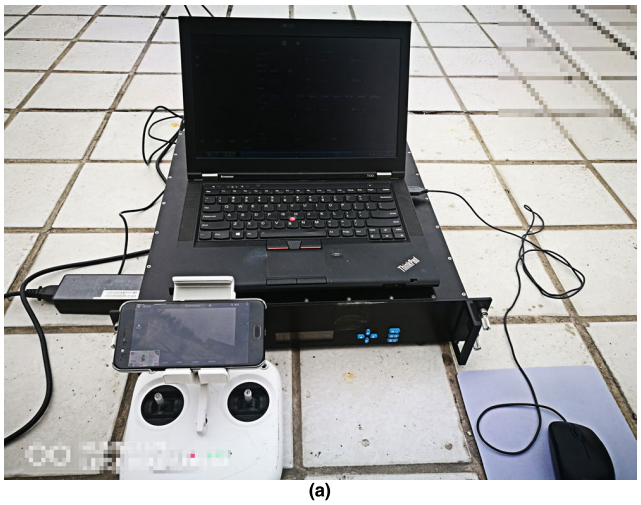
In the real-world environment, the minimum jamming profit value of spoofing and jamming performed by the equipment should be within the range calculated by (25). The closer the profit value is to the maximum value of the interval, the stronger the spoofing and jamming capability of the equipment in the dynamic game. If the value is not within this range, the equipment may fail to interfere because of its poor ability or it may be monitored by the anti-spoofing party.

V. DYNAMIC ANALYSIS OF SPOOFING AND JAMMING DECISION-MAKING IN A REAL SCENARIO

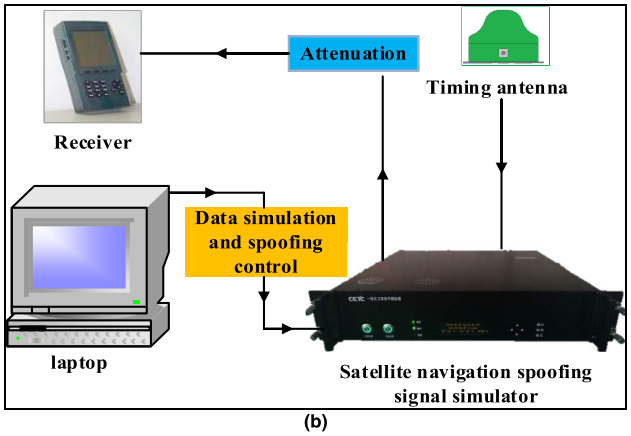
A. TEST SCENARIO AND INDEX VALUE ACQUISITION

The diamond tests (Fig. 3) were conducted using a satellite navigation spoofing signal simulator (shown in Fig. 3a),

$$\boldsymbol{E} = \begin{pmatrix} [0.3980, 0.6054] & [0.3002, 0.4662] & [0.4726, 0.7652] & [0.3941, 0.6324] & [0.4032, 0.6208] \\ [0.3767, 0.5729] & [0.3515, 0.5459] & [0.3984, 0.6452] & [0.4305, 0.6929] & [0.4097, 0.6307] \\ [0.3732, 0.5676] & [0.4051, 0.6291] & [0.3400, 0.5505] & [0.3074, 0.4947] & [0.4144, 0.6379] \\ [0.3478, 0.5290] & [0.4667, 0.7248] & [0.3657, 0.5921] & [0.3379, 0.5439] & [0.3612, 0.5560] \end{pmatrix} \tag{19}$$



(a)



(b)

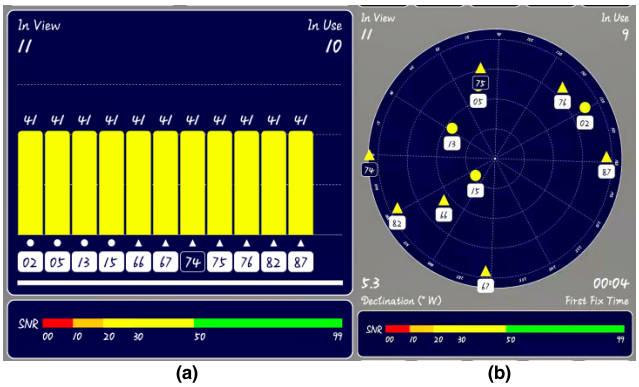
FIGURE 3. (a) Photograph and (b) schematic of the spoofing test platform.

