Design of Network Security Assessment and Prediction Model Based on Improved K-means Clustering and Intelligent Optimization Recurrent Neural Network

Qianqian Wang[1], Xingxue Ren[2]*, Lei Li[3], Huimin Peng[4]
Henan Vocational University of Science and Technology, Zhoukou 466000, China[1, 2, 3, 4]
Henan Inland Port Logistics Information Engineering Technology Research Center, Zhoukou 466000, China[2, 3]

***Abstract*—Aiming at the security problems in cyberspace, the study proposes a cyber security assessment and prediction model based on improved K-means and intelligent optimization recurrent neural network. Firstly, based on traditional self-encoder and K-means algorithm, sparse self-encoder and K-means++ algorithm are proposed to build a cyber security posture assessment model based on improved K-means. Then, a two-way gated loop unit is used for security posture prediction, and a particle swarm optimization algorithm is utilized for enhancing the two-way gated loop unit, and the prediction is performed jointly with the model based on convolutional neural network. The results show that the proposed safety assessment model can react quickly when a fault occurs and is not prone to misjudgment with good stability. The accuracy of the safety assessment model was 99.8%, the running time was 0.277 s, and the recall rate was 96.67%, which was 96.49% in the F1 metric. The proposed safety prediction model has the lowest mean absolute error and root mean square error, which are 0.18 and 0.30. The running time is relatively long, which is 703.23 s and 787.46 s, but still within the acceptable range. The model-predicted posture values fit well with the actual posture values. In summary, the model constructed by the study has a good application effect and helps to ensure the security of cyberspace.**

***Keywords*—K-means; cybersecurity; situational assessment; situational prediction; self-encoder**

I. Introduction

A. Research Background

As the evolution of science, a variety of Internet technologies are applied to daily life and have a wide impact on social development. However, with the large-scale utilization of Internet technologies, the number and types of network attacks are also increasing, and network security is getting more and more attention [1]. Network security posture (SP) assessment and prediction is an important way to maintain network security. Network SP assessment refers to comprehensive security testing and analysis of network systems and applications to assess their current security status and existing security risks. The purpose of the assessment is to identify potential vulnerabilities and security threats and provide recommendations for improvements to protect the system from possible attacks and data leakage [2-3]. Cybersecurity posture prediction, on the other hand, predicts possible future security threats and attack methods by analyzing and modelling data on the current cybersecurity situation and trends [4]. Its purpose is to identify and respond to possible cybersecurity incidents in advance, thus reducing possible risks [5]. Cybersecurity posture assessment and cybersecurity posture prediction are of great significance for safeguarding network security, protecting data assets and maintaining the normal operation of the organization, which helps to improve the resilience and flexibility of network security, strengthen network protection and emergency response, and safeguard network security and information security.

B. Research Content and Innovation

However, most of the current posture assessment models have the problem of slow convergence, and most of the prediction methods are on the basis of a single model, with some limitations in prediction accuracy. In this context, the research will build a cyber security assessment (SA) model on the basis of improved K-means (KM) and a cyber security prediction model on the basis of intelligent optimized recurrent neural network (RNN). There are two main innovations in this research, the first one is to build the SA model by combining the sparse self-encoder and KM++ algorithm. The second point is the introduction of Convolutional neural network (CNN) for joint multi-model prediction on the basis of a single prediction model. The main structure of this article is divided into six sections, Section II analyzes the current state of the art of related research; Section III and Section IV builds a network SA model based on improved KM and a network security prediction model on the basis of intelligent optimization RNN; Section V is to analyze the application effect of the proposed models; and Section VI is to summarize the whole study.

II. Related Works

Cybersecurity is the protection of the hardware and software of a network system and the data in its system from accidental or malicious interruptions of network services. Sengupta et al. analyzed the recent advances in the development of moving target defenses in response to the problem that cyber defenses on the basis of traditional tools, techniques, and processes are unable to account for the

intrinsic strengths of attackers. It also demonstrated that the utilization of domain knowledge and game theory models can help defenders to develop effective movement strategies, which can help to identify new research areas and future research directions [6]. Guo et al. addressed the problem that integrated air, land and sea networks are facing serious security challenges, and detailed the latest progress and research work on integrated air, land and sea network security in terms of security threats, attack methods and defense countermeasures. Some discussions on cross-layer attacks and security countermeasures are also presented, and new challenges and research directions for the future are identified [7]. Wheelus and Zhu address the security issues and privacy leakage problems associated with cyber-attacks on the Internet of Things (IoT) by firstly reviewing the security risks about IoT systems, and then proposing a machine-learning based using a real-world IoT system [8]. Jain et al. addressed the issue of social networks and media where information travels very fast and is, therefore, more susceptible to attacks, carried out a comprehensive review of various threats and existing solutions and also discussed the defence methods for online social network security [9]. Mughal studied the wireless network security architecture fundamentals and design methods, and to illustrate how to effectively perform and keep robust wireless network security, real cases are also analyzed, which helps to provide a reference resource for researchers in wireless network security [10]. Yang et al. solve the poor timeliness and difficulty in effectively extracting features of the existing methods for assessing the cybersecurity posture, and propose a method based on the network SP assessment method based on network attack behaviour classification. The outcomes showcase that the proposed method possesses a high accuracy and recall rate, and can more comprehensively assess the overall posture of network security [11].

