Journal of Systems Engineering and Electronics
Vol. 35, No. 2, April 2024, pp.361 – 373

Aerial target threat assessment based on gated recurrent unit and self-attention mechanism

CHEN Chen[1,2], QUAN Wei[1,2,*], and SHAO Zhuang[1,2]

1. School of Automation, Beijing Institute of Technology, Beijing 100081, China;
2. State Key Laboratory of Intelligent Control and Decision of Complex Systems, Beijing 100081, China

Abstract: Aerial threat assessment is a crucial link in modern air combat, whose result counts a great deal for commanders to make decisions. With the consideration that the existing threat assessment methods have difficulties in dealing with high dimensional time series target data, a threat assessment method based on self-attention mechanism and gated recurrent unit (SA-GRU) is proposed. Firstly, a threat feature system including air combat situations and capability features is established. Moreover, a data augmentation process based on fractional Fourier transform (FRFT) is applied to extract more valuable information from time series situation features. Furthermore, aiming to capture key characteristics of battlefield evolution, a bidirectional GRU and SA mechanisms are designed for enhanced features. Subsequently, after the concatenation of the processed air combat situation and capability features, the target threat level will be predicted by fully connected neural layers and the softmax classifier. Finally, in order to validate this model, an air combat dataset generated by a combat simulation system is introduced for model training and testing. The comparison experiments show the proposed model has structural rationality and can perform threat assessment faster and more accurately than the other existing models based on deep learning.

Keywords: target threat assessment, gated recurrent unit (GRU), self-attention (SA), fractional Fourier transform (FRFT).

DOI: 10.23919/JSEE.2023.000116

1. Introduction

In modern air-to-air combat, target threat assessment plays a significant role in improving the operational efficiency and self-survival probability of our aerial unit [1]. Its main task is to analyze the situation information of enemy targets (aircraft, missiles, etc.) detected by our aerial unit's sensors, evaluate the threat degree of enemy combat units, and provide effective references for situation awareness [2] and decision-making [3] for our commanders. Generally, the higher the threat level of the target, the more dangerous it is, and the higher the priority of weapon allocation.

At present, threat assessment focuses mainly on the air battlefields. The most common traditional theories are operations research and statistical methods, such as multi-attribute decision-making theory [4], technique for order preference by similarity to an ideal solution (TOPSIS) theory [5], Bayesian network [6], and fuzzy theory [7]. Zhen et al. [6] established the threat indicator system and constructed a threat level model based on expert experience and dynamic Bayesian theory, which can reliably and dynamically evaluate the threat of group targets in complex environments. Gao et al. [8] and Xu et al. [9] combined the intuitionistic fuzzy theory with the multi-attribute decision-making method to handle the target threat assessment. Due to the constraint that the traditional methods depend on subjective experience, these methods mainly focused on some specific scenarios with small-scale data. Some troubles of these methods will be exposed when dealing with problems with large-scale data threat assessment.

With the rapid development of battlefield big data technology, how to process nonlinear and complex information in the battlefield situation has become a difficult issue. Meanwhile, the availability of large datasets and rapid software and hardware advances enables artificial intelligence technology to grow dramatically [10]. Machine learning and deep learning inspired some scholars to establish threat assessment models for medium and large-scale situation data. Yang et al. [11] combined the *k*-means method with the analytic hierarchy process. This combination not only improves the data scale the model can handle but also overcomes the subjectivity of a single evaluation method. Wang et al. [12] designed an air

Manuscript received August 17, 2022.
*Corresponding author.
This work was supported by the National Natural Science Foundation of China (62022015; 62088101), Shanghai Municipal Science and Technology Major Project (2021SHZDZX0100), and Shanghai Municipal Commission of Science and Technology Project (19511132101).

target threat assessment model based on rough set theory and support vector machine (SVM), which is an effective attempt to apply machine learning to threat assessment.

When the scale of situation data increases to a certain degree, the disadvantages of machine learning algorithms are highlighted: feature selections have shown immense influence on the evaluation results and the solution speed. Therefore, threat assessment models based on deep learning have been proposed. Through learning a large number of data generated by expert systems or other methods, the deep learning method can facilitate continuously improving the generalization ability of the model, reduce the subjectivity of a single commander, and establish a model with rapidity and high accuracy. Chen et al. [13] integrated wavelet transformation into a neural network optimized by the genetic algorithm. The threat assessment model achieved good adaptive resolution, fine approximation ability, and fault tolerance. Zhai et al. [14] introduced the residual structure into the fully connected neural network to improve the accuracy of the evaluation of individual targets' threats. Yue et al. [15] optimized the grey neural network evaluation model with an improved moth extinguishing algorithm and verified the effectiveness of the model through simulation experiments. Yuan et al. [16] and Xi et al. [17] introduced intelligent optimization algorithms to optimize the parameter of the extreme learning machine (ELM) model, which effectively shortened the training time of the threat assessment model. The models in [13−17] are mainly based on multi-layer perceptron. Although they have been improved in different aspects, the main problems of these multilayer perceptron models still remain, such as parameter inflation, falling into local optimization, and difficulty in handling high-dimensional timing data.

Based on the above analysis, traditional threat assessment methods have limited ability to process large-scale time series situation data on the battlefield. Aiming to assess the aerial threat in air-to-air combat, a deep learning based assessment method is proposed to deal with these difficulties. Initially, a threat characteristic system is designed, which divides the threat features into air combat situation features and air combat capability features. Furthermore, on the basis of the encoder-decoder network structure, a threat assessment model based on the self-attention mechanism and gated recurrent unit (SA-GRU) is proposed. To be specific, the air combat situation features are firstly augmented based on fractional Fourier transform (FRFT) to expand the form of feature representation. Secondly, SA and GRU network are designed to extract the key time relationship between the enhanced data, and weaken the performance of redundant features. Thirdly, the extracted key situation feature information and air combat capability feature data are fused as the key input of the fully connected layers to obtain the threat level result of the target. Finally, through the comparison experiments, the proposed threat assessment method is verified to perform the characteristics of high accuracy and strong real-time. The major contributions are the followings:

(i) The SA-GRU model extends the machine learning based threat assessment method to satisfy the threat assessments with large-scale, high-dimensional, and time series situation data in modern air combat.

(ii) The data augmentation process is introduced to extract more high-dimensional abstract information in the air combat situation features. In the data augmentation process, FRFT is employed to map the limited air combat situation features into different frequency domains. After fusing the data with multiple FRFT with the original data, the difference between data will be amplified. This advantage of FRFT provides the SA-GRU model with more abundant situation features to analyze, making the threat assessment model more accurate.

(iii) The bidirectional GRU (BiGRU) structure and SA mechanism designed in this paper improve the classic encoder-decoder structure network based on GRU in air combat threat assessment. BiGRU structure is capable of extracting deep information on the historical status and subsequent flight status of the target in both directions. At the same time, the SA mechanism filters the features extracted by BiGRU, and gives high weights to key features. Benefited by these structures, the crucial evolution information can be captured and the accuracy of the model increases dramatically. It also provides a brand-new method for the design of threat assessments with time series data.

2. Threat feature system construction

The air combat target threat information includes the target timing information obtained by sensors as well as the uncertain information from the commander's experience, leading to the complexity, strong coupling, and nonlinearity of the combat information. Therefore, establishing a reasonable threat feature system is the basis of obtaining scientific evaluation results. Among massive factors influencing the target threat degree, the features to be selected should not only meet the requirements of completeness, significance, and commonality but also reflect nonlinear relations between the enemy situation data and the threat degree.