a high-frequency oscilloscope (DS0V334A; Keysight Technol., USA), a EXA signal analyzer and a counter (N9010A and 53131A; Agilent Technol., USA), a time-interval counter (SR620; Stanford Technol., USA), and a timing and jamming antenna. Furthermore, a hand-held target machine (K82B; BHC Navigation Co., Ltd., China) was used on a test platform (as depicted in Fig. 3b). At 10:22 a.m. (UTC) on November 5, 2019, the Global Positioning System (GPS) L1 C/A and Bei Dou Navigation Satellite (BDS) B1 signals were collected as examples. Spoofing control and data simulation software, which were self-developed, were employed to set up and run a spoofing scenario. The nominal power of the spoofing signal was −134 dBm, coherent accumulation time was 1 ms, and attenuation was set as 0 dB. The signal-to-noise ratio (*SNR*) and stellar map received by the target machine are shown in Figure 4.

During the test, the following three spoofing scenarios were set up, in which the real location of the target machine was a classroom in the school.

(1) Scenario 1: Using an indoor directional expelling scenario, the target was expelled southward from the parking lot of a shopping mall at a speed of 0.2 m/s (Fig. 5). The signal access time, pseudo-range rate accuracy, and timing accuracy of the synchronous clock (Fig. 6) were tested with reference to the steps shown in Table 7;

(2) Scenario 2: The target was deceptively led toward Arxan Mountain (Inner Mongolia) using a fixed-point spoofing scenario (Fig. 7), and the pseudo-range measuring accuracy was determined. The detection steps



(a) (b)

FIGURE 4. Schematic illustration of the reception of the target machine: (a) *SNR*; (b) stellar map.

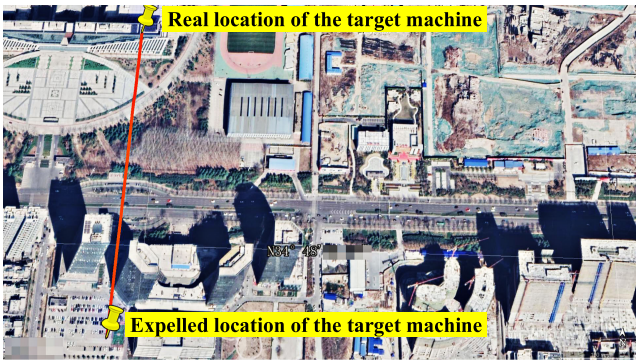


FIGURE 5. Overlaid diagram of a fixed-point expelling scenario.

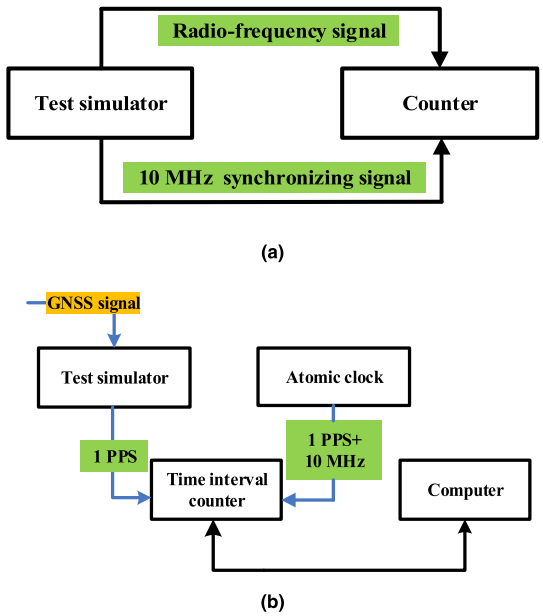


FIGURE 6. Test patterns of (a) the Pseudo-range rate accuracy and (b) the timing accuracy of a synchronous clock.

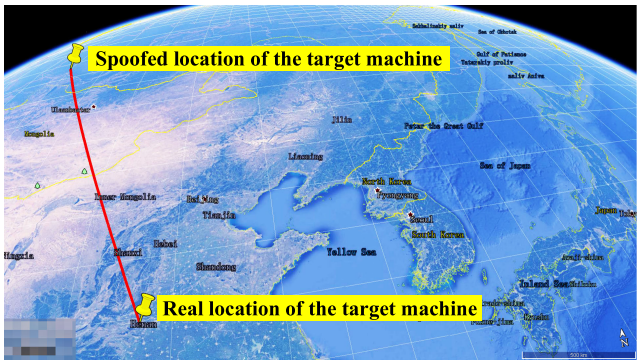


FIGURE 7. Global overlain schematic of a fixed-point spoofing scenario.