KM algorithm is the most classical division based clustering method and is widely used in maintaining cyber security. Alharbi et al. stated that many research has focused on emotional reflection on people's opinions and impressions, so a corpus was collected and provided with lightweight preprocessing techniques and KM clustering with potential Dirichlet allocation topic modeling approach was algorithm was validated. It helps to extract important themes from different texts [12]. Zhu et al. proposed an efficient data intrusion detection algorithm based on KM clustering and a network node control method that helps to protect the cybersecurity of the Internet of Things by clustering and analyzing the dataset with respect to the diversity and heterogeneity of the data captured in sensor networks. The outcomes showcase that the proposed method possesses better intrusion detection results compared to traditional intrusion detection methods [13]. Stiawan et al. addressed the problem that existing intrusion detection systems still have low detection accuracy because of the difficulty in recognizing the characteristics of denial of service attacks, wireless communication in different scenarios and generated clustering results utilizing KM algorithm and used confusion matrix to calculate the accuracy level. It helps to ensure the security of IoT [14]. Xu et al. proposed a density based KM algorithm for choosing the initial seed for clustering in response to the traditional KM clustering algorithm which is slow, unstable in accuracy, and difficult for satisfying the needs of big data. An improved K-dimensional tree nearest neighbor search is also used to improve the speed. The outcomes showcase that the proposed method possesses good stability [15]. Saheed et al. addressed the problem of how to improve the performance of classification algorithms for intrusion detection by proposing a proposed supervised and unsupervised learning techniques for detecting known and unknown attacks and applying KM clustering to normalized data. The outcomes showcase that the proposed model possesses more excellent robustness and performance with lower computational cost and can effectively reduce overfitting [16]. Liao and Li address the problem that it is hard for getting accurate labels for intrusion detection systems on the basis of supervised learning methods, and propose an anomaly detection model utilizing KM and active learning methods, which can help to build up a strong defense against cyber-attacks. The outcomes showcase that the proposed model possesses high detection accuracy, higher classification accuracy and better generalization [17].

In summary, many scholars carried lots of research on network security (NS) and affirmed the role of KM algorithm in maintaining NS. However, current network security assessment and prediction technologies still face issues such as the inability to accurately capture dynamic changes in network security risks and the inability to handle large-scale and complex data. Therefore, the design of network security assessment and prediction models based on improved K-means clustering and intelligent optimization of RNN has important practical application value and prospects. The Gated Recurrent Unit (GRU) structure of RNN can be used to effectively predict the dynamic state of network security risks, improving the accuracy of network security assessment and prediction.

III. NS Situation Assessment and Prediction Modeling

As the evolution of the number and types of attack techniques, the cybersecurity situation has become increasingly critical. In order to maintain the security of cyberspace, it is an effective measure to carry out the assessment and prediction of cyber SP. To this end, the study will build a cyber SP assessment model on the basis of improved KM and a cyber SP prediction model on the basis of intelligent optimized RNN.

A. NS Assessment Model Construction Based on Improved KM

NS posture assessment is designed to assess the current security status and existing security risks of network systems and applications through comprehensive security testing and analysis. A cybersecurity posture assessment typically includes the analysis and evaluation of network architecture, security policies, vulnerability scanning, security vulnerability exploitation testing, malware detection, and other components. Through a NS posture assessment, an organization can identify potential vulnerabilities and security threats to protect the system from possible attacks and data leakage, and understand its own weaknesses in NS as well as formulate appropriate security measures and prevention strategies. In order to assess the cybersecurity posture, this study firstly

employs an autoencoder to filter the redundant information in the data. Autoencoder (AE) is a kind of artificial neural network for unsupervised learning and data compression, which learns by characterizing the input information as a learning target [18]. AE mainly contains two parts, encoder and decoder, and the specific structure is showcased in Fig. 1.

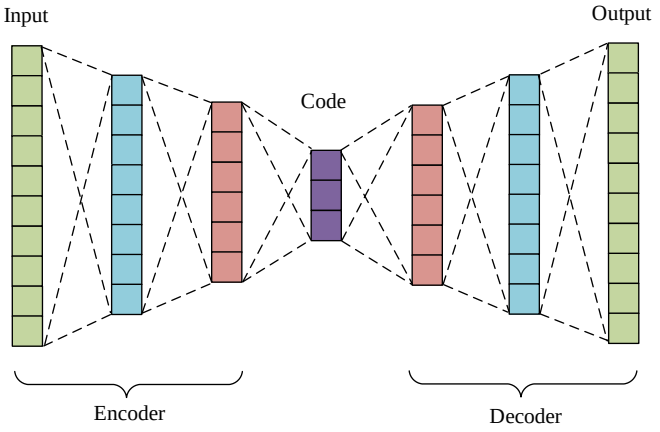

Fig. 1. The network structure of autoencoder.