With the comprehensive consideration of the detection capability and air combat features of airborne equipment, a threat feature system is constructed from two aspects:

air combat capability and air combat situation, as shown in Fig. 1. The air combat capabilities represent the static attributes of targets, including target type, strike capability, and jamming capability. The air combat situations indicate the target's dynamic attributes from the time sequence situation information, including angle threat, speed threat, and distance threat of the target.

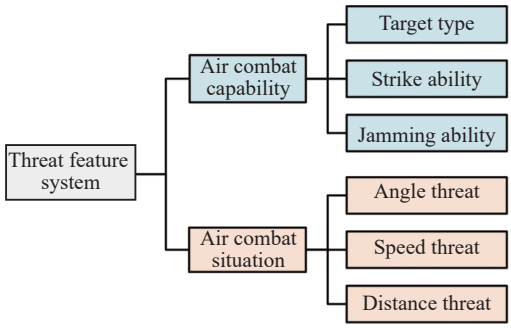


Fig. 1 Threat feature system

2.1 Air combat capability features

Account of the qualitative characteristics of air combat capability, the description language of these features needs to be quantified. Three typical air combat capability features are considered and processed based on the nine-level quantification theory [18].

(i) Target type. In air combat, different types of targets have their own features in attack intention, attack mode, and attack intensity, resulting in different threat degrees. This paper divides the target type into large targets (such as bombers, fighters, and missiles), medium targets (such as jammers and armed helicopters), and small targets such as unmanned aerial vehicles (UAVs) and reconnaissance aircraft. These target types' threat values are quantified as 0.9, 0.6, and 0.3 respectively.

(ii) Strike ability. Strike ability refers to the ability of the target to cause damage without being affected by the defense system. The stronger the target strike, the greater the lethality to our side, and the greater the threat. Divide the strike ability into very strong, strong, relatively strong, medium, relatively low, and low, which is quantified as 0.9, 0.8, 0.6, 0.5, 0.4, and 0.3 in turn.

(iii) Jamming ability. Jamming capability represents the targets' ability to destroy or disturb our radio equipment through their communication countermeasure equipment. The jamming capability is divided into four types: strong, medium, weak, and none, corresponding to 0.8, 0.6, 0.4, and 0.2.

2.2 Air combat situation features

Air combat situation features belong to complex time sequence data, reflecting the movement of attack targets and the transformation of battlefield situations. This paper mainly selects three typical air combat situation features: angle threat, speed threat, and distance threat [19].

(i) Angle threat. Motivated by [20,21], in which scholars adopt the attack angle of both sides to directly measure the threat value of the angle, this paper employs the attack angles of red army's weapons and the blue army's weapons to reflect the threat of angles. When red army's firepower is opposite to the target, the threat of the target would be greater. Meanwhile, the threat would be higher if the blue army's attack angle is toward the red army. As shown in Fig. 2, θ_W represents the angle the red army weapon deviates from the blue army's. The increase of θ_W would cause deviation from the enemy, meaning that the red army cannot quickly turn to attack the blue army. Thus, a higher threat shall be given. θ_T represents the angle of the blue army's weapon attack direction opposite to red army. As the angle increases, the blue army's weapons will gradually turn to the red army, resulting in the rise of threat. Both θ_W and θ_T have strong positive correlations with the angle threat. Therefore, the following angle threat equation is adopted:

$$T_{ij}^{a} = \frac{\theta_W + \theta_T}{360^\circ} \tag{1}$$

where the sum of θ_W and θ_T is employed to indicate the angle threat which ranges from 0 to 1 through normalization.

Fig. 2 further shows the relationship of (1) and the angle threat.

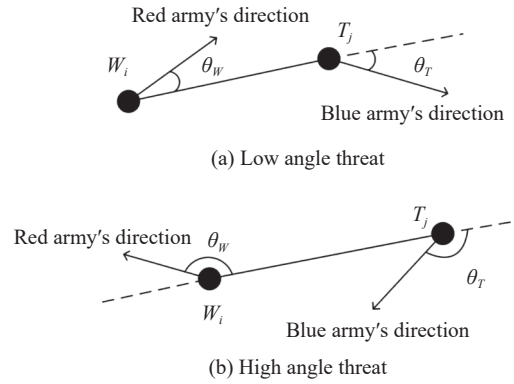


Fig. 2 Sketch map of the angle threat situation

The situation with a small threat value is shown in Fig. 2 (a). At this time, the red army's weapons point at the blue army, and the blue army's attack angle is away from the red army. Therefore, red army's direct attack on the target is prevailing while the blue army is difficult to fight back, resulting in a small threat. As the two angles increase, the red army's weapons are close to the opposite direction of the blue army, and the blue army's

weapons will directly point at the red army (Fig. 2 (b)). It is more likely to be directly attacked and difficult to quickly counter attack, leading to a greater threat.

(ii) Speed threat. Target speed reflects the change of target motion. Since both sides of the combat are air-moving bodies, the speed of red army's aerial unit and the blue army' are both relevant to the target's speed threat, indicating that the relation between their speeds must be considered. In specific, when red army's speed prevails over the blue army's, a threat caused by the blue army would be relatively small owing to red army's advantage in mobility. Furthermore, as the blue army's speed rises, its locomotivity would be strengthened, leading to an increase in the speed threat. Moreover, a high threat shall be given providing the blue army's speed is much over the red army's. Based on the above analysis, the threat of speed is divided into three sections, which are calculated by

$$T_{ij}^{v}=\begin{cases}0.1, & v_j \leqslant 0.6v_i\\ -0.5+\dfrac{v_j}{v_i}, & 0.6v_i < v_j \leqslant 1.5v_i\\ 1.0, & v_j > 1.5v_i\end{cases} \tag{2}$$

where v_j and v_i represent the speed of the target T_j and our aerial unit W_i.

In (2), the threat of speed is divided into three sections. When the blue army's speed is 0.6 times lower than the red army', it is considered that the blue army's mobility performance is far lower than the red army's, leading to a relatively low threat value of 0.1. Similarly, if the blue army's speed exceeds 1.5 times of the red army's, an extremely high threat value of 1 should be given to the blue army for its exceptional ability in speed. When the blue army's speed is within the above range, the threat value of the blue army will rise as the speed difference increases, from 0.1 to 1.

(iii) Distance threat. Target distance is a significant indicator to measure the threat degree of the target. Traditional target distance feature quantization only considers the distance between the two sides, which implies that the farther the distance is, the less the threat is. Considering the influence of the maximum attack distance and physical distance of both sides, a comprehensive distance threat quantization method is designed in this paper.

Suppose D is the distance between the two sides, D_W is the maximum attack distance of the red army's weapon, and D_T is the maximum attack distance of the blue army's weapon. Considering the relation among D_T, D_W and D, the definition of the distance threat is processed by segments.

Given that distance D exceeds the range of the blue army's weapon D_T, the threat of the blue army's would be the least, namely $D > D_T$:

$$T_{ij}^{d}=0. \tag{3}$$

If the blue army's weapon is within range D_T, and the red army's weapon is beyond the range D_W, the highest threat will be generated, namely $D_W < D \leqslant D_T$:

$$T_{ij}^{d}=1. \tag{4}$$

Provided that both aerial units are in their ranges, the threat value will be decided by the relation of D_W and D_T, which can be divided into two situations.