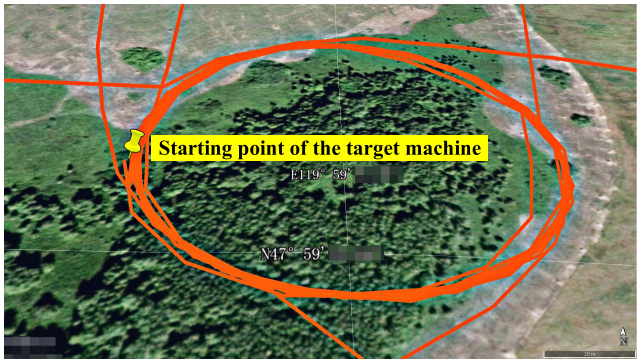


FIGURE 8. Track of a spoofing scenario with the initial point marked by a yellow pin.

TABLE 6. Root-Mean-Square errors of the four tests.

Test serial number	root-mean-square errors (*RMSE*) /m		
	X-scale	***Y***-scale	***H***-scale
Second test	0.070	0.053	0.065
Fourth test	0.063	0.044	0.026
Sixth test	0.087	0.070	0.068
Seventh test	0.041	0.010	0.024
Average result	0.065	0.044	0.046

are shown in Table 7. A total of 60 tests were conducted, and the obtained pseudo-range measuring accuracy of the simulator was approximately 6 m;

(3) Scenario 3: A track spoofing scene was used to give the target machine the illusion of moving in a circular motion with a radius of 100 m, a speed of 40 m/s, and an initial direction of 60°at the high altitude of a grassland in Hulun Buir (Fig. 8); and the success rate of the spoofing was identified. The entire track contained 574 points; because the power of the spoofing signal transmitted by the simulator was close to that of the real signal and the gain was 0 dB, the receiver was easily pulled by the real signal and mismatched for a short time, resulting in some positions deviating from the track. By using the detection steps of the corresponding indicators shown in Table 7, the obtained success rate of simulated spoofing was 83%.

A dynamic field test was necessary to complete the test of the accuracy of spoofing positioning, as shown in Table 7. The coordinate positions were based on the gaussian coordinate system. The smaller the difference was between the coordinates, the closer the curves were to zero. Furthermore, the higher the positioning accuracy was, the better the test results were. A total of seven tests were conducted on October 25, 2019, and the four tests (second test, fourth test, sixth test and seventh test) with the best results were selected to obtain the test results, as shown in Fig. 9 and Table 6.