In cybersecurity posture assessment, AE can be used for anomaly detection and identification of unknown threats. It can learn normal network traffic patterns and identify anomalous traffic that differs from normal behaviour, thus helping to detect potential cyber-attacks and security hazards. AE does not require labeled training data and can automatically learn potential features of the data. It can learn a valid representation of the data, which can help to extract important features of cybersecurity data. The ultimate goal of AE is to make the output maximally close to the output. First the encoder performs compression change on the unlabeled raw data $X[x_1, x_2, ..., x_n]$ to get $W[w_1, w_2, ..., w_m]$, then it is reconstructed by the decoder to get, $Y[y_1, y_2, ..., y_m]$ as showcased in Eq. (1).

$$\begin{cases} W = f_1(g_1 X + b_1) \\ Y = f_2(g_2 W + b_2) \end{cases} \tag{1}$$

In Eq. (1), f_1 and f_2 denote the activation functions of the hidden layer and the output layer. g_1 and g_2 denote the weight matrices of the encoder and decoder, respectively, which are usually made the same in order to simplify the model and facilitate training. b_1 and b_2 denote the bias. The model achieves the tuning of the parameters by minimizing the error function, as shown in Eq. (2).

$$\arg\min \|X - Y\| = 0 \tag{2}$$

The final parameters of the model can be obtained by continuously optimizing the weight matrix and bias so that the error function reaches the minimum value. The cross-entropy cost function is utilized in the process of model training, as shown in Eq. (3).

$$J(g,b) = -\frac{1}{n}\sum_{i=1}^{n}\frac{1}{2}\left(\left\|x^{(i)} - y^{(i)}\right\|^2\right) + \frac{\alpha}{2}\sum_{1=1}^{2}\sum_{i=1}^{S_2}\sum_{j=1}^{n}\left(g_{ji}^{(1)}\right)^2 \tag{3}$$

In Eq. (3), $\frac{1}{n}\sum_{i=1}^{n}\frac{1}{2}\left(\left\|x^{(i)} - y^{(i)}\right\|^2\right)$ denotes the mean square error term and $\frac{\alpha}{2}\sum_{1=1}^{2}\sum_{i=1}^{S_2}\sum_{j=1}^{n}\left(g_{ji}^{(1)}\right)^2$ denotes the weight attenuation term, which can prevent the model from overfitting. S_2 denotes the number of units in the hidden layer, and α denotes the weight decay parameter. However, AE cannot get a good compressed representation for feature extraction, so this study uses Sparse autoencoder (SAE) to extract features from security data. SAE continuously adjusts the parameters of AE by calculating the error between the output of the autoencoder and the original input, and finally trains the model, which can be utilized for compressing the input information and extract useful input features [19]. SAE works by adding sparse constraints to the AE so that most of the nodes are restricted to zero and only some of the non-zero nodes are retained. For the input x, the average activation value of the hidden neuron j is showcased in Eq. (4).

$$\hat{h}_j = \frac{1}{m}\sum_{i=1}^{m}\left[W_j(x^i)\right] \tag{4}$$

In Eq. (4), m serves as the number of data and $W_j(x^i)$ serves as the activation value of the hidden neuron. AE achieves sparsity by adding a penalty term and the penalty factor is shown in Eq. (5).

$$\sum_{j==1}^{S2} KL(h\|\hat{h}_j) = \sum_{j=1}^{S2}\left(h\log\frac{h}{\hat{h}_j} + (1-h)\log\frac{1-h}{1-\hat{h}_j}\right) \tag{5}$$

In Eq. (5), KL denotes the relative entropy. the total cost function of SAE is shown in Eq. (6).

$$J_s(g,b) = J(g,b) + \beta\sum_{j=1}^{S2} KL(h\|\hat{h}_j) \tag{6}$$

In Eq. (6), β denotes the weight of sparsity penalty factor weighing loss against classification interval, which is taken as 0.01 in this study. KM algorithm is an unsupervised clustering algorithm, which adopts the distance as the evaluation index of similarity, i.e., it is considered that the closer the distance between two objects, the more excellent the degree of similarity. It becomes the most widely used among all clustering algorithms because of its simple operation and high efficiency. However, the traditional KM algorithm is greatly affected by the initial point and K value, which will affect the iterations and even the clustering effect. For this reason, the study uses the KM++ algorithm for initialization improvement, so that the algorithm can find the initial center point with the best clustering effect and accelerate the convergence speed. The specific optimization strategy of the KM++ algorithm is shown in Fig. 2.

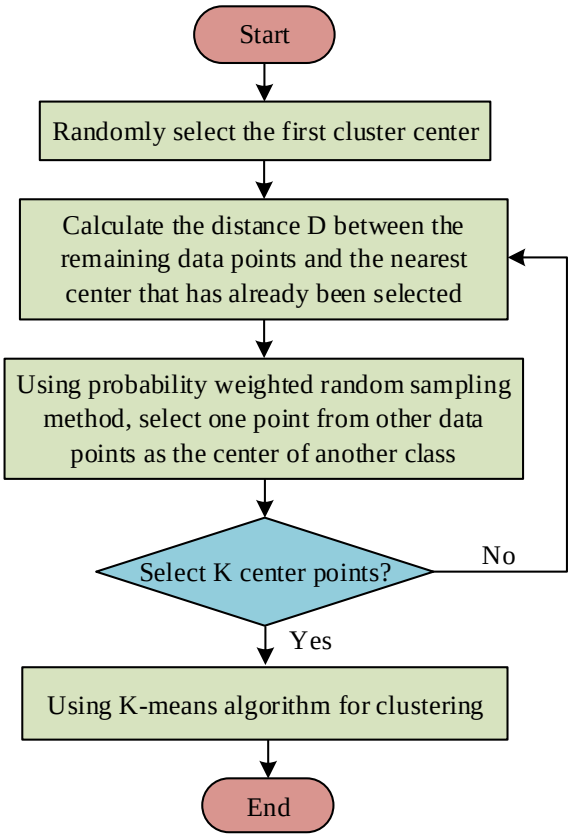

Fig. 2. Specific optimization strategies for K-means++ algorithm.