When $D \leqslant D_W < D_T$, the blue army can attack the red army in a longer distance, leading to the circumstance that the red army's aerial unit would be attacked unilaterally before coming into the range. When the red army's unit initially comes into the distance capable of attacking the blue army, the threat of the blue army will decrease. Moreover, as the distance decreases, the influence of ranges would be slight, and the distance would be the dominant factor of the blue army's threat. The threat will rise as distance reduces. Hence, the distance can be calculated by

$$T_{ij}^{d}=\begin{cases}1-0.625\dfrac{D}{D_W}, & 0 < D \leqslant 0.8D_W\\ 2.5\dfrac{D}{D_W}-1.5, & 0.8D_W < D \leqslant D_W\end{cases}. \tag{5}$$

In (5), when the red army initially comes into the attack range ($0.8D_W < D \leqslant D_W$), the threat of the blue army will decrease from 1 to 0.5. Furthermore, if the distance between them is lower than 0.8 times of the red army's range, it is considered distance D would dominate the blue army's threat. As a result, the threat will rise from 0.5 to 1 as distance reduces.

When $D \leqslant D_T \leqslant D_W$, red army attack range exceeds the blue army's range. Before the blue army comes into its range, the red army can attack the blue army unilateral, indicating the least threat. Thus, when the blue army is close enough to attack the red army, the threat value would increase with the decrease of the distance. Hence, the definition of distance threat under $D \leqslant D_T \leqslant D_W$ is

$$T_{ij}^{d}=1-0.9\frac{D}{D_T}. \tag{6}$$

In (6), when the blue army shifts from the state of beyond range to the state that is able to attack the red army, the threat value would increase from 0.1 to 1 as distance reduces.

3. Air target threat assessment model based on SA-GRU

3.1 Problem description and analysis

Air combat situation data has the characteristic of being complex and diverse. After being extracted from the feature system, the threat features data can be divided into two types: time series air combat situation features and static air combat capability features. Air target threat asse-

ssment is a process of extracting systematic threat features from situation information and classifying threat levels, which can be defined as a multi-classification problem.

Based on the above analysis, the air target threat assessment problem can be described in detail. Assuming that red army's sensor captures the situation information of multiple blue army targets, the threat feature set of the target i after extraction is defined as $O_i = \{D_i, S_i\}$, where $D_i = \{D_{i1}, D_{i2}, \cdots, D_{im}\}$ represent m air combat capability features of target i and $S_i = \{S_{i1}, S_{i2}, \cdots, S_{in}\}$ indicate n air combat situation features of it. Any element in the set S_i includes the time series information $S_{ij} = \{S_{ij}^{t+1}, S_{ij}^{t+2}, \cdots, S_{ij}^{t+\Delta t}\}$, which implies the jth time series feature of the target i from time $t+1$ to $t+\Delta t$. The goal of threat assessment can be described as evaluating the threat level r based on the threat feature set O_i, which can be mathematically described as $r = F(O_i)$. F represents the prediction function, which is the learning target of the threat assessment model.

3.2 Structure of the SA-GRU model

Target threat assessment is a mapping process from threat features to threat levels. The structure of the air target threat assessment model SA-GRU is shown in Fig. 3. The model input is threat feature data based on the threat feature system, including air combat situation features and air combat capability features. The model structure mainly includes three parts: situation feature augmentation, time series feature extraction, and feature fusion and classification.

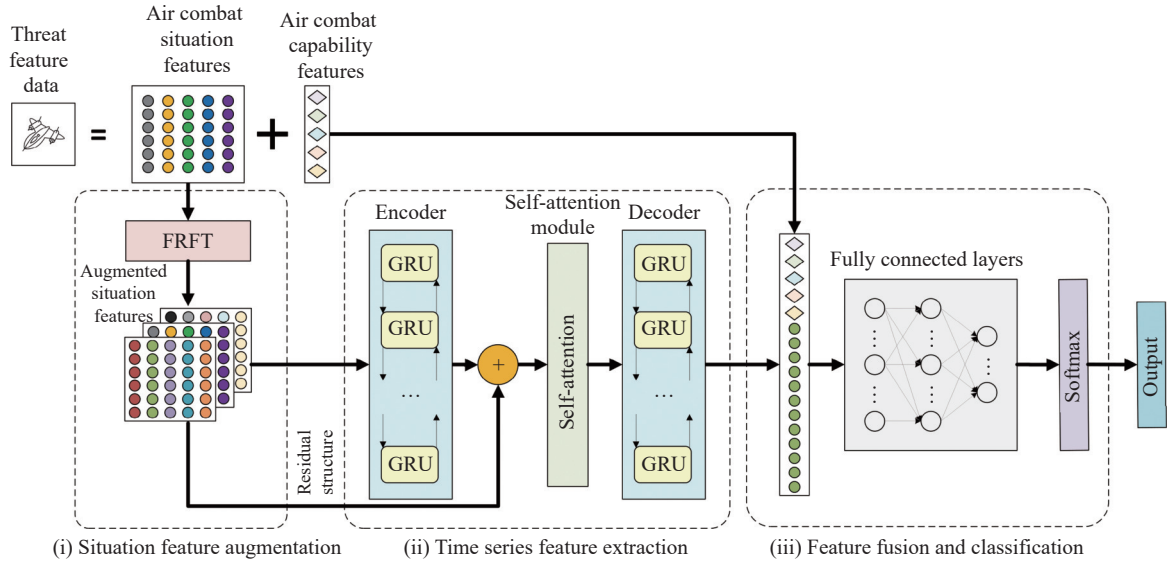


Fig. 3 Architecture of SA-GRU

The description of each part is as follows.

(i) Situation feature augmentation. The features of air combat situations are time series data with strong coupling and high complexity. Hence, to learn the potential time sequence relationship of air combat situation features and mine the evolution law of the battlefield, a data augmentation method based on FRFT is introduced to transform time sequence information into high-order abstract information.

(ii) Time series feature extraction. For the augmented high-dimensional situation features, an encoder-decoder neural network that embeds BiGRU structure is designed to handle the time relationship among situation features. Meanwhile, to reduce the impact of irrelevant features in high-dimensional data on the evaluation results, the self-attention mechanism is employed to weight the hidden states of all the time steps from the encoder.

(iii) Feature fusion and classification. The abstract situation features extracted from time series features are fused with air combat capability features by channel concatenation. Finally, the target threat classification level is obtained by fully connected layers.

3.3 Situation feature augmentation

Data augmentation technology enables the model to make full use of limited information, facilitating to improve the feature extraction ability and prediction accuracy of the model. The augmentation has two steps[22]: map the original situation data set $\boldsymbol{S}_{\text{raw}}$ to new feature set $\boldsymbol{S}_{\text{map}}$, and merge $\boldsymbol{S}_{\text{raw}}$ with $\boldsymbol{S}_{\text{map}}$ to obtain the augmented data $\boldsymbol{S}_{\text{aug}} = [\boldsymbol{S}_{\text{raw}}, \boldsymbol{S}_{\text{map}}]$.

Aiming to extract high-dimensional abstract features, a time series data augmentation technology based on FRFT is adopted which transforms the air combat situation fea-

tures into the frequency domain. FRFT is an important method for time-frequency analysis [23], mapping time domain data to different frequency domain spaces. For time series threat features, it is an effective method to extract high-dimensional abstract features. Through FRFT, air combat situations can be comprehensively interpreted, and the difference between data is fully amplified.