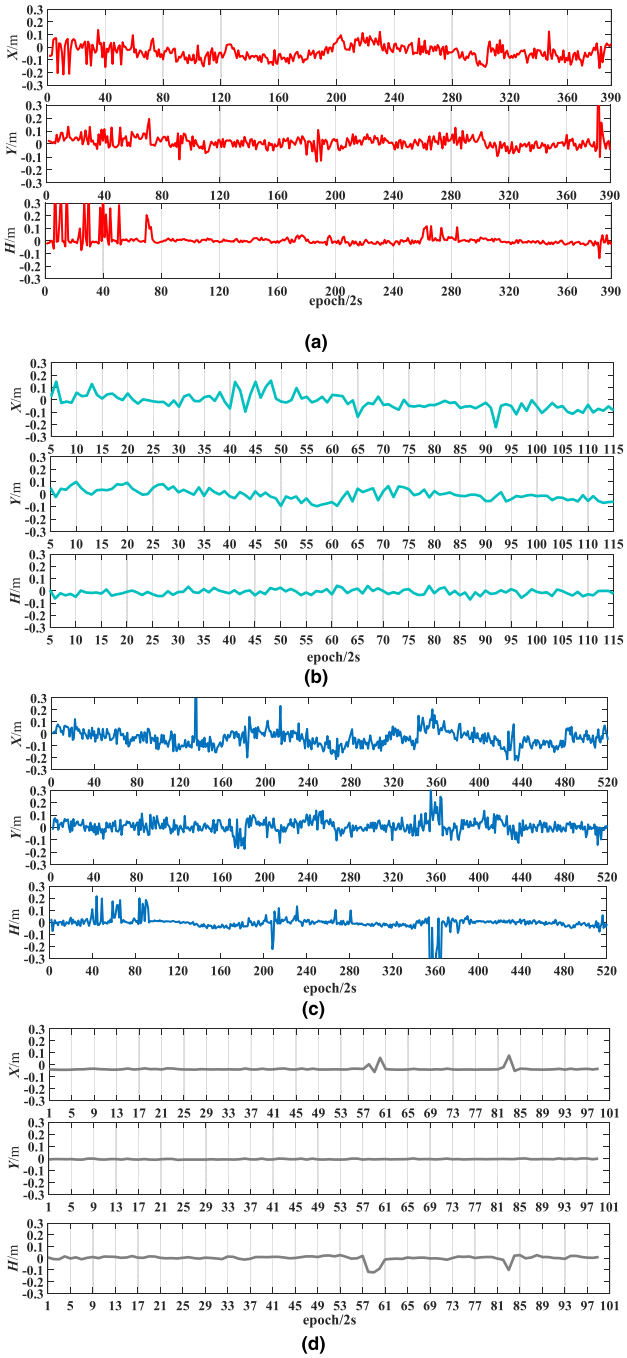


FIGURE 9. Results of (a) second test, (b) fourth test, (c) sixth test, and (d) seventh test of spoofing positioning accuracy.

The results showed that the *y*- and *h*-directions were relatively stable, whereas significant fluctuations were observed in the *x*-direction. Moreover, the positioning accuracies for the *y*-, *h*-, and *x*-directions were 0.044 m, 0.046 m,

TABLE 7. Index tests and results.

