Efficient Network Security Situation Assessment With Multi-Strategy DBO-SVR Hybrid Model

Xuetao Du[1,*], Ling Chang[1], Xin Yan[1], Chen Zhang[1]
{changling@cmdi.chinamobile.com}
[1]China Mobile Group Design Institute Co., Ltd., Beijing, China
* *Corresponding author*

Abstract. Network security situation assessment (NSSA) plays a critical role in addressing dynamic and complex network threats, yet existing approaches face notable limitations: traditional model-driven methods lack adaptability to large-scale dynamic networks, data-driven Support Vector Regression (SVR) is highly sensitive to parameter tuning, and the original Dung Beetle Optimization (DBO) algorithm suffers from insufficient population diversity, unbalanced search capabilities, and proneness to local optima. For mitigating these drawbacks, we introduce a multi-strategy improved DBO (MIDBO) algorithm. This method fuses the chaotic elite opposition-based learning strategy, Lévy flight strategy, and a modified spiral search mechanism, aiming to resolve the inherent limitations of the original DBO. Specifically, MIDBO is employed to optimize the kernel function parameters and penalty factors of SVR, constructing a hybrid MIDBO-SVR model for NSSA. Experimental results illustrate that the proposed model achieves more remarkable performance in assessment accuracy and convergence speed when compared to current methods such as SVR, APSO-SVR, and DBO-SVR.

Keywords: Network security, Situation assessment, Multi-strategy, DBO, SVR machine.

1 Introduction

Along with the swift advancement of internet technology, network security has emerged as a vital global concern requiring immediate attention. Confronted with increasingly severe network security challenges, developing reliable network security defense strategies holds significant implications. Existing research on network security defense has made certain progress. [1] proposed optimizing the sparrow search algorithm with simulated annealing for improving BP neural network parameters for constructing a network security situation assessment model, achieving improved accuracy and convergence speed. Wang et al. [2] utilized convolutional neural networks (CNNs) with long short-term memory networks for power network situation awareness. [3] designed a network security risk assessment system using BP neural networks optimized by chaotic particle swarm optimization, realizing favorable assessment effects with enhanced accuracy.

IIKI 2025, December 18-21, Chengdu, People's Republic of China

DOI 10.4108/eai.18-12-2025.2365269

However, artificial neural network algorithms suffer from inherent limitations such as the curse of dimensionality and overfitting in practical applications. Support Vector Regression (SVR), as a statistical learning method with a concise model structure, can balance empirical risk and structural risk effectively. It addresses issues like small samples and dimensionality curse prominently, thus gaining successful application in network security situation assessment models. Nevertheless, the network security situation is influenced by numerous evaluation indicators, leading to complex structures and low efficiency of multi-input SVR-based models, coupled with potential indicator redundancy. Consequently, the rational selection of kernel function parameters and penalty factors is critical to improving the efficiency of SVR-based network security situation assessment models.

The Dung Beetle Optimization (DBO) algorithm, inspired by the natural behavior of dung beetles, has recently drawn considerable attention due to its simplicity and robust global optimization capability. However, the original DBO still encounters issues such as low population diversity, poor balance between exploration and exploitation, and the tendency to become trapped in local optima. To address these limitations, this paper proposes a multi-strategy improved DBO (MIDBO) algorithm that integrates chaotic elite opposition-based learning, Lévy flight, and an improved spiral search strategy. On this basis, a MIDBO-SVR hybrid model is constructed for network security situation assessment.

2 Related work

Network security situation assessment has become an important topic in cybersecurity research. Existing studies mainly include model-driven methods, data-driven methods, and intelligent optimization-based prediction methods. Traditional assessment approaches often rely on expert rules or mathematical models, which provide interpretability but usually struggle with dynamic and large-scale network environments. Data-driven methods, including neural networks and regression models, offer stronger nonlinear modeling capability, but their performance depends heavily on parameter selection and data quality. Intelligent optimization algorithms have therefore been introduced to improve model parameter tuning and prediction accuracy.

In recent years, optimization-enhanced SVR models have shown promise in security situation prediction. Particle swarm optimization, ant colony optimization, and sparrow search algorithms have all been used to optimize SVR parameters. Nevertheless, these methods may still suffer from premature convergence or insufficient search diversity. DBO, as a newer swarm intelligence algorithm, provides a novel way to balance exploration and exploitation. Building upon this foundation, the proposed MIDBO introduces multiple improvement strategies to further strengthen optimization performance in NSSA tasks.