B. NS Prediction Model Building Based on Intelligent Optimization RNN

Cybersecurity posture prediction is the most critical aspect of cybersecurity posture awareness, which predicts the development trend and tendency of the cyber posture in the future period by reasonably analyzing the existing cybersecurity posture data. Most of the current prediction methods analyze the future trend on the basis of the posture time series. RNN has the advantages of memorability and parameter sharing for long term dependency, and is a commonly used method for predicting cybersecurity posture. Situation prediction requires high accuracy, and the prediction result should be as close as possible to the actual security situation value, which can be well achieved by RNN's memorization of long time series learning. Long Short-Term Memory (LSTM) and GRU are a kind of RNN, which are proposed to solve the shortcomings of RNN [20]. The performance of GRU is similar to that of LSTM, but with less computational overhead. The relevant structure is showcased in Fig. 3.

To further improve the accuracy of model prediction, this study introduces a bidirectional GRU on the basis of the traditional GRU to learn the posture time series data. The bi-directional GRU can learn all the SP attributes more comprehensively and reduce the errors in the posture prediction results. The bi-directional GRU includes a forward GRU and a backward GRU, and the forward GRU is updated as shown in Eq. (7).

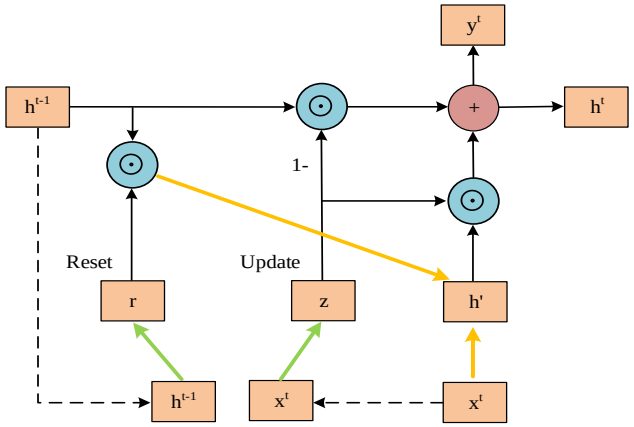

Fig. 3. Structure of Gated Recurrent Unit.

$$\begin{cases} z_t = \sigma\left(W_z \times \left[h_{t-1}, x_t\right]\right) \\ r_t = \sigma\left(W_r \times \left[h_{t-1}, x_t\right]\right) \\ \tilde{h}_t = \tanh\left(W \times \left[r_t * h_{t-1}, x_t\right]\right) \\ h_t = (1-z_t) * h_{t-1} + z_t * \tilde{h}_t \end{cases} \tag{7}$$

In Eq. (7), σ serves as the sigmoid function, W denotes the weights, h_{t-1} denotes the output of the GRU at the time of $t-1$, x_t denotes the input of the GRU at the time of t. The following are two gate control quantities that can control the flow and retention of information. z_t and r_t are two gate control quantities that can control its flow and retention, $\tilde{h}_t$ denotes the hidden state of the candidate, and h_t denotes the hidden state of the current time step. The backward GRU update is shown in Eq. (8).

$$\begin{cases} z_t = \sigma\left(W_z \times \left[h_{t+1}, x_t\right]\right) \\ r_t = \sigma\left(W_r \times \left[h_{t+1}, x_t\right]\right) \\ \tilde{h}_t = \tanh\left(W \times \left[r_t * h_{t+1}, x_t\right]\right) \\ h_t = (1-z_t) * h_{t+1} + z_t * \tilde{h}_t \end{cases} \tag{8}$$

On the basis of the single GRU situational prediction model, this study introduces CNN for joint prediction. CNN, along with RNN, is a representative model of neural networks, which is capable of mining and understanding data more comprehensively, although there is no concept of temporal order, and it is also widely used in the security situational prediction [21]. The relevant structure is indicated in Fig. 4.

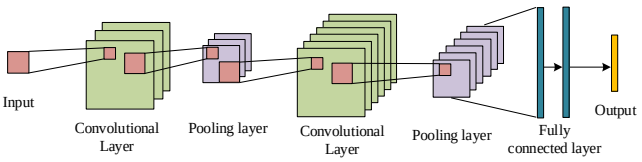

Fig. 4. The structure of convolutional neural networks.