Test items	Test procedures	Technical requirements	Test results	Notes (Test data and calculation formulas)
Signal access time (s)	Input the multi-channel spoofing signal into the target machine. The false signal is accessed when the receiving level of the target machine increases. Record the time t_{ai} when the simulator starts the simulation and the time t_{bi} when the false signal is accessed for the target machine, and then calculate the difference t. Repeat 50 times and calculate the mean.	≤10.00 (smaller is better)	4.86	$\bar{t} = \frac{1}{50}\sum_{i=1}^{50}\left(t_{bi} - t_{ai}\right)$
Maximum jamming distance (km)	In the actual test, place the simulator at a particular point. Place the target machine 50 km away from the simulator and observe whether the equipment successfully deceives the target machine. If spoofing is successful, place the target machine 100 km away from the jamming equipment and observe the equipment again until jamming fails (i.e., until the target machine is no longer deceived). In theoretical simulation, the specific calculation formulas can be referenced from S. J. Zhuang [22]; where, "λ_j" is a noncentral parameter, "ERP_j" is the equipment transmitting power, "J/S" represents the jamming-to-signal power ratio, and "G_j" represents the antenna gain.	≥150.00 (larger is better)	368.91	$R_{j\max} = \left(\lambda_j 10^{\frac{ERP_j - J/S - S + G_j}{20}}\right) \Big/ (4\pi)$
Pseudo-range rate accuracy (m/s)	Set up the working test mode, output the single-channel radiofrequency (RF) signal, and set the channel to the single-carrier working mode. Set the satellite to be stationary relative to the user and record the frequency (g_0) of the counter. Set the relative speed between the user and the satellite as 1000 m/s, acceleration and jerk as 0, and record the frequency (g_1) of the counter. Calculate the Doppler shift ($g_d = g_1 - g_0$), the velocity according to $h_r = (-g_d / g_0) * c$, and the difference h between the measured value h_r and the set value h_0 (Fig. 5).	≤0.005 (smaller is better)	0.003	$g_1 = 1575414744.95$ Hz $g_0 = 1575420000.00$ Hz $h_0 = 1000$ m/s $c = 299792458$ m/s $h = \left[-\frac{(g_1 - g_0)c}{g_0}\right] - h_0$
Pseudo-range measuring accuracy (m)	Set up the target machine in the field. After the target machine starts normally, turn on the simulator. When the positioning result ρ_{ri} is stable and near the preset spoofing target ρ_{0i}, select a specific period to repeatedly detect the position 60 times and calculate the accuracy, $RMSE_\rho$.	≤20 (smaller is better)	6	$RMSE_\rho = \sqrt{\frac{1}{60}\sum_{i=1}^{60}\left(\rho_{ri} - \rho_{0i}\right)^2}$
Spoofing position accuracy (m)	Set up the target machine in the field. After the target machine starts normally, turn on the simulator. When the positioning result is stable and near the preset spoofing target, calculate the $RMSE$ of the target's spoofed coordinate positions (x_{ri}, y_{ri}, h_{ri}) and the preset coordinate positions (x_{0i}, y_{0i}, h_{0i}) n times (Fig. 9 and Table 6).	≤0.200 (smaller is better)	0.044 ($\boldsymbol{Y}$-scale)	$RMSE = \begin{cases} \sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(x_{ri} - x_{0i}\right)^2} (\boldsymbol{X}) \\ \sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(y_{ri} - y_{0i}\right)^2} (\boldsymbol{Y}) \\ \sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(h_{ri} - h_{0i}\right)^2} (\boldsymbol{H}) \end{cases}$
Timing accuracy of synchronous clock (ns/h)	The test environment is composed of a navigation simulator, an atomic clock, and a time-interval counter. The counter measures the deviation between the 1-pps signal output by the time keeping unit and the atomic clock. Power the simulator, disconnect the antenna after positioning for 24 h, record the time difference output by the counter through the computer, and record the data $\triangle t$ for 1 h. Calculate the average value of the first 100 points Δt_{fi} of the time difference information output within this hour and the last 100 points $\triangle t_{li}$; then, record the difference $\triangle$ between them (Fig. 5).	≤200 (smaller is better)	198	$\Delta = \frac{1}{100}\left\lvert\sum_{i=1}^{100}\Delta t_{fi} - \sum_{i=1}^{100}\Delta t_{li}\right\rvert$
High-precision time-delay control/chip	For the empirical value of the test scenario, refer to S. Bian [1].	≤1.0 (smaller is better)	0.5	
Noise power intensity (dB)	Preset value of the test scenario	10–22	17	
Doppler loss	To set the value of the test scenario, refer to L. Huang [23] for specific calculations, where, "f_d" is carrier doppler, "T_a" is the coherent integral time.	1–10 (smaller is better)	4	$\sin c^2\left(\pi f_d T_a\right)$
Power intensity of spoofing signal (dB)	Preset the value of the test scenario	4–25	5	
Success rate of spoofing (%)	Turn on the simulator and set a jamming distance of 10 m. If the error S_r^2 between the measured result of the target machine and the preset spoofing position is less than 5% of the preset position, spoofing will be regarded as a successful. If the number of successes is m, the success rate of spoofing ω can be obtained by dividing it by the total number of tests n.	≤100 (larger is better)	83	$\begin{cases} S_r^2 = \left(\frac{1}{n}\right)\sum_{i=1}^{n}\left[\begin{array}{l}\left(x_{ri} - x_{0i}\right)^2 + \\ \left(y_{ri} - y_{0i}\right)^2 + \\ \left(h_{ri} - h_{0i}\right)^2\end{array}\right] \\ \leq 0.05\left(x_{0i}^2 + y_{0i}^2 + h_{0i}^2\right), \omega = m/n \end{cases}$
Ratio of power levels of correlation peaks (dB)	For the setting value of the test scenario, refer to L. Huang [23] for specific calculations, where, "P_{Sat}" is the real signal powers, "P_{Sp}" is the spoofing signal powers, "$P_{\mathrm{Sat\_}R}$" is the power of real signal of correlation peaks, and "$P_{\mathrm{Sp\_}R}$" is the power of spoofing signal of correlation peaks.	≤31.00	24.80	$\frac{P_{\mathrm{Sat\_}R}}{P_{\mathrm{Sp\_}R}} = \frac{P_{\mathrm{Sat}} T_a^2 / 4}{P_{\mathrm{Sp}} T_a^2 \sin c^2\left(\pi f_d T_a\right) / 4}$
Average capture time (s)	Turn on the simulator and record the start-up time of the device $t_{\mathrm{open}i}$, simulate the spoofing signal, and output it to the target machine. When the signal-to-noise ratio of the target machine is generally increasing, the time $t_{\mathrm{work}i}$ is recorded and two time points are subtracted. Conduct the test 50 times and calculate the average value.	12.00–70.00 (smaller is better)	55.86 (Cold start)	$t_{\mathrm{capture}} = \frac{1}{50}\sum_{i=1}^{50}\left(t_{\mathrm{work}i} - t_{\mathrm{open}i}\right)$
Traction time of the tracking loop (s)	Turn on the simulator and record the time $t_{\mathrm{work}i}$ when the signal-to-noise ratio of the target machine increases. When the positioning result of the target machine is stable and near the preset spoofing target, the time $t_{\mathrm{finish}i}$ is recorded immediately, and two time points are subtracted. Conduct the test 50 times and calculate the average value.	7–3069 (smaller is better)	255	$t_{\mathrm{track}} = \frac{1}{50}\sum_{i=1}^{50}\left(t_{\mathrm{finish}i} - t_{\mathrm{work}i}\right)$
Relative position of transmitting antenna	The scoring value given by experts according to the test scenario	1–9 (larger is better)	6	
Carrier frequency Doppler control	The scoring value given by experts according to the test scenario	1–9 (smaller is better)	5	

and 0.065 m, respectively. These values could meet the requirements of the spoofing evaluation.