3 Basic Theories

3.1 Support Vector Regression (SVR)

SVR maps input vectors into a high-dimensional feature space and constructs an optimal regression function by minimizing structural risk. Given a training set, the regression function can be expressed as

$$f(x) = \omega \cdot \varphi(x) + b \tag{1}$$

where ω is the weight vector, $\varphi(x)$ is the nonlinear mapping function, and b is the bias term.

To obtain the optimal regression hyperplane, the optimization problem is written as

$$\min \ \frac{1}{2}\|\omega\|^2 + C\sum_{i=1}^{n}(\xi_i + \xi_i^*) \tag{2}$$

where C is the penalty factor, and ξ_i, ξ_i^* are slack variables. In this study, SVR is employed as the core regression model for network security situation assessment.

3.2 Dung Beetle Optimization (DBO)

The DBO algorithm simulates the typical behavioral patterns of dung beetles in nature, including rolling, dancing, breeding, foraging, and stealing. These behaviors collaboratively enable the algorithm to search for the global optimum.

Rolling Behavior. During the rolling process, dung beetles update their positions according to

$$x_i^{t+1} = x_i^t + a \cdot k \cdot x_i^{t-1} + b \cdot \left|x_i^t - x_{\text{worst}}^t\right| \tag{3}$$

where k is the deflection coefficient, $a \in \{-1, 1\}$ controls the direction, and $b \in (0, 1)$ is a random disturbance factor.

Dancing Behavior. When encountering obstacles, dung beetles perform dancing behavior to adjust direction:

$$x_i^{t+1} = x_i^t + \tan\theta \cdot \left|x_i^t - x_i^{t-1}\right| \tag{4}$$

where θ is a random angle.

Breeding Behavior. When a promising region is found, the breeding area is adaptively shrunk as

$$\begin{cases} \text{Ub}^* = \min\left(x^* \cdot (1+R), \text{Ub}\right) \\ \text{Lb}^* = \max\left(x^* \cdot (1-R), \text{Lb}\right) \end{cases} \tag{5}$$

where $R = 1 - t/T_{\max}$. The egg ball update rule is

$$B_i^{t+1} = x^* + b_1 \times \left(B_i^t - \text{Lb}^*\right) + b_2 \times \left(B_i^t - \text{Ub}^*\right) \tag{6}$$

where b_1 and b_2 are random vectors.

4 Improved Dung Beetle Optimization (MIDBO)

4.1 Chaotic Elite Opposition-Based Learning Strategy

To increase initial population diversity and accelerate convergence, chaotic elite opposition-based learning is introduced. The chaotic variable is generated as

$$z_{i+1} = \mu z_i(1 - z_i) \tag{7}$$

where μ is the control parameter. Based on elite individuals, the opposite solution is generated to enlarge the search space.

$$x_i' = \alpha\,(\mathrm{Ub} + \mathrm{Lb}) - x_i \tag{8}$$

where α is a random coefficient.

4.2 The Lévy flight strategy

To improve the algorithm's ability to escape local optima, Lévy flight is incorporated into the global search phase:

$$\mathrm{Levy}(\beta) = \frac{u}{|v|^{1/\beta}} \tag{9}$$

where u and v follow normal distributions.

$$x_i^{t+1} = x_i^t + \mathrm{Levy}(\beta) \otimes \left(x_i^t - x_{\mathrm{best}}^t\right) \tag{10}$$

This strategy helps the algorithm perform occasional long jumps and enhances exploration.

4.3 Improved Spiral Search Strategy

An improved spiral search strategy is introduced to enhance local exploitation around promising regions. Its position update rule is expressed as

$$x_i^{t+1} = x_i^t \cdot e^{bl} \cdot \cos(2\pi l) + x_{\mathrm{best}}^t \tag{11}$$

where b is a constant and l is a random number in $[-1, 1]$.

By modifying the original Equations (4) and (6), the updated position update formulas for the corresponding behaviors are

$$\begin{aligned} x_i^{t+1} &= x_i^t + k_1 \times \left(x_i^t - Lb^b\right) + k_2 \times \left(x_i^t - Ub^b\right) \\ B_i^{t+1} &= x_i^t + k_3 \times \left(B_i^t - Lb^*\right) + k_4 \times \left(B_i^t - Ub^*\right) \end{aligned} \tag{12}$$

5 MIDBO-SVR Based Network Security Situation Assessment Method

To optimize the network security situation assessment process, the MIDBO algorithm is introduced to improve the performance of SVR and applied to the assessment process. Fig. 1 shows the schematic diagram of the assessment model. The specific process of MIDBO-SVR network situation assessment is as follows.

