Jamming effect evaluation method based on radar behavior recognition

Zhenyong Chu¹, Nan Xiao² and Jun Liang³

¹School of Information Engineering, Xijing University, Xi’an, 710123, China
²Information and Navigation College, Air Force Engineering University, Xi’an, 710077, China
³Information and Navigation College, Air Force Engineering University, Xi’an, 710077, China

Corresponding author and e-mail: Zhenyong Chu, mccdma@126.com

Abstract. Rapid and accurate evaluation of radar jamming effect is an important link to enhance the effectiveness of cognitive electronic warfare. Based on the correlation between nodes of networked combat systems, this paper proposes a method to judge the jamming effect of radar through behavior recognition. The attacker utilizes its own sensors to perceive the behaviors of victim radar and its cooperative radar, uses support vector machine (SVM) algorithm to identify and classify their behaviors, marks the classification result as jamming effect label, determines the influence of jamming on the working state of radar, and evaluates the jamming effect of the victim radar. The simulation results show that the proposed method has higher accuracy than the traditional method that only considers victim radar’s behaviors, and the kernel function selection and the dimension of behavior parameters are closely related to the accuracy of the evaluation results.

1. Introduction

Cognitive electronic warfare equipment has intelligence and self-learning ability. The attacker can perceive the state information of the target party from its own perspective, optimize the jamming strategy through machine learning algorithm, and always keep the optimal jamming pattern. We usually use the OODA loop to describe a complete attack process. The prerequisite to realize the OODA loop is that the information transmission between the four stages of "observation, adjustment, decision and action" should form a closed loop. The basic idea of cognitive electronic warfare is just to form a closed loop of electronic attack OODA loop through the closed loop of "reconnaissance identification - jamming implementation - evaluation feedback", and use the feedback evaluation results to assist decision-making.

In the process of electronic attack, it is difficult for the attacker to judge the effect of the attack intuitively, so the rapid and accurate evaluation of the effect of the attack becomes an important link to improve the effectiveness of cognitive electronic warfare. The traditional electronic attack effect evaluation method is usually based on the evaluation method of the target (such as a victim radar), because the target can provide necessary data for the evaluation, such as receiver input SIR, maximum detection range, detection area, suppression coefficient, detection probability, cheating probability, etc. [1-2]. However, in the real confrontation process, the main difficulty is that the attacker cannot
directly obtain such data, which makes it difficult to achieve information closed-loop in OODA loop. To solve this problem, literatures [3-8] studied the jamming effect evaluation problem based on the attacker side, by using artificial neural network, random forest reinforcement learning, support vector machine (SVM), supervised/unsupervised state recognition method, etc. These methods are used to indirectly evaluate the effects of jamming mainly based on the changes of the working state of the signal characteristics before and after the target is jammed, and some valuable results have been obtained. Literature [3] puts forward the necessity, criteria and specific methods of jamming effect evaluation based on the attacker, which is of great significance for real-time evaluation of the effectiveness of jamming. Aiming at the evaluation of real-time jamming effect in modern electronic warfare, literature [4] studied the criteria, methods and process of online jamming effect evaluation, based on the target information obtained by radar reconnaissance system and infrared warning system. Literature [5] established the mapping relationship between state change and jamming effect by identifying radar attributes and radar working state, and proposed a jamming effect evaluation method based on radar working state change. Literature [6] established the mapping relationship between radar behavior parameter changes and jamming effect evaluation and the knowledge base, and trained the knowledge base through SVM to realize the radar online jamming effect evaluation based on the attacker side. Literature [8] studied the unknown radar status recognition method in cognitive radar confrontation and proposed the recognition algorithm based on supervised classification and unsupervised clustering respectively.

There is ambiguity in the evaluation of electronic attack effect between the attacker and the target [9]. These evaluation methods only consider the behavior of the victim radar and do not include the behavior of other relevant nodes in the evaluation process, which makes these evaluation methods have certain limitations. Based on the model of cognitive electronic attack, this paper presents a method for evaluating the jamming effect of radar suppression. Through joint observation of the behavior of victim radar and its related combat nodes, we use SVM to classify and identify the behavior observation results, so as to obtain more accurate evaluation results, thus effectively supporting the decision of the optimal attack pattern in the future and accelerating the iterative process of the electronic attack OODA loop.