By using the evaluation process proposed in this study, and under the specified test scenarios, when the simulator was spoofing and jamming, the profit matrix formed by the jamming effect was:

$$\boldsymbol{E} = \begin{pmatrix} 0.5516 & 0.4085 & 0.6972 & 0.5730 & 0.5696 \\ 0.5220 & 0.4783 & 0.5879 & 0.6260 & 0.5787 \\ 0.5172 & 0.5513 & 0.5016 & 0.4470 & 0.5853 \\ 0.4821 & 0.6351 & 0.5395 & 0.4914 & 0.5102 \end{pmatrix} \tag{26}$$

The profit matrix was solved using a linear programming algorithm and the obtained minimum jamming profit, $\boldsymbol{E} = 0.5500$. This result shows that the tested simulator had a strong spoofing and jamming ability in navigation antagonism and was thus applicable in real-world environments.

B. DYNAMIC ANALYSIS OF SPOOFING AND JAMMING DECISION-MAKING

Jamming decision-making is an uncertain process. With the advancement of a game, the jamming strategy of a simulator changes when the target machine changes its defense strategy. However, the varying ability to recognize the defense strategy adopted by the target machine largely determines the selected jamming strategy. The three types of decision-making processes in such real scenarios are as follows:

(1) Under the blind information condition, the simulator will not judge any anti-spoofing measure taken by the target machine. It can only directly use the linear programming algorithm to derive the optimal mixed strategy, $\boldsymbol{X}^* = (0.4264, 0.0168, 0.3148, 0.0217, 0.2203)$, of the spoofing party, and the jamming profit is $\geq$0.5500. Therefore, in a real-world scenario, the spoofing equipment will adopt the repeater spoofing mode or a spoofing mode in the capture phase for interference;

(2) A partial-information condition refers to a part of the anti-spoofing measures adopted by the target machine of the other party that spoofing equipment can identify. Assuming that the spoofing party knows that the anti-spoofing party will not use a target machine equipped with a high-precision clock, then the spoofing party will enter into a selection state of partial information. This would be transformed into a linear programming problem to obtain the optimal mixed strategy, $\boldsymbol{X}^* = (0.0000, 0.0000, 0.0743, 0.0001, 0.9256)$, of the simulator. At this time, the spoofing party will adopt the spoofing strategy of a multi-antenna transmitting signal, and the jamming profit will be greater than or equal to 0.5791. Thus, the profit of the simulator is greater under a partial information condition than it is under blind information conditions. However, following the increased exhaustiveness of the information on the spoofing party, its jamming profit will also increase.

(3) A complete information condition means that the equipment can completely identify all the anti-spoofing measures of the other party's target machine. At this time, the spoofing party will choose the strategy with the greatest jamming profit according to all the identified information. Based on (26), if the target machine chooses a receiver equipped with a high-precision clock, the simulator will directly select generation spoofing and jamming, and the jamming profit will be 0.6351. Simultaneously, the target machine will immediately change its original strategy and choose an integrated receiver with a multiple GNSS system. The jamming profit of the simulator will then decline to 0.4085. In order to improve the jamming profit, the spoofing party will then immediately change its strategy to spoofing and jamming in the capture stage and their jamming profit will increase to 0.6972.

VI. CONCLUSION

In this study, the methods of game theory were used to obtain an index system corresponding to the different spoofing modes. In particular, a combined weight and an interval-valued fuzzy comprehensive evaluation was performed. Thereafter, the profit matrix was established, and the value of jamming efficacy was evaluated. Finally, the method was validated using real-world examples.

In the real test environment, the minimum jamming profit of the equipment conducting spoofing and jamming should be within [0.3905, 0.6114]. The closer the profit is to the maximum value of the range, the stronger is the spoofing and jamming abilities of the equipment in the dynamic game of navigation antagonism. If the value of jamming efficacy is not within the range, the equipment is ineffective at spoofing. The minimum jamming profit of the tested simulator was $\boldsymbol{E} = 0.5500$, which indicates that the spoofing equipment used in this study exhibited high spoofing and jamming capabilities and thus is applicable in real-world environments.