Step 1: Establish the network security situation assessment index system, then normalize the collected situation data via the formula below to ensure data uniformity:

$$x' = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \tag{13}$$

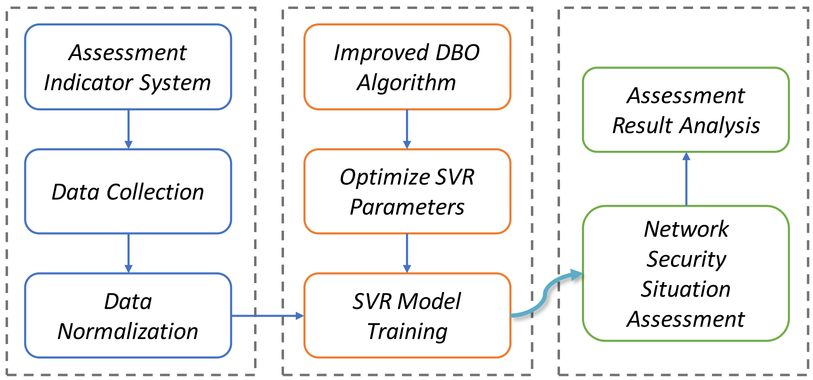

Fig. 1. MIDBO-SVR situation assessment model.

where x denotes the original sample data, and x' represents the normalized result.

Step 2: Initialize the weights and thresholds of network security situation indicators, which lays the groundwork for subsequent analysis and evaluation.

Step 3: Determine the dung beetle population size N, and configure parameters including the proportion of individuals engaged in rolling, dancing, breeding, foraging, and stealing behaviors, the maximum iteration count $T_{\max}$, breeding/foraging boundaries, and search dimensions.

Step 4: Initialize the positions of individual dung beetles using the improvement strategies above.

Step 5: Compute the fitness values of all individuals, then identify the dung beetles corresponding to the current worst and optimal positions.

Step 6: Update the positions of dung beetles performing rolling, foraging, stealing, and breeding behaviors.

Step 7: Recompute the fitness values and adjust individual positions: if the new fitness value is superior, update the corresponding dung beetle position; otherwise, retain the original position.

Step 8: Identify the optimal kernel function parameters and penalty factors through the above steps to optimize the SVR model. Train the normalized data samples using this optimized model; after training, denormalize the data and output the final simulation results.

6 Experiments

To facilitate intuitive analysis and result interpretation, network security situation assessment outcomes are divided into five grades with corresponding quantitative intervals: “Excellent” ($[0, 0.2]$), “Good” ($(0.2, 0.4]$), “Medium” ($(0.4, 0.6]$), “Poor” ($(0.6, 0.8]$), and “Dangerous” ($(0.8, 1]$).

6.1 Data Collection and Preprocessing

To validate the effectiveness of the SVR-based network security situation assessment model, this study focuses on threat indicators confronting network security systems. Typically, these threat indicators can be subdivided into five third-level indicators. The experimental dataset comprises authentic samples made available on the official platform of the National Internet Emergency Response Center (CNCERT/CC), which are split into a training set (7342 samples) and a test set (100 samples).

To more intuitively characterize the network threat level, indicator weights are assigned using the method detailed in Table 1. The calculation formula for the weekly network security situation value is expressed as

$$V_{\mathrm{nst}} = \omega_i \sum_{i=1}^{t} \cdot \frac{ST_i}{ST_{i,\max}} \tag{14}$$

where ST_i denotes the count of the i-th security threat type in a given week, $ST_{i,\max}$ represents the maximum count of that threat type in the experimental dataset, and ω_i is the weight corresponding to the i-th threat indicator.

Table 1: Weight distribution of cybersecurity threat indicators.

Threat Indicator	Weight
Infected Virus Hosts	0.4
Phishing Websites	0.2
New Security Vulnerabilities	0.2
Backdoor-Infected Networks	0.2

6.2 Experimental Result Analysis

Two evaluation indicators, Mean Absolute Percentage Error (MAPE) and Mean Squared Error (MSE), are selected to compare the relative errors and output errors between the network security situation assessment values of SVR, APSO-SVR, DBO-SVR, MIDBO-SVR and the known assessment values of the National Internet Emergency Center. The results are shown in Figs. 2 and 3, and in Table 2.

It can be found from the comparison that the MIDBO-SVR situation assessment model has the slightest fluctuation in absolute error and relative error and remains closest to the zero-error line. This finding highlights that the MIDBO-SVR situation assessment model has higher superiority in accuracy compared with the other three assessment models.