Denote the original air combat situation features as $\boldsymbol{S}_{\text{raw}} = [f_1(t), f_2(t), \cdots, f_N(t)]$, where $f_i(t)$ represents the time series feature data. The calculation process of FRFT on any $f_i(t)$ in $\boldsymbol{S}_{\text{raw}}$ is

$$f_p(u) = \int_{-\infty}^{+\infty} K_p(u,t) f(t) \mathrm{d}t \tag{7}$$

where

$$K_p(u,t) = \begin{cases} A_\alpha \exp[\mathrm{j}\pi(u^2\cot\alpha - \\ \qquad 2ut\csc\alpha + t^2\cot\alpha)], & \alpha \neq n\pi \\ \delta(u-t), & \alpha = 2n\pi \\ \delta(u+t), & \alpha = (2n+1)\pi \end{cases}. \tag{8}$$

In (8), $\alpha = p\pi/2$ indicates the angle between the time axis and the u axis with $p \in (0,1)$, and A_α is defined as

$$A_\alpha = \frac{\exp[-\mathrm{j}\pi\mathrm{sgn}(\sin\alpha)/4 + \mathrm{j}\alpha/2]}{|\sin\alpha|^{1/2}}. \tag{9}$$

Since each data in the air combat situation features can be regarded as a discrete signal, the application of (7) needs to be discretized. Ozaktas sampling discrete method [24] is adopted to adjust the transformation:

$$f_p(u) = \frac{A_\alpha}{2x} \sum_{-N}^{N} \exp\left(\mathrm{j}\pi\gamma u^2\right) \exp\left[-\mathrm{j}\pi\beta u\left(\frac{n}{2x}\right)\right] \cdot \left\{\exp\left[\mathrm{j}\pi\gamma u\left(\frac{n}{2x}\right)^2\right] f\left(\frac{n}{2x}\right)\right\} \tag{10}$$

where $\beta = \csc\alpha$, $\gamma = \cot\alpha$. The order p in A_α is an important parameter in FRFT, which considerably affects the performance [25].

The data augmentation process is shown in Fig. 4.

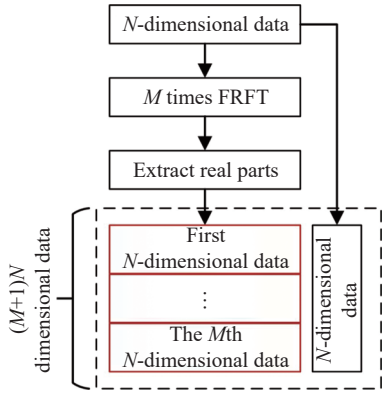


Fig. 4 Data augmentation process

Initially, all N dimensional data $\boldsymbol{S}_{\text{raw}}$ are mapped m times according to (10), and the real parts of the mapped data are taken as the new feature $\boldsymbol{S}_{\text{map}}$. Next, combine $\boldsymbol{S}_{\text{raw}}$ and $\boldsymbol{S}_{\text{map}}$ to obtain the enhanced feature $\boldsymbol{S}_{\text{aug}} = [\boldsymbol{S}_{\text{raw}}, \boldsymbol{S}_{\text{map}}]$, and the dimension of $\boldsymbol{S}_{\text{aug}}$ becomes $(M+1)N$.

Take battle simulation data as an example. The speed threat features of an enemy target over a period of time are extracted based on (2). Perform five FRFT with the parameter $p \in \{0.01, 0.02, 0.03, 0.04, 0.05\}$. The original speed threat feature data and the transformed data are shown in Fig. 5.

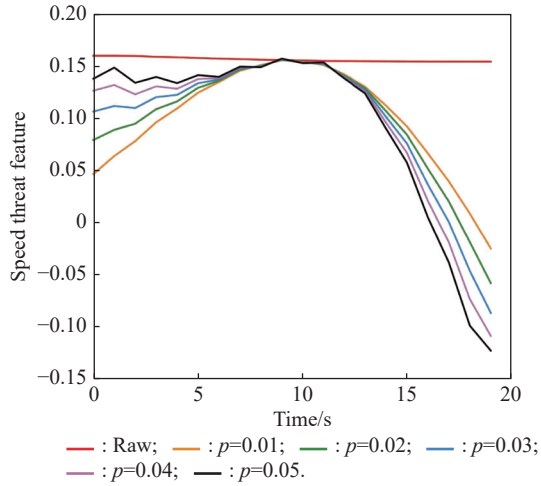


Fig. 5 Sketch of speed threat feature augmentation

Red represents the original speed threat feature, and the other colors are the results after the transformation of different orders. After FRFT, slight changes of speed threat features in time domain are fully reflected in the frequency domain, and the differences between features are amplified, which is conducive to improving the classification ability of the assessment model.

3.4 Time series feature extraction

3.4.1 Encoder-decoder structure

After data augmentation, the situation features become high-order complex sequences. In order to effectively learn the rich semantic information, an encoding-decoding structure based on sequence to sequence (seq2seq) is adopted. The main modules are encoder and decoder, which employ BiGRU network.

GRU network has ability to memorize time series information and effectively avoid the gradient vanishing problem. In the past few years, it has been widely applied in time series data processing. Compared with the popular time series feature extraction model short-term and long-term memory (LSTM) network, GRU introduces an

update gate to control the amount of information retained from the historical state, instead of additional memory units. Hence, relatively few parameters and a relatively small amount of calculation will be involved in GRU model. The structure of GRU is shown in Fig. 6.

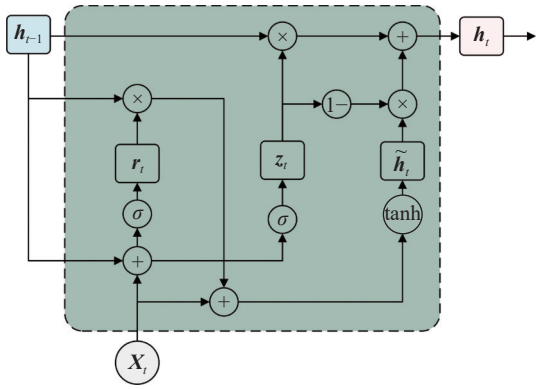


Fig. 6 Architecture of GRU

The input of each unit is the state at time t and the hidden state at time $t-1$, and the output is the hidden state at the current time. The status update method of GRU network is

$$\boldsymbol{r}_t = \sigma(\boldsymbol{W}_r x_t + \boldsymbol{U}_r \boldsymbol{h}_{t-1} + \boldsymbol{b}_r), \tag{11}$$

$$\boldsymbol{z}_t = \sigma(\boldsymbol{W}_z \boldsymbol{x}_t + \boldsymbol{U}_z \boldsymbol{h}_{t-1} + \boldsymbol{b}_z), \tag{12}$$

$$\tilde{\boldsymbol{h}}_t = \tanh[\boldsymbol{W}_h \boldsymbol{x}_t + \boldsymbol{U}_h(\boldsymbol{\rho}_\tau \odot \boldsymbol{h}_{t-1}) + \boldsymbol{b}_h], \tag{13}$$

$$\boldsymbol{h}_t = \boldsymbol{z}_t \odot \boldsymbol{h}_{t-1} + (1 - \boldsymbol{z}_t) \odot \tilde{\boldsymbol{h}}_t, \tag{14}$$

where $\boldsymbol{W}_r, \boldsymbol{W}_z, \boldsymbol{W}_h$ are weight matrices, $\boldsymbol{b}_r, \boldsymbol{b}_z, \boldsymbol{b}_h$ are bias vectors, $\boldsymbol{z}_t$ and $\boldsymbol{r}_t$ are update gate and reset gate, σ states Sigmoid function, and $\odot$ represents Hadamard product of matrices.

In the actual battlefield environment, the situation threat degree of the target at a certain time is dynamically related to the historical status and subsequent status. However, GRU is only able to sense the context information in the forward direction, leading to difficulties in learning the relationship between the future and current status in the reverse direction. Therefore, the BiGRU module is adopted in the encoder and decoder to extract the deep information in the enhanced feature from the forward and backward directions. The BiGRU structure is shown in Fig. 7.