2. Cognitive model

The advantage of networked combat systems is that it improves the overall robustness of the system. If one combat node is attacked, the linkage of other nodes will be triggered; if the function of one node fails, the lost combat capability will be made up by other nodes, and the combat effectiveness of the whole system will not be reduced due to single point failure. Therefore, we can think that after the victim radar is subjected to electronic attack. First, its internal state will change, leading to changes in external behavior. Second, the behavior of the combat nodes associated with it will be adjusted accordingly. For example, a victim radar will adopt anti-jamming measures, change the working mode or even shut down to deal with the impact of jamming, and the victim radar's cooperative radar will choose to turn on to help complete the detection task. These behaviors may not only have a causal relationship with the attack, but also have a correlation with the response of the victim Radar after the attack, both of which reflect the impact of the attack on the victim radar and its associated combat systems. When a behavioral observation space is established and sufficient data is obtained, the information can be used to evaluate the jamming effect by identifying the behaviors and changes of these nodes.

Due to the non-cooperative relationship between the attack and defense parties, it is difficult for the attacker to directly obtain the changes in the working performance of the victim radar after being jammed, so it is impossible to judge the jamming effect accordingly. In order to ensure that the attacker can objectively evaluate the jamming effect and accelerate the OODA cycle, the information needed for performance evaluation can only be obtained by constructing the behavior observation space. In the radar jamming cognition model shown in Figure 1, the behavioral observation space is composed of two parts. The first is the victim radar's behavior space after being attacked. The second
is the behavior space of the cooperative radar. The attacker recognizes and processes the information obtained from the behavior observation space, so as to evaluate the effect of the attack and provide a basis for making the next attack strategy.

![Behavior recognition / Jamming effect evaluation](image)

**Figure 1.** Radar jamming cognitive model.

3. **Definition of behavior parameters**

Combined with the model in Figure 1, a relatively simple combat scenario is designed here. When the working performance of the radar is reduced to a certain threshold, cooperative radar will be turned on to enhance the detection ability of the air target. The working state of radar is simplified to search, track and shut down. Under the influence of electronic attack, radar will switch between the three working states. The radar usually works in the search state and turns to the tracking state when the target is found. When it is disturbed, anti-jamming measures can be taken; when the target is lost, the tracking state is changed to the search state. When the jamming is strong enough to prevent normal operation, the radar will be turned off. The cooperative radar can provide auxiliary detection when the victim radar is jammed, and can even completely replace the victim radar to complete the detection task.

After the electronic attack, the victim radar and its cooperative radar may take actions including changing working parameters, changing working state or working mode, etc., which will eventually be reflected in the change of behavior parameters. In the selection of radar behavior parameters, radar signal parameters, working characteristics and jamming patterns should be considered, including carrier frequency, pulse frequency, pulse width, data rate, signal strength, radar switching state and other parameters of victim radar and its cooperative radar. These parameters can feed back the performance and working status of victim radar in real time and can be acquired by radar reconnaissance in real time.

Without loss of generality, we can define the sample set of behavior parameters as follows:

1. The sample set of behavior parameters for the evaluation of the jamming effect is $S = \{s_1, s_2, ..., s_n\}$, the sample number is $n$.

2. The $i$th sample of the behavior parameters sample set is $s_i$, which includes attack parameters $a_i$, victim radar behavior parameters $x_i$, and cooperative radar behavior parameters $y_i$.

3. The attack parameter $a_i$ is defined as $a_i = \{a_{i1}, a_{i2}, ..., a_{il}\}$, which represents the value corresponding to the main parameters of the attack pattern in the $i$th sample.

4. The victim radar behavior parameters $x_i$ is defined as $x_i = \{x_{i1}, x_{i2}, ..., x_{il}\}$, which represents the corresponding values of the victim radar behavior parameters in the $i$th sample.

