Journal of Electronic Research and Application, 2026, Volume 10, Issue 3
http://ojs.bbwpublisher.com/index.php/JERA
ISSN Online: 2208-3510
ISSN Print: 2208-3502

IoT Security Situation Prediction Based on AGWO-Optimized BiGRU-ATTN

Menghao Niu, Wen Chen*

School of Artificial Intelligence and Computer, North China University of Technology, Beijing 100144, China

***Corresponding author:** *Wen Chen, 2920912486@qq.com*

***A*bstract:** To address the complexity and variability of Internet of Things (IoT) security situation prediction, this paper proposes an IoT security situation prediction model based on an improved Grey Wolf Optimizer (AGWO) optimized Bidirectional Gated Recurrent Unit with an attention mechanism (BiGRU-ATTN). Aiming at the shortcomings of the standard Grey Wolf Optimizer, such as slow convergence and susceptibility to local optima, the algorithm is enhanced through chaotic mapping-based population initialization, a nonlinear adaptive convergence factor, and a fitness-weighted position updating strategy, thereby improving the global search capability and convergence speed. Moreover, a BiGRU network is employed to capture complex temporal correlations in security situation sequences, while an attention mechanism dynamically assigns different weights to key features. Finally, the improved grey wolf optimizer is used to optimize the hyperparameters of the BiGRU-ATTN network. Experimental results demonstrate that, compared with traditional methods, the proposed model achieves superior fitting performance and faster convergence.

Keywords: Network security; Situation prediction; Bidirectional gated recurrent unit; Attention mechanism; Grey wolf optimizer

Online publication: April 22, 2026

1. Introduction

With the widespread deployment of Internet of Things (IoT) devices in smart homes, industrial control systems, and healthcare monitoring, the attack surface of networks has expanded exponentially, making security situation prediction a core technology for ensuring the reliability of IoT systems [1]. Traditional prediction models often suffer from limited accuracy and slow convergence when dealing with multi-peak, high-dimensional time-series data, and they are particularly ineffective in extracting features of complex attack behaviors, which reduces the timeliness of situation assessment [2].

The essence of IoT security situation prediction lies in analyzing the temporal evolution of network states to quantify risks and forecast future threat trends. In recent years, the integration of deep learning and optimization

algorithms has provided new perspectives for IoT security situation prediction. Zhang *et al.* proposed a BiGRU-ATTN network optimized by a deep whale optimization algorithm for network security situation prediction in IoT environments [3]. Du *et al.* combined an optimized Clockwork Recurrent Neural Network with the Grey Wolf Optimizer to capture spatiotemporal characteristics of network security situations [4]. Yang *et al.* designed a network attack behavior classification model integrating parallel feature extraction, BiGRU, and an attention mechanism for security situation assessment [5].

However, existing studies still face limitations in modeling complex temporal dependencies and selecting critical features in network security situation time series, making it difficult to cope with the highly dynamic, large-scale, and complex feature relationships of IoT environments. To this end, this paper integrates a Bidirectional Gated Recurrent Unit (BiGRU) with a self-attention mechanism and combines it with an improved Grey Wolf Optimizer (AGWO) to construct an AGWO-optimized BiGRU-ATTN IoT security situation prediction model. This model enables more accurate characterization of complex patterns and latent dependencies during the evolution of security situations.

The main contributions of this paper are summarized as follows:

(1) An improved Grey Wolf Optimizer (AGWO) is proposed by introducing chaotic initialization, nonlinear adaptive convergence factors, and fitness-weighted position updates to enhance optimization performance;

(2) An AGWO-BiGRU-ATTN prediction model is designed to capture temporal dependencies and highlight important features in security situation sequences;

(3) Experimental results demonstrate that the proposed model achieves superior prediction accuracy compared with several baseline models.

2. Methodology

2.1. BiGRU-ATTN temporal feature modeling network

The Gated Recurrent Unit (GRU) is a variant of recurrent neural networks that reduces computational complexity while maintaining strong sequence modeling capability [6]. Specifically, the input to the GRU at time step t consists of the current input vector x_t and the hidden state h_{t-1} from the previous time step, which carries relevant information from earlier states. The output of the GRU is the hidden state h_t at time step t. By combining the previous hidden state h_{t-1} and the current input x_t, the GRU generates two gating states. Among them, the update gate controls the amount of historical information retained from the previous state and the amount of new information incorporated from the candidate state, as defined in **Equation (1)**.