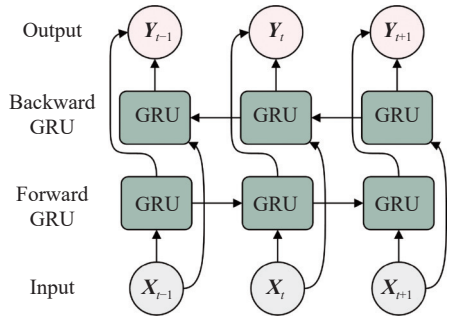


Fig. 7 Architecture of BiGRU

In BiGRU, two GRU networks with opposite directions are employed to process sequential and reverse situation feature sequences respectively. The output of the model is the combination of hidden layer states in two directions

$$\boldsymbol{Y}_t = [\mathrm{GRU}(\boldsymbol{X}_t, \boldsymbol{h}_{t-1}^f), \mathrm{GRU}(\boldsymbol{X}_t, \boldsymbol{h}_{t+1}^b)] \tag{15}$$

where $\boldsymbol{h}_{t-1}^f$ represents the hidden layer states of the forward GRU, and $\boldsymbol{h}_{t+1}^b$ represents the hidden layer states from the backward GRU.

3.4.2 SA mechanism

Due to the structure characteristic, the encoder-decoder module will compress the input sequence on the last output vector of the encoder. When the input sequence is too long, the weight assigned to the effective information will be reduced, resulting in the omission of high-value input information. SA mechanism is widely used to model relationship among information from sequences [26]. Therefore, to solve the problem of information compression in long sequences, the SA module is designed [27]. In the structure shown in Fig. 3, an SA module is added between the decoder and encoder to enhance the dependency information among time series. Meanwhile, a residual mechanism is introduced to prevent the gradient from disappearing during network training. The procedure of the self-attention mechanism is presented as follows.

Step 1 Calculate the output sequence of the encoder model $\boldsymbol{S}_{\text{out}}$ through the augmented input situation sequence $\boldsymbol{S}_{\text{aug}} = [\boldsymbol{s}_1, \boldsymbol{s}_2, \cdots, \boldsymbol{s}_N]$.

Step 2 Combine the input sequence $\boldsymbol{S}_{\text{aug}}$ and processed sequence $\boldsymbol{S}_{\text{out}}$ to get the input feature of the attention model $\boldsymbol{H} = \boldsymbol{S}_{\text{aug}} + \boldsymbol{S}_{\text{out}} = [\boldsymbol{h}_1, \boldsymbol{h}_2, \cdots, \boldsymbol{h}_N]$.

Step 3 Map feature $\boldsymbol{H}$ to three linear spaces by linear transformations to obtain the query matrix $\boldsymbol{Q}$, key matrix $\boldsymbol{K}$, and value matrix $\boldsymbol{V}$:

$$\begin{cases} \boldsymbol{Q} = \boldsymbol{H}\boldsymbol{W}_q \\ \boldsymbol{K} = \boldsymbol{H}\boldsymbol{W}_k \\ \boldsymbol{V} = \boldsymbol{H}\boldsymbol{W}_v \end{cases} \tag{16}$$

in which $\boldsymbol{W}_q, \boldsymbol{W}_k, \boldsymbol{W}_v \in \boldsymbol{R}^{\mathrm{N}\times\mathrm{d}}$ are the parameter matries of three linear mappings determined by experiments.

Step 4 Normalize the attention weight matrix based on the following equation:

$$\boldsymbol{W}_{\mathrm{att}} = \mathrm{softmax}\left(\frac{\boldsymbol{Q}\boldsymbol{K}^{\mathrm{T}}}{\sqrt{d}}\right). \tag{17}$$

Step 5 Compute the weighted sum of the value matrix $\boldsymbol{V}$ and weights $\boldsymbol{W}_{\mathrm{att}}$ to obtain the output of the SA module $\mathbf{out}_{\mathrm{att}}$:

$$\mathbf{out}_{\mathrm{att}} = \boldsymbol{W}_{\mathrm{att}} \cdot \boldsymbol{V}. \tag{18}$$

Through the above procedures, the output information of the encoder module has been weighted with different values, which strengths the key features and weakens others.

3.5 Feature fusion and classification

The target threat degrees have a close relation to the features of the target air combat capability. Therefore, after extracting the time sequence relationship in the situation features, the output of the decoder $\boldsymbol{S}_{\mathrm{out}}$ and air combat capability feature $\boldsymbol{D}$ are concatenated to obtain the fusion feature, which is expressed as $\boldsymbol{M} = [\boldsymbol{S}_{\mathrm{out}}; \boldsymbol{D}]$. The fully connected network is applied to map the fusion features into threat categories by

$$\boldsymbol{y} = f(\boldsymbol{W}^{\mathrm{T}}\boldsymbol{M} + \boldsymbol{b}) \tag{19}$$

where $\boldsymbol{W}^{\mathrm{T}}$ states the weight matrix, and $\boldsymbol{b}$ represents the bias vector.

The probability of each threat level can be generated through the softmax function:

$$p_i = e^{z_i} / \sum_{j=1}^{N} e^{z_j}, \ \ i \in [1, N] \tag{20}$$

where p_i indicates the probability of threat level i, Z_i is the score of the ith output of the fully connected layer.

Finally, the threat level with the highest probability would be selected as the current output of the network.

3.6 Loss function

In virtue of the multi-classification nature of the target threat assessment problem, the cross-entropy function is employed as the loss function:

$$\mathrm{Loss} = -\frac{1}{M}\sum_{i=1}^{M}\sum_{j=1}^{N} p(x_{ij}) \ln[q(x_{ij})] \tag{21}$$

where M represents the number of samples, N is the number of threat level categories, $p(x_{ij})$ states the expected probability that the ith sample has the jth threat level, and $q(x_{ij})$ indicates the output probability of the model.

4. Simulation experiments and result analysis

4.1 Dataset generation and processing

Since no public battlefield situation dataset exists in this research area, this paper generates the original situation information through a combat simulation system. Through multiple groups of combat scenarios simulated in this system, an assessment dataset is generated based on the data collected in the simulation deduction.

A battle scenario is shown in Fig. 8.

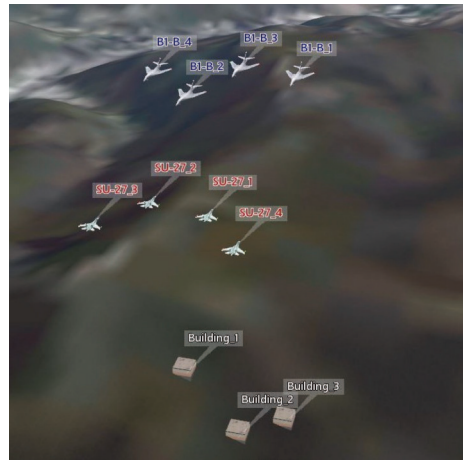


Fig. 8 Air combat scenario

The blue army sent four planes to attack the red army, while the red army had four fighters to fight with them and protect three buildings. During simulation, the red army's sensor will capture the enemies' information continuously and transmit it to the background, including the position, speed, and other information.

Extract multiple groups of air-to-air combat counter information from the system as the original dataset. Meanwhile, referring to the structure entropy weight method in [16], the threat level of all targets at each time step is calculated as set L. To make the dataset more suitable for training, sample data is preprocessed as follows.

Step 1 Extract the target air combat situation and capability features based on the index system from the simulation system, which is denoted as $\boldsymbol{S}$ and $\boldsymbol{D}$ respectively.