Compared to the RNN-based cybersecurity posture prediction model, CNN-based prediction can process correlated data more efficiently and reduce the iteration time. Combining CNN with GRU can give full play to the

advantages of different models and maximize the model performance and prediction accuracy. Finally, considering the influence of different cybersecurity posture attributes on posture values, the study also introduces an attention mechanism to assign values to different cybersecurity posture attribute features. The bi-directional GRU inputs the results to the attention layer for weighting, and this process is shown in Eq. (9).

$$\begin{cases} u_t = \tanh(W_w P_t + b_w) \\ a_t = soft\max(u_t^T, u_w) \\ v = \sum a_t P_t \end{cases} \tag{9}$$

In Eq. (9), W_w denotes the random generation, P_t denotes the output of the two-way GRU posture prediction model, a_t serves as the importance weight, and v serves as the predicted value of cybersecurity posture after weighted summation. However, the performance is easily influenced by various hyper-parameters, so in order to find the optimal hyper-parameters, this study introduces Particle Swarm Optimization (PSO) for optimizing the hyper-parameters of the bidirectional GRU. PSO algorithm initializes a group of particles by simulating the behavior of an animal searching for food, and then iterates over them. and then iterates over them, which possesses the advantages of fast convergence speed and easy implementation. Assuming that the velocity and position update strategy of particles in D dimensional space is shown in Eq. (10).

$$\begin{cases} v_i(t+1) = wv_i(t) + c_1 rand(Pbest_i - x_i(t)) + c_2 rand(Gbest_i - x_i(t)) \\ x_i(t+1) = x_i(t) + v_i(t+1) \end{cases} \tag{10}$$

In Eq. (10), w denotes the inertia weight, v_i denotes the particle velocity, *rand* denotes the stochastic factor, $Pbest_i$ denotes the optimal value experienced by the i th particle in the past, x_i denotes the current position. And *Gbest* denotes the optimal value experienced by the population, and c_1 and c_2 denote the acceleration factors. Since the acceleration factor of the traditional PSO is fixed, it is impossible to find the optimal distance adjustment position, and in this study, an adaptive strategy is used to adjust the acceleration factor, as shown in Eq. (11).

$$\begin{cases} c_1 = \dfrac{1}{1+\left(\exp-(Pbest_i - x_i(t)\right)} \\ c_2 = \dfrac{1}{1+\left(\exp-(Gbest_i - x_i(t)\right)} \end{cases} \tag{11}$$

The fitness function for all particles is shown in Eq. (12).

$$fit = \left(\frac{1}{P} \sum_{p=1}^{p} \frac{y_t - y_p}{y_p} \right) \tag{12}$$

In Eq. (12), y_t denotes the real label and y_p denotes the prediction result of the model. In addition, further for enhancing the training efficiency of the model and the accuracy of the prediction, the data need to be preprocessed. In this study, one-hot is utilized for processing the discrete time series data and normalizing all the data, and the normalization operation is shown in Eq. (13).

$$x^* = \frac{x - \min(x)}{\max(x) - \min(x)} \tag{13}$$

In Eq. (13), x^* denotes the processed data and x denotes the pending data. In summary, on the basis of the variant of RNN, i.e., GRU prediction model, this study introduces the attention mechanism to assign different cybersecurity posture attributes, and introduces the CNN model for joint prediction. The structure of the finally built cybersecurity posture prediction model is showcased in Fig. 5.

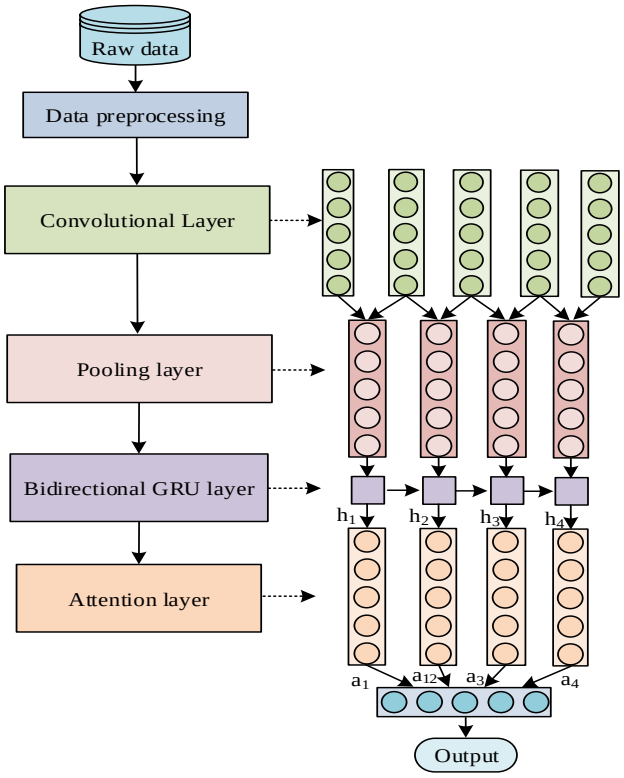

Fig. 5. The structure of network security situation prediction model.

IV. NS Posture Assessment and Prediction Model Effect Analysis

In this study, a cybersecurity posture assessment model on the basis of improved KM and a cybersecurity posture prediction model on the basis of intelligent optimized RNN are constructed, but the effect of their practical application has to be further verified. The study mainly analyzes two aspects, firstly analyzing the effect of the NS posture assessment model, and then verifying the effect of the NS posture prediction model.

A. Effectiveness Analysis of Cybersecurity Posture Assessment Models

Aiming at verifying the effectiveness of the NS assessment model on the basis of improved KM, the TEP dataset is selected for experiments in this study. Faults are introduced at the 161st moment and the operational data of the system in the dataset at two different faults are used as the test set.

Comparison with AE-K means++ algorithm and SAE-K means algorithm is made and the outcomes are showcased in Fig. 6. Fig. 6(a) showcases that all the three algorithms reacted when a fault occurred, but both the AE-K means++ algorithm and the SAE-K means algorithm misjudged the fault before it occurred. Fig. 6(b) demonstrates that all three algorithms responded when a fault occurred, but both the AE-K means++ algorithm and the SAE-K means algorithm misjudged before the 161 moment. In addition, the algorithms in this study have smaller variance and greater stability.