$$h_t=(1-z_t)\odot h_{t-1}+z_t\odot \tilde{h}_t \tag{1}$$

Here, z_t denotes the update gate, whose operation is defined in **Equation (2)**. The candidate hidden state $\tilde{h}_t$ is computed according to **Equation (3)**.

$$z_t=\sigma(W_z\cdot[h_{t-1},x_t]) \tag{2}$$

$$\tilde{h}_t=\tanh(x_tW_{hx}+(r_t\odot h_{t-1})W_{hh}+b_h) \tag{3}$$

The reset gate is defined as:

$$r_t=\sigma(W_r\cdot[h_{t-1},x_t]) \tag{4}$$

While GRU networks can only process time series unidirectionally, BiGRU can simultaneously process

sequential data from both forward and backward directions due to its unique bidirectional structure, enabling more comprehensive capture of dependencies within time series.

To further improve the model's ability to focus on important time steps, a self-attention mechanism is introduced. The self-attention mechanism calculates the relevance among sequence elements using the Query-Key-Value (QKV) structure. Each element dynamically assigns weights to other elements in the sequence, enabling the model to emphasize key temporal features and improve prediction accuracy.

2.2. Improved Grey Wolf Optimizer (AGWO)

To address the problems of the standard Grey Wolf Optimizer (GWO), such as uneven initial population distribution, insufficient balance between global exploration and local exploitation, and limited position update precision in complex high-dimensional optimization problems, this paper proposes an improved Grey Wolf Optimizer, referred to as the Advanced Grey Wolf Optimizer (AGWO). By introducing chaotic mapping–based population initialization, a population-state-based nonlinear adaptive convergence factor, and a fitness-weighted position updating strategy, AGWO systematically enhances the traditional GWO, thereby accelerating convergence speed while maintaining strong global search capability and improving final optimization accuracy. Furthermore, AGWO is employed to adaptively optimize the key hyperparameters of the BiGRU-ATTN network.

2.2.1. Chaotic mapping–based population initialization strategy

To increase population diversity, a Tent chaotic mapping strategy is used to initialize the population. Chaotic sequences have strong randomness and ergodicity, enabling the algorithm to generate more uniformly distributed initial solutions.

The Tent mapping function is defined as:

$$x_{k+1} = \begin{cases} \frac{x_k}{\mu} & (0 \le x_k < \mu) \\ \frac{1-x_k}{1-\mu} & (\mu \le x_k \le 1) \end{cases} \quad (5)$$

After removing the initial transient iterations, the chaotic sequence is mapped to the solution space to generate the initial population.

2.2.2. Population-state-based nonlinear adaptive convergence factor

In the standard GWO algorithm, the convergence factor decreases linearly from 2 to 0. However, this strategy cannot adapt to changes in the population state during optimization.

To address this problem, a nonlinear convergence factor based on a power function is introduced:

$$a = 2 - 2 \times \frac{t}{T_{max}} \quad (6)$$

where t denotes the current iteration number and T_{max} denotes the maximum number of iterations.

This strategy enables the algorithm to maintain strong global exploration ability in the early stage and improve local search accuracy in the later stage.

2.2.3. Fitness-weighted position updating strategy

In the standard GWO, the positions guided byα, β, and δ wolves are averaged with equal weights. This approach ignores the fitness differences among leading wolves.

Let the fitness values of the α, β, and δ wolves be denoted as f_α, f_β, and f_δ, respectively.

$$r_\alpha = \frac{f_\alpha}{f_\alpha+f_\beta+f_\delta+\varepsilon}, r_\beta = \frac{f_\beta}{f_\alpha+f_\beta+f_\delta+\varepsilon}, r_\delta = \frac{f_\delta}{f_\alpha+f_\beta+f_\delta+\varepsilon} \quad (7)$$

$$w_\alpha = \frac{r_\alpha}{r_\alpha+r_\beta+r_\delta}, w_\beta = \frac{r_\beta}{r_\alpha+r_\beta+r_\delta}, w_\delta = \frac{r_\delta}{r_\alpha+r_\beta+r_\delta} \quad (8)$$

Where ε is a very small constant introduced to avoid division by zero. Where $w_\alpha+w_\beta+w_\delta=1$, and $w_\alpha > w_\beta > w_\delta$.

The final weighted position updating formula is given as follows:

$$X(t+1) = w_\alpha \cdot X_\alpha + w_\beta \cdot X_\beta + w_\delta \cdot X_\delta \quad (9)$$

When the fitness of the α wolf is significantly better than that of the β and δ wolves $f_\alpha \leq f_\beta, f_\delta$), the weight w_α approaches 1, and the ω wolves converge strongly toward the position of the α wolf.