Compared with the traditional evaluation methods, the interval theory and fuzzy theory were first combined to reduce the fuzziness and randomness of the influencing factors. By using game theory, the static evaluation mode was changed, and the dynamic effectiveness was studied by adjusting it according to the strategies adopted by both sides during the navigation antagonism. Subsequently, the feasibility of the method was demonstrated via examples. Future studies should focus on establishing additional navigation antagonism field experiments to develop more accurate models and more effective spoofing as well as jamming equipment.

REFERENCES

[1] S. F. Bian, Y. F. Hu, and C. Chen, "Research on GNSS repeater spoofing technique for fake Position, fake time & fake velocity," *Proc. IEEE Int. Conf. Adv. Intell. Mechatronics (AIM)*, Munich, Germany, Jul. 2017, pp. 1430–1434, doi: 10.1109/AIM.2017.8014219.

[2] S. Bian, Y. Hu, and B. Ji, "Research status and prospect of GNSS anti-spoofing technology," *Scientia Sinica Inf.*, vol. 47, no. 3, pp. 275–287, 2017, doi: 10.1360/N112016-00073.
[3] J. Yu, Z.-J. Ming, G.-X. Wang, J. Huang, and Y. Yan, "Comprehensive evaluation method for combat effectiveness of machine gun considering interval uncertainty," *Acta Armamentarii*, vol. 39, no. 10, pp. 2048–2055, 2018, doi: 10.3969/j.issn.1000-1093.2018.10.019.
[4] Y. Yan, J. Hao, Z. M. Chen, G. Wang, and J. Sha, "Design scheme evaluation based on fuzzy decision maps and grey relational analysis," *Acta Armamentarii*, vol. 37, no. 10, pp. 1934–1940, 2016, doi: 10.3969/j.issn.1000-1093.2016.10.021.
[5] J. X. Wei, D. L. Yang, P. H. Du, and P. Y. He, "Power grid emergency management capability assessment based on the fuzzy-AHP comprehensive evaluation," *Adv. Mater. Res.*, vols. 1092–1093, pp. 429–433, Mar. 2015, doi: 10.4028/www.scientific.net/amr.1092-1093.429.
[6] J. X. Qi, S. L. Liu, and Z. Y. Sun, "Study on post-evaluation for the power transmission and transformation project based on AHP-fuzzy comprehensive," *Adv. Mater. Res.*, vols. 756–759, pp. 2668–2672, Sep. 2013, doi: 10.4028/www.scientific.net/amr.756-759.2668.
[7] J. An, Y. X. Xu, X. Zeng, Z. Li, and G. Zhu, "Equipment quality condition assessment under fusion information based on combination weighting," *Control Decis.*, vol. 33, no. 9, pp. 1693–1698, 2018, doi: 10.13195/j.kzyjc.2017.0575.
[8] C. Cheng, M. Gao, X. D. Cheng, D. Fang, and S. Yao, "Research on operational efficiency evaluation of anti-tank missile weapon of anti-tank missile weapon system based on combination weighting," *Syst. Eng. Theory Pract.*, vol. 38, no. 1, pp. 241–251, 2018, doi: 10.12011/1000-6788(2018)01-0241-11.
[9] K. F. Wan, X. G. Gao, B. Li, and J. Mei, "Optimal power management for antagonizing between radar and jamming based on continuous game theory," *Trans. Nanjing Univ. Aeronaut. Astronaut.*, vol. 31, no. 4, pp. 386–393, 2014, doi: 10.16356/j.1005-1120.2014.04.007.
[10] N. Henareh and Y. Norouzi, "Game theory modeling of MIMO radar and ARM missile engagement," in *Proc. 8th Int. Symp. Telecommun. (IST)*, Sep. 2016, pp. 515–520, doi: 10.1109/istel.2016.7881875.
[11] M. Ghazal and A. A. Doustmohammadi, "Novel target tracking algorithm for simultaneous measurements of radar and infrared sensors," *Adv. Electr. Comput. Eng.*, vol. 16, no. 3, pp. 57–64, 2016, doi: 10.4316/AECE.2016.03009.
[12] Y. Y. Huang, "A methodology of simulation and evaluation on the operational effectiveness of weapon equipment," in *Proc. Control Decision Conf.*, Jun. 2009, pp. 131–136, doi: 10.1109/CCDC.2009.5195131.
[13] T. L. Saaty, "The modern science of multicriteria decision making and its practical applications: The AHP/ANP approach," *Oper. Res.*, vol. 61, no. 5, pp. 1101–1118, Oct. 2013, doi: 10.1287/opre.2013.1197.