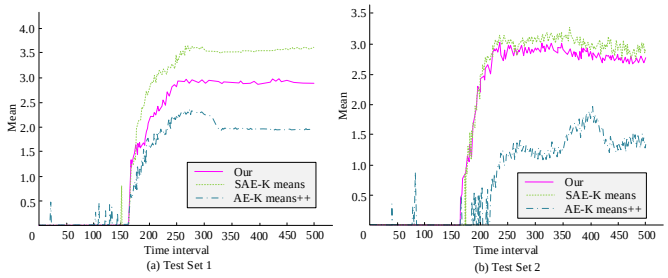

Fig. 6. Test results of three algorithms.

Aiming at verifying the assessment accuracy and efficiency, the posture assessment results are averaged and relative to the accuracy and running time of the traditional KM algorithm, AE-K means++ algorithm and SAE-K means algorithm. The outcomes are showcased in Fig. 7. Fig. 7(a) demonstrates that among the four algorithms, the accuracy of this study's algorithm is the highest at 99.8%, and the KM algorithm has the lowest accuracy at 82.7%. Fig. 7(b) demonstrates that among the four algorithms, the KM algorithm has the shortest running time of 0.176 s, and the present study algorithm has the longest running time of 0.277 s, but it is still within the acceptable range. The outcomes showcase that the NS assessment model on the basis of improved KM possesses a high assessment accuracy.

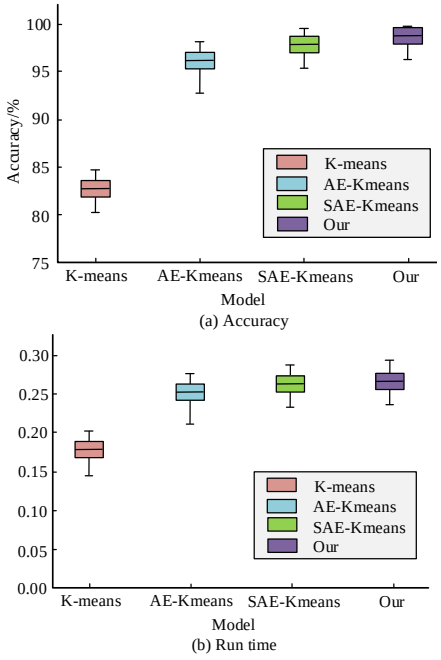

Fig. 7. Comparison of accuracy and runtime of four algorithms.

Aiming at further validating the assessment performance of the improved KM-based cybersecurity assessment model, this study utilizes the UNSW-NB15 dataset for testing and comparing with four posture assessment methods, namely, Random forest (RF), Probabilistic Neural Networks (PNN), Support Vector Machine (SVM), and PNN combined with AE for four posture assessment methods. Fig. 8(a) demonstrates that among the five assessment methods, the model has the highest recall rate of 96.67% and the PNN algorithm has the worst performance of 78.89%. Fig. 8(b) demonstrates among the five evaluation methods, the model of this study has the best performance in terms of F1 metrics with 96.49% and the PNN algorithm has the worst performance with 80.19%. The outcomes showcase that the NS assessment model on the basis of improved KM has better performance in recall and F1 value, and has better performance in NS posture assessment.

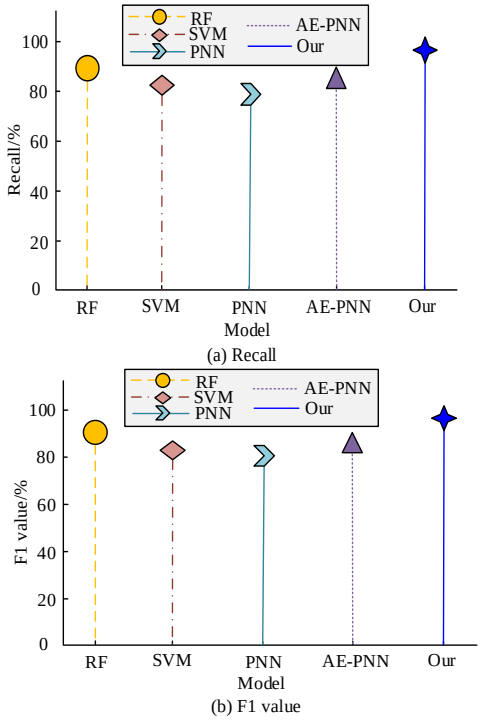

Fig. 8. Comparison of evaluation performance of five situation assessment methods.

B. *Feasibility Analysis of Cybersecurity Posture Prediction Models*

Aiming at validating the performance of the cybersecurity posture prediction model, this study uses the KDDCUP99 dataset as dataset 1 and the CNCERT dataset as dataset 2. The normalized posture sequence values of the two datasets are shown in Fig. 9.