3. Experiments and analysis

3.1. Dataset description

Experiments are conducted using the publicly available ToN-IoT dataset [7]. The dataset simulates a realistic IoT environment and contains multiple attack types, including DoS, scanning, injection, ransomware, and others. During preprocessing, categorical features are converted into numerical representations through one-hot encoding. Min-Max normalization is then applied to scale all features into the range [0,1].

3.2. Network security situation value construction

Since the ToN-IoT dataset does not provide ground-truth security situation values, an attack-threat-based method is used to construct situation indicators [8]. The proposed indicator system incorporates both an attack quantity factor and an attack threat factor. The attack quantity factor represents the number of attack samples within a given time interval and is denoted by N. The attack threat factor reflects the threat level posed by a specific attack type to network security and is denoted by . The threat factors corresponding to different attack types are listed in **Table 1**. Accordingly, the security situation value at time interval t, denoted as, is defined as:

$$SA(t) = f(N, X_i) = \sum_{i=1}^{N} X_i \quad (10)$$

Table 1. Attack threat factors

Attack type	Threat factor	Attack type	Threat factor
normal	1	mitm	6
password	2	backdoor	7
scanning	3	injection	8
dos	4	ddos	9
xss	5	ransomware	

According to the temporal order of attack samples, every 800 consecutive samples are treated as one time interval. The raw situation values SA(t) calculated for all intervals are then normalized and mapped into the range [0,1]. When network attacks occur frequently, the corresponding security situation score increases, indicating a

higher threat level; conversely, when the number of attacks is small, the situation score decreases, reflecting a lower threat level. Based on **Equation (10)**, the ground-truth situation value for each time interval is generated, as illustrated in **Figure 1**.

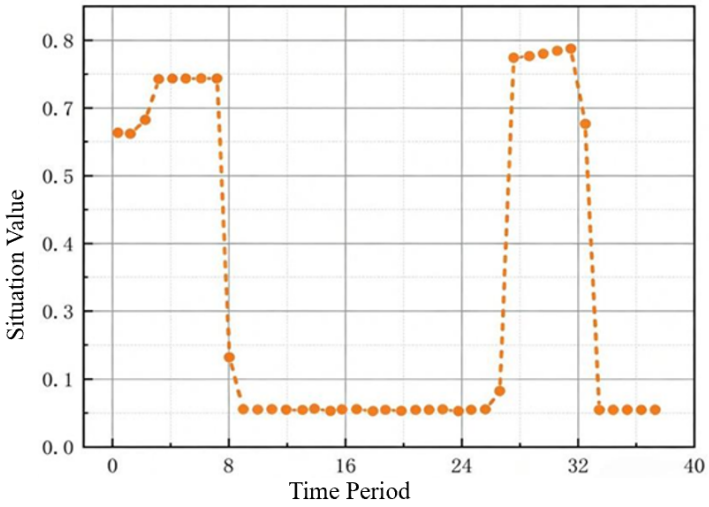

Figure 1. Ground-truth security situation values.

To quantitatively evaluate the performance of different models in the security situation prediction task, this study adopts the Mean Squared Error (MSE), Mean Absolute Percentage Error (MAPE), and the coefficient of determination (R^2) as evaluation metrics. Specifically, MSE measures the average squared deviation between the predicted values and the ground-truth values, MAPE reflects the relative magnitude of prediction errors, and R^2 evaluates the goodness of fit of the model to the data.

3.3. Experimental results and analysis

This section evaluates the performance of the proposed AGWO-BiGRU-ATTN model from three perspectives: prediction curve comparison, quantitative evaluation metrics, and model mechanism analysis. The proposed model is compared with several representative baseline models, including LSTM, BiGRU, and GWO-BiGRU. All comparative experiments are conducted under the same data partitioning strategy and parameter settings to ensure fairness, and the models are evaluated in terms of stability, convergence behavior, and prediction accuracy.

3.3.1. Comparison of network security situation prediction

To verify the prediction capability of the AGWO-BiGRU-ATTN model in IoT environments, the predicted security situation sequences of different models are first visualized and compared. The comparison involves AGWO-BiGRU-ATTN, BiGRU, GWO-BiGRU, and LSTM models. As shown in **Figure 2**, the prediction trend of the AGWO-BiGRU-ATTN model is highly consistent with the ground-truth situation values and exhibits a significant improvement over the other models.