[14] W. Zhou, G. P. Xia, and N. Yan, "Multi attribute evaluation method for missile weapon system effectiveness based on WGA operator," *J. Beijing Univ. Aeronaut. Astronaut.*, vol. 34, no. 10, p. 26, 2008, doi: 10.13700/j.bh.1001-5965.2008.10.013.
[15] H. Guo, H. J. Xu, and L. Liu, "Measurement of combat effectiveness of early-warning aircraft based on interval number," *Syst. Eng. Electron.*, vol. 32, no. 5, pp. 1007–1010, 2010, doi: 10.3969/j.issn.1001-506X.2010.05.027.
[16] Y. Q. Wei, J. S. Liu, and X. Z. Wang, "Concept of consistence and weights of the judgement matrix in the uncertain type of AHP," *Syst. Eng. Theory Pract.*, vol. 14, no. 4, pp. 16–22, 1994.
[17] S. C. Wang, X. S. Jia, Q. Hu, and Q. Wang, "Effectiveness evaluation for equipment maintenance support system based on normal grey cloud model," *Syst. Eng. Electron.*, vol. 41, no. 7, pp. 1576–1582, 2019, doi: 10.3969/j.issn.1001.-506 X.2019.07.19.
[18] Y. Chen, X. Wu, X. Bu, and R. Bai, "EMMD-Prony approach for dynamic validation of simulation models," *J. Syst. Eng. Electron.*, vol. 26, no. 1, pp. 172–181, Feb. 2015, doi: 10.1109/jsee.2015.00022.
[19] L. C. Wen, X. F. Zhang, and L. M. Zhu, "Method of ameliorative multi-objective synthetic evaluation based on entropy weight and its application," in *Proc. Control and Decision Conf.*, Jun. 2009, pp. 1538–1541, doi: 10.1109/CCDC.2009.5192218.
[20] J. Dombi, "Membership function as an evaluation," *Fuzzy Sets Syst.*, vol. 35, no. 1, pp. 1–21, Mar. 1990, doi: 10.1016/0165-0114(90)90014-w.
[21] L. Izzi, G. Oricchio, and L. Vitale, "Expert judgment-based rating assignment process," in *Basel III Credit Rating Systems*. London, U.K.: Palgrave Mackmillan, 2012, doi: 10.1057/9780230361188.
[22] S. J. Zhuang, L. R. Cheng, and B. Wang, "Efficiency analysis of jamming on cruise missile guided by GPS," *Fire Control Command Control*, vol. 40, no. 2, pp. 66–69, 2015, doi: 1002-0640(2015)02-0066-04.
[23] L. Huang, Z. C. Li, and F. X. Wang, "Spoofing pattern research on GNSS receivers," *J. Astronaut.*, vol. 33, no. 7, pp. 884–890, 2012, doi: 10.3873/j.issn.1000-1328.2012.07.005.

YUE WANG was born in 1994. She is currently pursuing the M.S. degree in surveying and mapping with the National Digital Switching System Engineering and Technological Research Center, Zhengzhou, China. Her current research interest includes the evaluation of GNSS spoofing effectiveness.

JIN-MING HAO was born in 1962. He has worked with the National Digital Switching System Engineering and Technological Research Center for over thirty years. He participated in the construction of the second generation of BDS. His current research interests mainly include global satellite navigation technologies, such as GNSS precise positioning, GNSS precise orbit determination and spoofing technique of navigation.

WEI-PING LIU was born in 1986. He received the Ph.D. degree from the National Digital Switching System Engineering and Technological Research Center, Zhengzhou, China, in 2014. He is currently working with the National Digital Switching System Engineering and Technological Research Center. His current research interests include precise orbit determination of satellite, effective evaluation of GNSS spoofing and jamming equipment.

XIAN WANG was born in 1994. He received the B.S. degree in electronic information engineering from Northwestern Polytechnical University, Xi'an, China, in 2017. He is currently pursuing the M.S. degree in information and communication engineering with the National Digital Switching System Engineering and Technological Research Center, Zhengzhou, China.