70% of the dataset is taken as the training set, 20% of the dataset is used as the training set and 10% of the dataset is used to verify the accuracy of the model. Mean Absolute Error (MAE), Root Mean Square Error (RMSE) and runtime are used as evaluation metrics, and four situational prediction models, namely CNN, LSTM, GRU and Particle Swarm Optimization - Support Vector Machine (PSO-SVM) are used. Support Vector Machine (PSO-SVM) four posture prediction

models are compared, and the outcomes are showcased in Table I. Table I demonstrates that in the two datasets, this study's model possesses the lowest MAE and RMSE values of 0.18 and 0.30, and a relatively long running time of 703.23 s and 787.46 s, respectively. The outcomes showcase that the proposed situational prediction model possesses a small error and has a good performance of cybersecurity situational prediction.

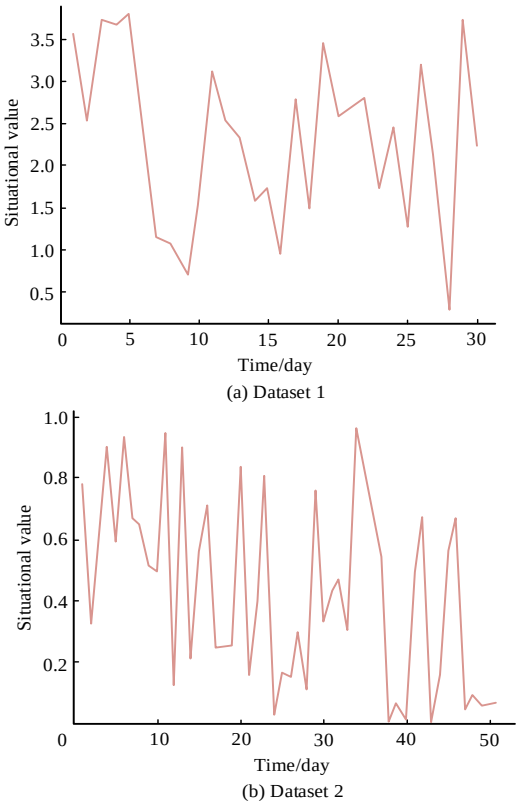

Fig. 9. Situation sequence values of two datasets.

TABLE I. COMPARISON RESULTS OF INDICATORS FOR FOUR SITUATIONAL PREDICTION MODELS

Model	Dataset 1			Dataset 2		
	MAE	RMSE	Time/s	MAE	RMSE	Time/s
CNN	0.27	0.47	404.34	0.22	0.28	516.34
LSTM	0.37	0.59	527.28	0.24	0.37	640.38
GRU	0.37	0.53	443.20	0.23	0.35	570.62
PSO-SVM	0.79	1.23	643.73	0.46	0.76	732.83
Our	0.24	0.30	703.23	0.18	0.31	787.46

The prediction results of the above four models for the posture time series data are showcased in Fig. 10. Fig. 10(a) demonstrates that in dataset 1, the predicted posture values of this study's model are very close to the actual posture values, and the PSO-SVM algorithm has the poorest prediction results, with a large difference from the actual values, as compared to the other three models, which have the highest fit to the actual values. Fig. 10(b) demonstrates that in dataset 2, the posture values of the model of this study are still very close to the actual posture values. The outcomes showcase that the proposed posture prediction model possesses an excellent prediction effect and can significantly improve the traditional CNN model and GRU model, which has certain feasibility and effectiveness.

For further verifying the improvement effect of this study's model compared to the traditional RNN-based model, it was tested in dataset 1 and compared with the traditional GRU and LSTM, and the results are showcased in Fig. 11. Fig. 11 indicates that although all three models are able to predict the SP better, the model of this study is the closest to the actual value, and has a better fit to the actual posture curve, which has a better prediction effect. The outcomes indicate that the proposed NS prediction model on the basis of intelligent optimization RNN has a better prediction effect, and it can improve the traditional RNN-based model with certain superiority.

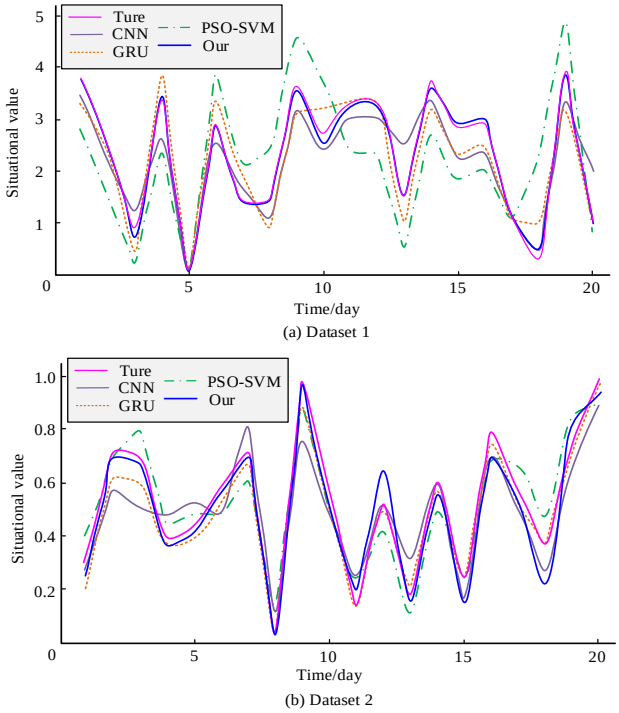

Fig. 10. Comparison of prediction results of four models.