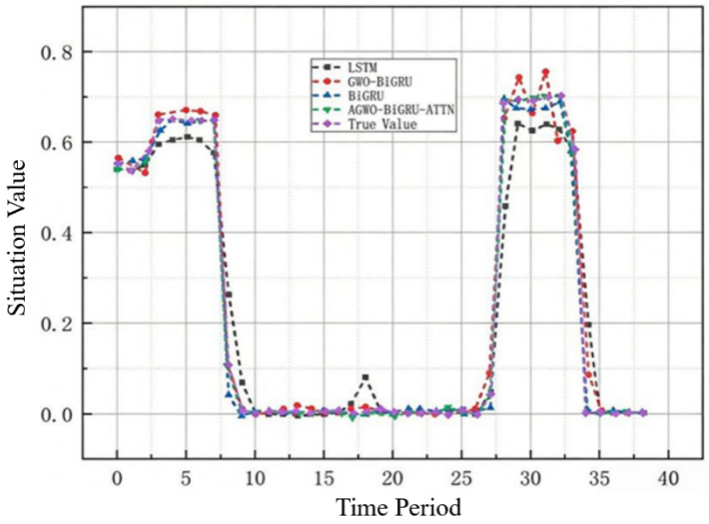

Figure 2. Comparison results.

3.3.2. Analysis of performance evaluation metrics

To further evaluate the performance of the proposed model in IoT security situation prediction tasks, **Table 2** presents the evaluation results of different models in terms of MAPE, MSE, and R^2. The comprehensive evaluation based on these three metrics indicates that AGWO-BiGRU-ATTN not only significantly reduces prediction errors but also more accurately captures the complex fluctuations inherent in IoT security situations. The observed performance gains can be attributed to the superior hyperparameter configurations obtained by AGWO during the optimization stage, which enable the BiGRU-ATTN model to achieve more stable and efficient performance when dealing with non-stationary and high-noise time-series data.

Table 2. Comparison of model performance

Model name	MAPE/%	R^2	MSE
AGWO-BiGRU-ATTN	19.33	0.972	0.00310
GWO-BiGRU	30.62	0.932	0.00578
BiGRU	35.47	0.885	0.00925
LSTM	40.25	0.867	0.01127

4. Conclusion

This paper addresses the limitations of existing prediction models in dynamically capturing IoT security situations, and proposes an IoT security situation prediction model based on AGWO-optimized BiGRU-ATTN. The model precisely extracts key features from temporal data through a self-attention mechanism, thereby enhancing the stability of model training. GWO undertakes parameter optimization tasks within the model, enabling more efficient capture of security situation changes in dynamic environments, and thus further improving the model's prediction accuracy. Experimental results demonstrate that the model exhibits significant advantages in both accuracy and stability.

Disclosure statement

The author declares no conflict of interest.

References

[1] Begum M, Yogeshwaran A, Nagarajan N, et al., 2025, Dynamic Network Security Leveraging Efficient CoviNet with Granger Causality-Inspired Graph Neural Networks for Data Compression in Cloud IoT Devices. Knowledge-Based Systems, 2025(309): 112859.

[2] Jablaoui R, Liouane N, 2025, Network Security Based Combined CNN-RNN Models for IoT Intrusion Detection System. Peer-to-Peer Networking and Applications, 18(3).

[3] Zhang S, Fu Q, An D, 2023, Network Security Situation Prediction Model Based on VMD Decomposition and DWOA Optimized BiGRU-ATTN Neural Network. IEEE Access, 2023(11): 129507–129535.

[4] Du X, Ding X, Tao F, 2023, Network Security Situation Prediction Based on Optimized Clock-Cycle Recurrent Neural Network for Sensor-Enabled Networks. Sensors, 23(13): 6087.

[5] Yang H, Zhang Z, Xie L, et al., 2022, Network Security Situation Assessment with Network Attack Behavior Classification. International Journal of Intelligent Systems, 37(10): 6909–6927.

[6] Rahul D, Salem F, 2017, Gate-Variants of Gated Recurrent Unit (GRU) Neural Networks, Midwest Symposium on Circuits and Systems, 1597–1600.

[7] Moustafa N, 2021, A New Distributed Architecture for Evaluating AI-based Security Systems at the Edge: Network TON_IoT Datasets. Sustainable Cities and Society, 2021(72): 102994.

[8] Zhao D, Wu Y, Zhang H, 2022, Network Security Situation Prediction based on IPSO-BiLSTM. Computer Science, 49(7): 357–362.