Step 2 Aiming to avoid the impact of data with huge dimensions on small dimension index data [28], combat situation data S_{ij} is normalized. The normalized element S'_{ij} can be calculated by

$$S'_{ij} = \frac{S_{ij} - \min(S_{ij})}{\max(S_{ij}) - \min(S_{ij})}. \tag{22}$$

Step 3 Based on (10), enhance all air combat situation features in $\boldsymbol{S}_{\text{nor}}$ for five times with parameter $p = \{0.1, 0.3, 0.5, 0.7, 0.9\}$. The enhanced data set is denoted as $\boldsymbol{S}_{\text{aug}}$.

Step 4 In order to enable the form of input data to meet the actual battlefield demand, $\boldsymbol{S}_{\text{aug}}$ is reconstructed by sliding window [29].

Initially, fix the sliding window with a time step of 100. Subsequently, extract the data of this sliding window size from $\boldsymbol{S}_{\text{aug}}$, and aggregate it with the corresponding data from set $\boldsymbol{D}$. Furthermore, choose the threat level in set $\boldsymbol{L}$ at the last timestamp t of the sliding window as the corresponding label of the current sliding window data. Finally, move the sliding window to the next time step until all data processing is completed.

After the above procedures, the threat assessment dataset is created with a total of 75 751 samples, and the threat levels range from 1 to 11. The specific information is shown in Table 1.

Table 1 Information of threat assessment dataset

Threat level	Samples number	Ratio/%
1	7 124	9.40
2	6 412	8.46
3	11 809	15.59
4	10 346	13.66
5	6 689	8.83
6	5 420	7.16
7	6 085	8.03
8	7 665	10.12
9	8 891	11.74
10	3 310	4.37
11	2 000	2.64

For the threat assessment dataset, divide 70% of it into the training set, 10% into the validation set, and the remaining 20% into the test set to verify the performance of the model.

4.2 Evaluation metrics

Metrics for the evaluation are further discussed. In machine learning, true positive (TP) and true negative (TN) denote the correctly predicted positive samples and negative samples, respectively; false positive (FP) represents the scenario that the actual class is negative and the predicted class is positive [30]; false negative (FN) represents the opposite situation of FP.

Based on the above four parameters, this paper adopts accuracy, precision, recall, and $F1$-score to evaluate the comprehensive performance of the model.

Accuracy: This index states the proportion of the number of samples with correct classification to the total number of samples. The accuracy indicates the overall prediction performance of the model under all threat levels.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{FN} + \text{TN}} \tag{23}$$

Precision: It represents the proportion that the threat level predicted by the model is real. The higher precision is, the lower the false alarm is.

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{24}$$

Recall: This indicator represents the ratio of the targets correctly identified as level r to all incoming targets with threat level r.

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{25}$$

$F1$-score: The weighted macro average method is adopted to represent the harmonic average of accuracy and recall, which can reduce the impact of category imbalance on the results [31]. The higher F1-score behaves, the better the balance between accuracy and recall is achieved.

$$F1 = \sum_{i=1}^{L} \left(\frac{2P_i R_i}{P_i + R_i} \cdot \omega_i \right) \tag{26}$$

where ω_i is the proportion of level i in the total category, and L represents the number of total categories. P_i and R_i are precision and recall of the level i.

4.3 Experimental environment and parameters

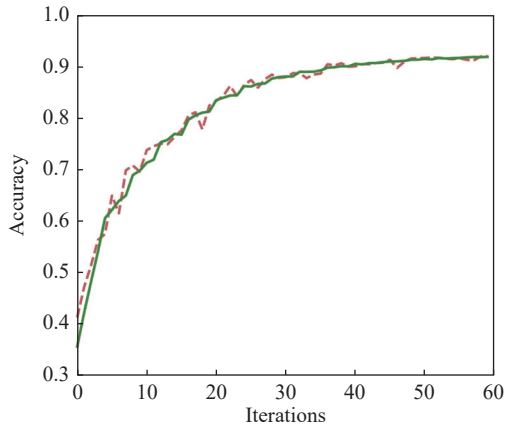
The proposed model is achieved based on PyTorch framework by Python 3.7.7. The hardware environment is Intel (R) Xeon (R) Silver 4210R CPU@2.40 GHz, 128G memory, NVIDIA GeForce RTX 3090 GPU.

The super parameters and training strategy are set as follows. The number of training iterations is set to 60. In the process of model training, the Adam optimizer is used to optimize model parameters with an initial learning rate value of 0.01, which decreases by 30% every five generations. For the encoder-decoder layer, the number of neurons in the encoder and decoder hidden layer is determined to be 64 by the grid search method of the range $\{32, 64, 128\}$. For fully connected layers, the number of layers is set to 3, and the number of hidden layer nodes

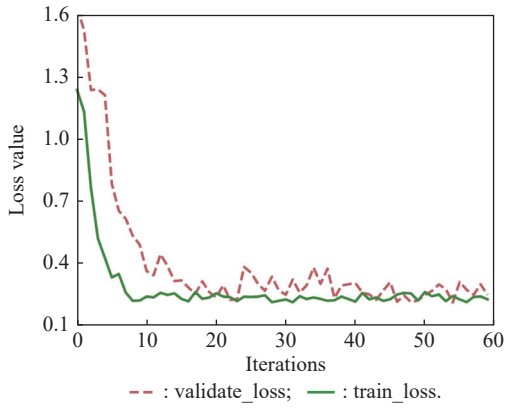
M is decided to be 115 according to the Kolmogorov formula $M=\sqrt{m+n+a}$, where m and n are the input and output data dimension, and $a\in\{x\in \mathrm{Z}|1\leqslant x\leqslant 10\}$.

4.4 Performance evaluation

Train the SA-GRU model with the training set and validation set, the accuracy and loss curve in the training process is shown in Fig. 9.



(a) Accuracy curve of SA-GRU



(b) Loss curve of SA-GRU

Fig. 9 Training curve of SA-GRU

From the curve, the trend of the validation curve is basically the same as the training curve. When the model starts training, the fluctuation range of the accuracy curve is relatively large. With the increase in the number of iterations, the fluctuation range of the curve decreases, and the model gradually converges. After training for 60 iterations, the loss and accuracy curves of the validation set reach convergence. The accuracy of the model exceeds 90%, and the value of the loss function is stable below 0.4.

The classification performance of SA-GRU under different threat levels based on the test is shown in Table 2.

Table 2 Performance of the SA-GRU %

Threat level	Precision	Recall	$F1$-score
1	92.5	92.0	92.3
2	93.2	91.3	92.2
3	90.6	82.5	86.4
4	89.7	92.7	91.1
5	95.7	93.9	94.8
6	81.9	99.0	89.6
7	84.0	56.8	67.7
8	79.8	77.0	78.0
9	82.5	87.1	84.7
10	93.4	90.7	92.0
11	93.5	91.8	92.6

The accuracy of the proposed model for most samples exceeds more than 90%, although the recognition ability for samples with threat levels of 7 and 8 is slightly poor. The classification result shows that the SA-GRU model can fit the data law of air combat features well and achieve an ideal classification effect.

4.5 Model comparison experiments

In order to further verify the effectiveness of the proposed model, three typical threat assessment models based on deep learning is selected for comparative experiments: the single-hidden-layer fuzzy recurrent wavelet neural network optimized by genetic algorithm (GA-SLFRWNN) [13]; ELM optimized by improved glowworm swarm (IGSO-ELM) [16]; ResNet [14], a fully connected neural network model combining batch standardization and residual structure. Meanwhile, the typical time series processing model LSTM-seq2seq model (LSTM-LSTM) [32] is also selected to compare with the proposed model.