5. The cooperative radar behavior parameter $y_i$ is defined as $y_i = \{y_{i1}, y_{i2}, ..., y_{im}\}$, which represents the value corresponding to the behavior parameters in the $i$th sample.
Meanwhile, the jamming effect parameter $e_i$ is defined as $e_i = \{e_{i_1}, e_{i_2}, ..., e_{i_m}, ..., e_{i_n}\}$, which represents the evaluation value of the jamming effect in the $i$th sample. $e_i = +1$ indicates that the jamming is valid, $e_i = -1$ indicates that the jamming is invalid.

The following table shows an example of a sample parameter definition.

| Parameter          | Victim radar / Cooperative radar | Attack parameters | Jamming effect parameters |
|--------------------|---------------------------------|------------------|--------------------------|
| $x_{i_1}/y_{i_1}$ | $x_{i_2}/y_{i_2}$               | $x_{i_3}/y_{i_3}$ | $x_{i_4}/y_{i_4}$       |
| Meaning            | RF                              | PRI              | PW                       |
| Bandwidth          | Pulse compression ratio          | Data rate        | Beam-pointing offset     |
| PW                 | Signal strength                 | Attack pattern   | Power                    |
|                    |                                 | RF               | Valid or invalid         |

The parameters listed in the table 1 are all the data that the attacker knows or can obtain by means of detection, so that the subsequent evaluation of jamming effect can be operated. In the actual working process, the values of radar’s behavior parameters are discrete values, and its working state is generally composed of multiple parameters in different configurations. It is defined that the victim radar has certain parameter adjustment capability and hardware support capability, and its behavior parameters can be adjusted within a reasonable range according to the changes of the battlefield environment.

### 4. Behavior identification and jamming effect evaluation

SVM algorithm can solve the practical problems of small sample, nonlinear, high dimension and local extremum. The basic idea of SVM algorithm is to map the sample space to the high-dimensional feature space to make it linearly separable in the feature space, and then construct an optimal classification hyperplane in the high-order feature space to separate the two types of samples by the maximum distance. Fig. 2 shows the flow chart of jamming effect evaluation based on SVM algorithm.

In the evaluation of jamming effect, the behavior parameter samples were divided into "effective jamming" ($e_i = +1$) and "invalid jamming" ($e_i = -1$) by SVM algorithm, and the jamming effect was judged according to the classification attributes of the input samples. Table 1 shows an example of a behavior parameter sample definition, the variation of which is closely related to the actual impact of jamming on the victim radar and the cooperative radar. In the proposed method, the behavior parameter sample space is composed of victim radar behavior parameters and cooperative radar behavior parameters. Under the condition of given behavior parameter training samples, the mapping relationship between the jamming effect and behavior parameter is obtained by SVM algorithm, and the jamming effect evaluation result is obtained from this, so as to provide support for the jamming decision of cognitive electronic warfare. SVM algorithm can ensure that the learning results obtained on a limited number of samples can be more accurately used to evaluate the jamming effect in a variety of confrontation situations, with good generalization ability.

Since the original sample parameters have different values and dimensions, in order to eliminate the impact of these differences on the evaluation results, the original data should be standardized to speed up the convergence speed and computational efficiency of the algorithm. In order to eliminate the effects of these differences to the evaluation result, it is necessary to standardize raw data processing, to speed up the convergence speed and calculation efficiency of the algorithm. We usually normalize all kinds of original data into dimensionless values, and the range is limited within $[0, 1]$. Here, the maximum-minimum linear transformation normalization method is adopted to process the original data, and the formula is as follows:
\[ x'_{j,i} = \left( x_{j,i} - \min \right) / \left( \max - \min \right) \]  

(1)

Where, \( x'_{j,i} \) is the original data, \( \min \) & \( \max \) are the maximum and minimum values in the original data set, \( \max = \max \left( x_{j,i} \right), \min = \min \left( x_{j,i} \right), i = 1,2,\ldots,n. \)