Moreover, Table 2 demonstrates that the MIDBO-SVR model achieves remarkable improvements in both key metrics compared to the other three models. The MAPE of MIDBO-SVR is only 2.856%, while the MSE is 0.000229, indicating substantial gains in prediction accuracy and stability.

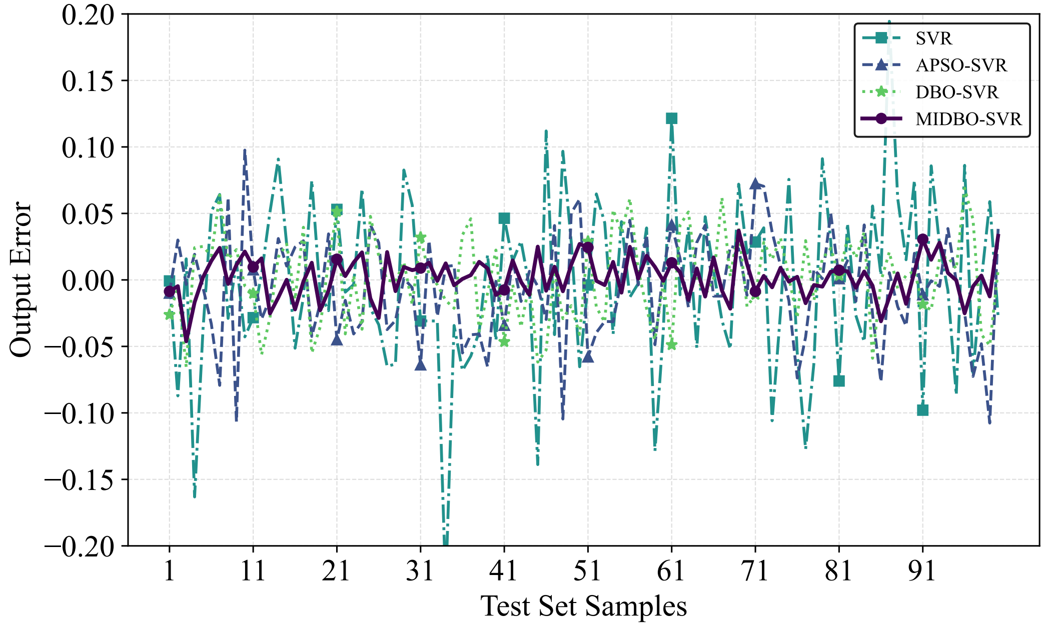

Fig. 2. Comparison of output errors.

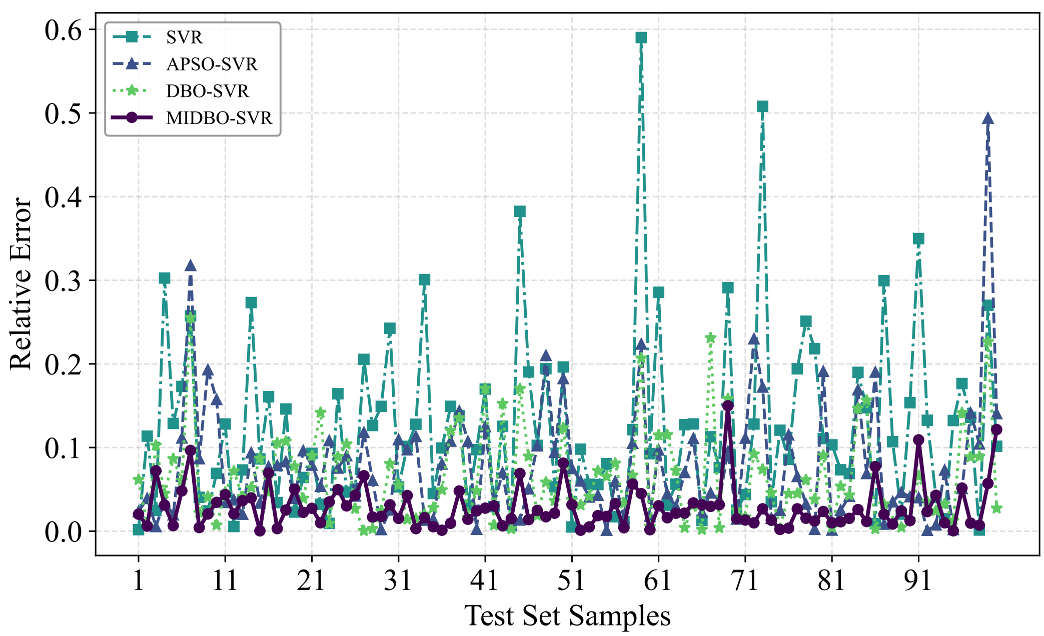

Fig. 3. Comparison of relative errors.