Train the five models based on the threat assessment dataset. The accuracy curve during the training process is shown in Fig. 10.

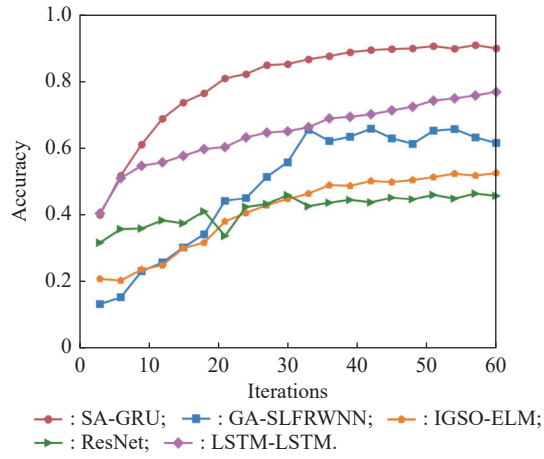


Fig. 10 Comparison of accuracy curves

From the change curve, SA-GRU model performs significantly better than other network models. The lowest oscillation amplitude of the accuracy curve and the highest convergence value of the model are shown in the SA-GRU, indicating that the proposed model can more effectively learn the relationship between enemy target threat feature data and threat level.

The performances of the different algorithms on test sets are shown in Table 3.

Table 3 Performance comparison %

Model	Accuracy	Precision	Recall	*F*1
SA-GRU	**90.4**	**90.4**	**90.5**	**90.3**
GA-SLFRWNN	64.2	64.2	64.1	63.4
IGSO-ELM	55.6	55.6	56.0	55.3
ResNet	41.9	41.9	43.5	36.0
LSTM-LSTM	76.7	79.3	77.4	77.4

From Table 3, SA-GRU model behaves better than the other four algorithms. Having partial similarity in structure, IGSO-ELM and ResNet are suitable for small-scale non-sequential data processing, leading to poor effects in large-scale sequential threat assessment experiments. Therefore, their classification accuracy is less than 60%. GA-SLFRWNN adopts the wavelet function as the neuron activation function, which improves the time-frequency analysis ability of the model [33], and can fit the threat feature data to a certain extent. However, its effect is still not ideal. Owing to inherent advantages in time series data processing, LSTM-LSTM can achieve a relatively better performance than the others except for SA-GRU.

Aiming to test the real-time quality of models, 10 000 pieces of data are selected from the data set as the input of five models to calculate the prediction time. The comparison of results is shown in Fig. 11.

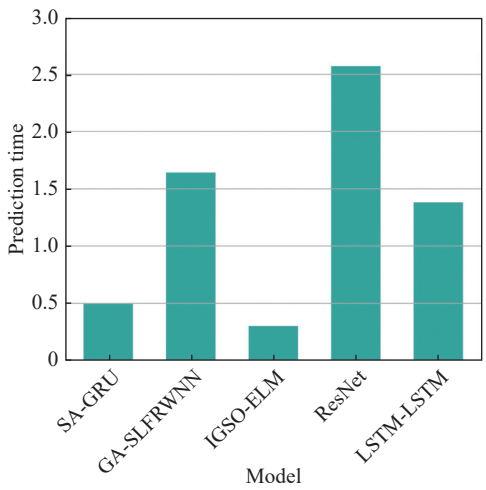


Fig. 11 Comparison of running time

Based on the experimental results, all models take less than 3 s when processing 10 000 data, meeting the real-time requirements. ResNet works in the longest prediction time of 2.57 s, and SA-GRU and IGSO-ELM run for less than 0.5 s, which takes the least time.

4.6 Ablation experiment

In order to verify the necessity of situation feature data augmentation and the rationality of model structure design, data ablation experiments and model structure ablation experiments are set up in this section.

In SA-GRU, the air combat situation features are augmented by the FRFT, increasing the data dimension from 3 to 18. To verify the effect of the data augmentation, the model with the dataset before and after augmentation is trained to compare the performance, as shown in Table 4.

Table 4 Performance comparison of data augmentation %

Augmentation	Accuracy	Precision	Recall	*F*1
No	60.3	69.7	60.3	57.0
Yes	**90.4**	**90.4**	**90.5**	**90.3**

Through data augmentation, the accuracy of the model increases from 60.3% to 90.4%, and the *F*1-score also has a high increase by 33.3%. Therefore, the FRFT assisted model obtains more abstract features, leading to a significant improvement of all metrics.

SA-GRU mainly includes three components: encoder-decoder structure (denote as seq2seq), SA module, and residual module. Aiming to evaluate the function of each module, all modules are combined with others, as shown in Table 5, where 0 means that the module is not applied and 1 means that the module is applied.

Table 5 Definition of combined model

Model	seq2seq	SA	Residual
ResNet	0	0	1
seq2seq	1	0	0
Res-seq2seq	1	0	1
SA-seq2seq	1	1	0
SA-GRU	1	1	1

Based on the threat assessment dataset, the classification performance of all combined models is shown in Table 6.

Table 6 Performance comparison of combined model %

Model	Accuracy	Precision	Recall	*F*1
ResNet	41.9	41.9	43.5	36.0
seq2seq	75.4	75.3	76.2	75.7
Res-seq2seq	80.0	79.6	80.1	79.8
SA-seq2seq	86.2	86.3	85.7	86.0
SA-GRU	**90.4**	**90.4**	**90.5**	**90.3**

As can be seen from Table 6, without the seq2seq structure and self-attention modules, the ResNet model only achieves relatively low behaviors, indicating that the combination of situation feature processed by the time series feature extraction module and the air combat capabilities contains more valuable information than the direct combination of them. Subsequently, due to the seq2seq structure's inherent advantages in processing time series data, its accuracy and $F1$-score reach 75.4% and 75.7%. Meanwhile, the accuracy and $F1$-score of the Res-seq2seq model are 4.6% and 4.1% higher than seq2seq respectively, indicating that the residual structure plays a certain role in improving the effectiveness of the model. Further more, all the indexes of the SA-seq2seq model exceed the first two, proving that the self-attention mechanism can effectively extract the depth information in the battlefield situation features and facilitate to improve the overall performance of the model. Among all the models, SA-GRU achieves the best behavior, verifying the effectiveness of the proposed structure and self-attention module in threat assessment missions.

5. Conclusions

Considering that the existing threat assessment methods are difficult to deal with high-dimensional time series target data, an air-to-air combat target threat assessment model SA-GRU is proposed. The SA-GRU model can simultaneously process high-dimensional time series situation features and static air combat capability features data. Through comparison and ablation simulation experiments, the following conclusions are drawn:

(i) Situation features augmentation enables the model to fully mine the deep information in battlefield evolution. Compared with no data enhancement, the classification accuracy of the model improves from 60.3% to 90.4%, leading to a significant improvement in the performance of the model.

(ii) SA mechanism assists to filter the features extracted by BiGRU by giving high weights to key features and weakening the others. Ablation experiments have proved the superiority of SA-GRU model structure.

(iii) SA-GRU model is able to better extract the time series relationship in the threat features and fuse them with the air combat capability features to realize the accurate identification of the target threat level.

(iv) The threat assessment model based on deep learning is capable of performing good nonlinear approximation ability and response speed. SA-GRU model can process large-scale situation data with faster speed and higher accuracy, meeting the requirements of real-time and accuracy.