The SVM algorithm is used for jamming assessment, and the classifier is trained by using known sample data. At the training stage of classifier, the training sample set is \( \left( s_1 ; e'_1, s_2, e'_2, \ldots, s_n, e'_n \right) \), where \( s_i \) represents the i th sample, the dimension of the behavior parameter contained therein can be selected according to needs, and \( e'_i \) is the corresponding output. In the process of SVM training, it is assumed that there is a referee, which is sufficient to understand the actual working state of the attacker and the victim radar, and can provide accurate jamming assessment result \( e'_i \) for the input training sample \( s_i \), so \( e'_i \) can be used as the label for the training set.

After the classifier training, test data are used to verify the trained classifier. When the accuracy of evaluation results meets the requirements, the classifier can be applied to the evaluation of jamming effect.

![Figure 2. Flow chart of jamming effect evaluation.](image)

5. Semi-physical simulation experiment
Two radar simulators and an electronic warfare pod simulator are used to simulate the air-to-ground electronic warfare scene, and a wideband receiver is used to observe the radars’ behaviors. Radar simulators and electronic warfare pod simulator can generate real radio frequency radiation signals, which belong to semi-physical simulator. The radar simulators are set according to the parameters of a certain type of ground search radar, and can generate RF radiation signals according to the working mode of this type of radar. Channel simulator and RF attenuator are used to simulate the radio wave propagation environment. The test data has high credibility.

The training sample of the simulation experiment contains the attacker data, the victim radar behavior data and the cooperative radar behavior data. The selection of parameters \( x_{1,j}, x_{2,j}, x_{\gamma,j}, y_{\gamma,j}, a_{\delta,j}, a_{\psi,j} \), respectively is the victim radar’s RF, PRI and signal strength, the cooperative radar’s signal strength, the power and frequency of jamming. In the actual battlefield environment, the attacker can obtain these behavior parameters through its own observation, so this setting is of practical value.

The quadratic kernel function, Gaussian radial basis kernel function, polynomial kernel function, multilayer perceptron kernel function and linear kernel function were selected respectively, and the influence of different kernel functions on the evaluation results was compared through simulation. A total of 1300 samples were used in the simulation experiment, and each sample was labeled with the
jamming effect. 1000 samples were randomly selected for SVM classification training, and another 300 samples were used as test data. A comparative experiment was used to evaluate the results. 1000 tests were conducted for each experiment, and the evaluation results of the test data were compared and statistically averaged with the sample markers to obtain the accuracy of the evaluation results.

For test 1, the sample space parameters are selected in 5 dimensions ($x_{i,t}$, $x_{i,j}$, $y_{i,j}$, $a_{2,j}$, $a_{3,j}$), including the victim radar’s RF and signal strength, signal strength of cooperative radar, the power and frequency of jamming.

For test 2, the sample space parameters are selected in 4 dimensions ($x_{i,t}$, $x_{i,j}$, $a_{2,j}$, $a_{3,j}$), including the victim radar’s RF and signal strength, jamming power and jamming frequency.

For test 3, the sample space parameters are selected in dimension 6 ($x_{i,t}$, $x_{i,j}$, $y_{i,j}$, $a_{2,j}$, $a_{3,j}$), including the victim radar’s RF, PRI and signal strength, the cooperative radar’s signal strength, the power and frequency of jamming.

The test 2 identifies the victim radar's behavior and obtains the evaluation result, without considering the influence of cooperative radar's behavior. Table 2 shows the final test results of jamming effect evaluation accuracy under different test conditions.

Test results show:

1. The selection of different kernel functions has an impact on the evaluation results, among which the use of Gaussian radial kernel function has the best effect, the use of quadratic kernel function, polynomial kernel function and linear kernel function has a slightly lower evaluation accuracy, and the use of multilayer perceptron kernel function has the lowest accuracy.