Table 2: Comparison of the accuracy of different models.

	SVR	APSO-SVR	DBO-SVR	MIDBO-SVR
MAPE/%	12.342	7.764	6.385	2.856
MSE	0.004297	0.001626	0.001009	0.000229

7 Conclusion

To tackle the problems of insufficient optimization performance, weak global search ability and insufficient convergence accuracy in the original dung beetle optimization (DBO) algorithm, this paper introduces a multi-strategy improved dung beetle optimization algorithm, termed MIDBO. By integrating multiple improved strategies, the enhanced algorithm effectively elevates its search efficiency, convergence speed and stability in complex optimization spaces. On this basis, the MIDBO algorithm is utilized to optimize the critical parameters of the support vector regression (SVR) model, so as to overcome the shortcomings of manual parameter tuning and insufficient model fitting effect, and a network security situation assessment model based on MIDBO-SVR is constructed accordingly. A large number of simulation experiments and comprehensive comparative analyses with multiple mainstream assessment models are carried out to verify the performance of the proposed model. The experimental results demonstrate that the MIDBO-SVR model presents faster convergence speed, higher convergence accuracy, stronger data fitting ability and better generalization performance, while significantly improving its adaptive capacity and learning efficiency in network security situation quantification. With higher assessment precision and stronger robustness in practical application scenarios, the proposed model provides an effective technical solution and important reference for the in-depth research, design and practical application of cyberspace security situation assessment systems in the future.

References

[1] Zhang R, et al. A model of network security situation assessment based on BPNN optimized by SAA-SSA. International Journal of Digital Crime and Forensics (IJDCF). 2022;14(2):1-18.

[2] Wang Q, et al. Toward the prediction level of situation awareness for electric power systems using CNN-LSTM network. IEEE Transactions on Industrial Informatics. 2020;17(10):6951-61.

[3] Li Y, Wu F. Improved population intelligence algorithm and BP neural network for network security posture prediction. International Journal of Distributed Sensor Networks. 2023;2023(1):9970205.

[4] Guo C, Wang X, Chu P. Fuzzy AHP-Based Security Evaluation for Wireless Integrated Access System. In: 2021 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS). IEEE; 2021. p. 1-4.

[5] Zeng B, et al. A novel grey Verhulst model with four parameters and its application to forecast the carbon dioxide emissions in China. Science of The Total Environment. 2023;899:165648.

[6] Liu S. Grey systems analysis: methods, models and applications. Cham, Switzerland: Springer Nature; 2025.

[7] Rane NL, et al. Machine learning and deep learning for big data analytics: A review of methods and applications. Partners Universal International Innovation Journal. 2024;2(3):172-97.

[8] Guo X, et al. Research on network security situation awareness and dynamic game based on deep Q learning network. Journal of Internet Technology. 2023;24(2):549-63.

[9] Chen Z. Research on internet security situation awareness prediction technology based on improved RBF neural network algorithm. Journal of Computational and Cognitive Engineering. 2022;1(3):103-8.

[10] He Z, Wang X, Li C. A Time Series Intrusion Detection Method Based on SSAE, TCN and Bi-LSTM. Computers, Materials & Continua. 2024;78(1):1-18.

[11] Abualigah L. Particle Swarm Optimization: Advances, Applications, and Experimental Insights. Computers, Materials & Continua. 2025;82(2):2847-75.

[12] Liu Y, et al. Review of the grey wolf optimization algorithm: variants and applications. Neural Computing and Applications. 2024;36(6):2713-35.

[13] Xue J, Shen B. Dung beetle optimizer: A new meta-heuristic algorithm for global optimization. The Journal of Supercomputing. 2023;79(7):7305-36.

[14] Ji X, et al. Improved DBO Algorithm Incorporating Disorienting Behavior and Dynamic Population Strategy for Engineering Problem Solving. Engineering Letters. 2025;33(1):1-15.

[15] Zhang F, O'Donnell LJ. Support vector regression. In: Machine Learning. Boston, MA, USA: Academic Press; 2020. p. 123-40.

[16] Ma Z, Liu S, Xu L. Enhancing dung beetle optimization algorithm with hybrid multi-strategy and its engineering applications. Neural Computing and Applications. 2025:1-53.

[17] Reynolds AM, Rhodes CJ. The Lévy flight paradigm: random search patterns and mechanisms. Ecology. 2009;90(4):877-87.

[18] Campeau W, Simons AM, Stevens B. The evolutionary maintenance of Lévy flight foraging. PLOS Computational Biology. 2022;18(1):e1009490.