References

[1] ZHANG K, KONG W, LIU P P, et al. Assessment and sequencing of air target threat based on intuitionistic fuzzy entropy and dynamic VIKOR. Journal of Systems Engineering and Electronics, 2018, 29(2): 305–310.

[2] XI Z F, XU A, KOU Y X, et al. Target maneuver trajectory prediction based on RBF neural network optimized by hybrid algorithm. Journal of Systems Engineering and Electronics, 2021, 32(2): 498–516.

[3] ZHANG J D, YANG Q M, SHI G Q, et al. UAV cooperative air combat maneuver decision based on multi-agent reinforcement learning. Journal of Systems Engineering and Electronics, 2021, 32(6): 1421–1438.

[4] KONG D P, CHANG T Q, WANG Q D, et al. A threat assessment method of group targets based on interval-valued intuitionistic fuzzy multi-attribute group decision-making. Applied Soft Computing, 2018, 67: 350–369.

[5] SUN H W, XIE X F. Threat evaluation method of warships formation air defense based on AR(p)-DITOPSIS. Journal of Systems Engineering and Electronics, 2019, 30(2): 297–307.

[6] ZHEN H F, BEN H S, JIN Y C, et al. A novel dynamic Bayesian network based threat assessment algorithm. Proc. of the 4th International Conference on Systems and Informatics, 2017: 611–615.

[7] ZHAO R J, YANG F B, JI L N, et al. Dynamic air target threat assessment based on interval-valued intuitionistic fuzzy sets, game theory, and evidential reasoning methodology. Mathematical Problems in Engineering, 2021, 2021: 6652706.

[8] GAO Y, LI D S, ZHONG H. A novel target threat assessment method based on three-way decisions under intuitionistic fuzzy multi-attribute decision making environment. Engineering Applications of Artificial Intelligence, 2020, 87: 103276.

[9] XU Y J, WANG Y C, MIU X D. Multi-attribute decision making method for air target threat evaluation based on intuitionistic fuzzy sets. Journal of Systems Engineering and Electronics, 2012, 23(6): 891–897.

[10] CHEN J, SUN J, WANG G. From unmanned systems to autonomous intelligent systems. Engineering, 2022, 12(5): 16–19.

[11] YANG C, XIA X C, LI T B, et al. Analysis of rationality of K-means cluster analysis in target threat assessment. Ship Electronic Engineering, 2017, 37(11): 21–23, 86. (in Chinese)

[12] WANG F, WU Z Q, SHI H Q. Research on anti-air threat assessment based on SVM. Fire Control & Command Control, 2018, 40(8): 1760–1768. (in Chinese)

[13] CHEN X, LIU Z L, LIANG H L. Assessment of aerial target threat based on genetic algorithm optimizing fuzzy recurrent wavelet neural network. Journal of Northwestern Polytechnical University, 2019, 37(2): 424–432. (in Chinese)

[14] ZHAI X Y, YANG F B, JI L N, et al. Air combat targets threat assessment based on standardized fully connected network and residual network. Fire Control & Command Control, 2018, 43(8): 66–69. (in Chinese)

[15] YUE L F, YANG R N, ZUO J L, et al. Air target threat assessment based on improved moth flame optimization-gray neural network model. Mathematical Problems in Engineering, 2019, 2019: 4203538.

[16] YUAN C, KOU Y X, AN X, et al. Target threat assessment in air combat based on improved glowworm swarm optimization and ELM neural network. International Journal of

Aerospace Engineering, 2021, 2021: 4687167.
[17] XI Z F, XU A, KOU Y X, et al. Target threat assessment in air combat based on PCA-MPSO-ELM algorithm. Acta Aeronautica et Astronautica Sinica, 2020, 41(9): 211–226. (in Chinese)
[18] XU J Q, BI Y M, LIANG W, et al. Airport threaten degree evaluation based on maximal deviations. Systems Engineering and Electronics, 2011, 33(8): 1816–1819. (in Chinese)
[19] LI S Y, CHEN M, WU Q X, et al. Threat sequencing of multiple UCAVs with incomplete information based on game theory. Journal of Systems Engineering and Electronics, 2022, 33(4): 986–996.
[20] XU X M, YANG R N, YU Y. Threat assessment in air combat based on ELM neural network. Proc. of the IEEE International Conference on Artificial Intelligence and Computer Applications, 2019: 114–120.
[21] LI S Y, WU Q X, CHEN M, et al. Air combat situation assessment of multiple UCAVs with incomplete information. Proc. of the Chinese Intelligent Systems Conference, 2021: 18–26.
[22] LI G Q, SONG Z Y, FU Q. A convolutional neural network based approach to sea clutter suppression for small boat detection. Frontiers of Information Technology & Electronic Engineering, 2020, 21(10): 1504–1520.
[23] GAO W B, LI B Z. Convolution theorem involving n-dimensional windowed fractional Fourier transform. Science China (Information Sciences), 2021, 64(6): 244–246.
[24] OZAKTAS H M, ARIKAN O, KUTAY M A, et a1. Digital computation of the fractional Fourier transform. IEEE Trans. on Signal Processing, 1996, 44(9): 2141–2150.
[25] WU X, TAO R, HONG D F, et al. The FrFT convolutional face: toward robust face recognition using the fractional Fourier transform and convolutional neural networks. Science China (Information Sciences), 2020, 63(1): 235–237.
[26] ZHANG X C, QIU X P, PANG J M, et al. Dual-axial self-attention network for text classification. Science China (Information Sciences), 2021, 64(12): 80–90.
[27] VASWANI A, SHAZEER N, PARMAR N, et al. Attention is all you need. Proc. of the 31st International Conference on Neural Information Processing Systems, 2017: 6000–6010.
[28] SHAO Z, CHEN C. Aerial battlefield targets grouping based on DTW-DBSCAN algorithm. Proc. of the 40th Chinese Control Conference, 2021: 3397–9402.
[29] HAN H, XIE T. Lane change trajectory prediction of vehicles in highway interweaving area using Seq2Seq-attention network. China Journal of Highway and Transport, 2020, 33(6): 106–118. (in Chinese)
[30] SU J Y, COOMBES M, LIU C J, et al. Machine learning-based crop drought mapping system by UAV remote sensing RGB imagery. Unmanned Systems, 2020, 8(1): 71–83.
[31] SABOR N, LI Y F, ZHANG Z, et al. Detection of the interictal epileptic discharges based on wavelet bispectrum interaction and recurrent neural network. Science China (Information Sciences), 2021, 64(6): 203–221.
[32] XIANG Z R, YAN J, DEMIR I. A rainfall-runoff model with LSTM-based sequence-to-sequence learning. Water Resources Research, 2020, 56(1): 165–181.
[33] GRAF R, ZHU S, SIVAKUMAR B. Forecasting river water temperature time series using a wavelet-neural network hybrid modelling approach. Journal of Hydrology, 2019, 578: 124115.

Biographies

CHEN Chen was born in 1982. She received her Ph.D. degree from Beijing Institute of Technology. She is a professor in Beijing Institute of Technology. Her research interests are intelligent optimization and decision-making of complex systems, and military operations research.
E-mail: xiaofan@bit.edu.cn

QUAN Wei was born in 1998. He received his B.S. degree from Beijing Institute of Technology in 2021. He is currently a master degree candidate in Beijing Institute of Technology. His research interests are battlefield situation assessment and effectiveness evaluation.
E-mail: 810765805@qq.com

SHAO Zhuang was born in 1997. He received his B.S. degree from Civil Aviation University of China in 2019. He received his M.S. degree from Beijing Institute of Technology in 2022. His research interests are battlefield situation understanding and machine learning.
E-mail: zshao_15@qq.com