2. From the perspective of behavior recognition, the attacker recognizes the behavior of both the victim radar and the cooperative radar and estimates the jamming effect, the accuracy of the method is higher than that of the victim radar. This method is closer to the cognition of the real battlefield situation, and the evaluation result is more consistent with the actual situation.

3. Based on the analysis of the dimension of sample data, it is obvious that the higher the data dimension is, the more detailed the description of radar behavior will be, and the higher the accuracy of evaluation results will be. In the case of Gaussian radial kernel function, when the dimension of sample space parameter is 6, the accuracy of jamming effect evaluation is close to 1. When the data in the high-dimensional sample space are classified, the influence of parametric noise on the classification results is correspondingly reduced, which enhances the generalization ability of the evaluation algorithm.

**Table 2. Accuracy of jamming effect evaluation.**

| Kernel function type            | Test 1  | Test 2  | Test 3  |
|--------------------------------|---------|---------|---------|
| Quadratic kernel               | 92.23%  | 84.64%  | 98.08%  |
| Gaussian Radial Basis Function kernel | 92.29%  | 84.72%  | 99.92%  |
| Polynomial kernel              | 92.19%  | 84.58%  | 99.61%  |
| Multilayer Perceptron kernel   | 92.97%  | 56.78%  | 52.71%  |
| Linear kernel                  | 91.89%  | 83.88%  | 94.92%  |

**6. Conclusions**

Based on the networked characteristics of the combat system, the attacker observes the behaviors of the victim radar and the cooperative radar from its own perspective, uses the SVM algorithm to identify and classify the observed sample space data, and finally obtains the evaluation result of jamming effect. The simulation results show that the new method is more accurate than the traditional method. This method is characterized by low computational complexity, no need to introduce subjective evaluation factors, good adaptability and strong generalization ability. It provides a new
way for online evaluation of cognitive electronic warfare jamming effect under complex battlefield conditions.

Acknowledgement
This work was supported by National Natural Science Foundation of China (No. 61871474), and Shaanxi Key Research and Development Projects (2019GY-055).

References
[1] Qin F, Meng J, Du J, et al. Radar Jamming Effect Evaluation Based on Adaboost Combined Classification Model. The 4th IEEE International Conference on Software Engineering and Service Science, Beijing, China: IEEE, 2013: 910-913.
[2] Ran X, Zhu W and Xing Q 2018 Review of Electronic Countermeasures Jamming Effectiveness Evaluation. Journal of Ordnance Equipment Engineering, vol 39, no.8, pp 117-121. (In Chinese)
[3] Li C, Zhou J Q 2008 Jamming Effectiveness Evaluation from the Jamming Side. Electronic Information Warfare Technology, vol 23, no.2, pp 46–49. (In Chinese)
[4] Liu S, Jiang N, Liu Z X 2016 Online Evaluation Method of Jamming Effects of Shipboard Electronic Countermeasure. Electronic Information Warfare Technology, vol 31, no.4, pp 63 –67. (In Chinese)
[5] Zhao Y D, Xu W 2016 A Method of Real-Time Electronic Attack Effectiveness Evaluation Based on State Transition of Radar. Electronic Information Warfare Technology, vol 31, no.3, pp 42–46. (In Chinese)
[6] Xing Q, Jia X, Zhu W G and Meng X H 2018 Radar Online Jamming Effect Evaluation Based on Jamming Side. Electronic Information Warfare Technology, vol 33, no.6, pp 57–62. (In Chinese)
[7] Weng X J 2019 Effectiveness Evaluation of Radar Jamming Based on Machine Learning. University of Electronic Science and Technology of China, (Cheng Du). (In Chinese)
[8] Li Y, Gao M G and Cui S Y 2018 Unknown Radar State Recognition Method for Cognitive Radar Countermeasure. Journal of Terahertz Science and Electronic Information Technology, vol 16, no.4, pp 233–238. (In Chinese)
[9] Chu Z Y, Yang J J, Li W and Gao K J 2015 Research on Layered Attack in Information Operations, Journal of Air Force Engineering University (Military Science Edition), vol 15, no.4, pp 27-31. (In Chinese)