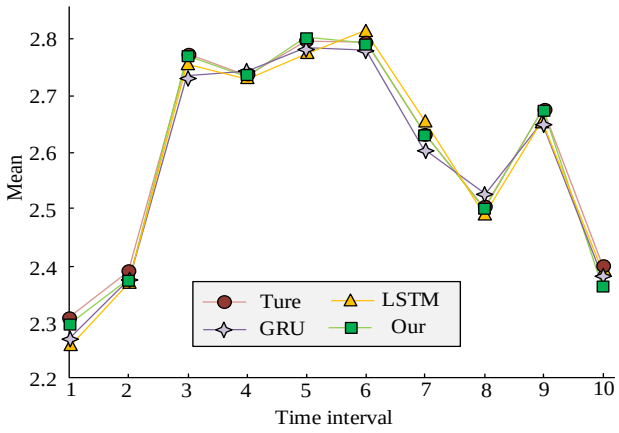

Fig. 11. Security situation prediction curves for three models.

V. Results and Discussion

To verify the performance of the proposed network security situation assessment model based on improved K-means and the network security situation prediction model based on intelligent optimized RNN, the application effects of the two models were analyzed. The analysis of the effectiveness of the network security situation assessment model shows that the proposed network security assessment model can quickly respond to faults and is less prone to misjudgments, with stronger stability. The accuracy of the security assessment model is the highest, at 99.8%, which proves the effectiveness of the proposed K-means algorithm improvement strategy. But the running time of the proposed model is 0.277 seconds, which is greater than the K-means algorithm, AE-K means++algorithm, and SAE-K means algorithm, but it is still within an acceptable range. This is because the improvement strategy for K-means has also increased the complexity of the model to a certain extent. The recall rate of the proposed model is the highest, at 96.67%, and it performs the best in the F1 indicator, at 96.49%, proving the evaluation performance of the network security situation assessment model based on improved K-means.

The feasibility analysis of the network security situation prediction model shows that the MAE and RMSE values of the network security prediction model based on intelligent optimized RNN are the lowest, 0.18 and 0.30 respectively, with small errors and good network security situation prediction performance. The proposed network security prediction model has a relatively long running time of 703.23s and 787.46s, respectively, but it is still within an acceptable range. This is also due to the increased model complexity brought about by the improvement strategy. The network security situation prediction model predicts situation values that are very close to the actual situation values, and has the highest fitting degree compared to the comparison model and the actual values, indicating a good prediction effect. Prove that the proposed model can significantly improve traditional CNN and GRU models, and has certain feasibility and effectiveness. The prediction curve of the proposed model has a high degree of fit with the actual situation curve, and the prediction effect is better than GRU and LSTM, which proves the superiority of the proposed model.

VI. Conclusion

As the evolution and application of Internet technology, it brings convenience to life and also generates certain security risks. Aiming at the assessment and prediction of NS situation, the study builds a NS situation assessment model on the basis of improved KM and a NS situation prediction model on the basis of intelligent optimization RNN. The experimental results verify the network security situation assessment and prediction performance of the proposed model, which is helpful to maintain network security and promote the development and application of the Internet in more fields. However, the proposed NS posture prediction model has increased in time consumption. Therefore, in the future research, deep learning theory and SP prediction should be further combined for enhancing the prediction efficiency to better guarantee the smooth operation of cyberspace.

Acknowledgment

This study is supported by Zhoukou City 2021 Science and Technology Development Plan Project, "Research on Information Dynamic Recommendation System Based on Collaborative Filtering Data Mining Algorithm" (project number: 2021GG02062).

References

[1] A. Talpur and M. Gurusamy, "Machine learning for security in vehicular networks: A comprehensive survey," IEEE Commun Surv Tutorials, vol. 24, no. 1, pp. 346-379, November 2021.

[2] Q. Liu and M. Zeng, "Network security situation detection of internet of things for smart city based on fuzzy neural network," IJRIS, vol. 12, no. 3, pp. 222-227, September 2020.

[3] Z. Chen, "Research on internet security situation awareness prediction technology based on improved RBF neural network algorithm," JCCE, vol. 1, no. 3, pp. 103-108, March 2022.

[4] H. Hu, Y. Liu, C. Chen, H. Zhang, and Y. Liu, "Optimal decision making approach for cyber security defense using evolutionary game," IEEE Trans Netw Serv Manage, vol. 17, no. 3, pp. 1683-1700, May 2020.

[5] L. Tan, K. Yu, F. Ming, X. Cheng, and G. Srivastava, "Secure and resilient artificial intelligence of things: A HoneyNet approach for threat detection and situational awareness," IEEE Consumer Electron Mag, vol. 11, no. 3, pp. 69-78, May 2021.

[6] S. Sengupta, A. Chowdhary, A. Sabur, A. Alshamrani, D. Huang, and S. Kambhampati, "A survey of moving target defenses for network security," IEEE Commun Surv Tutorials, vol. 22, no. 3, pp. 1909-1941, March 2020.

[7] H. Guo, J. Li, J. Liu, N. Tian, and N. Kato, "A Survey on Space-Air-Ground-Sea Integrated Network Security in 6G," IEEE Commun Surv Tutorials, vol. 24, no. 1, pp. 53-87, November 2021.

[8] C. Wheelus and X. Zhu, "IoT network security: Threats, risks, and a data-driven defense framework," IoT, vol. 1, no. 2, pp. 259-285, October 2020.

[9] Jain A K, Sahoo S R, and Kaubiyal J. Online social networks security and privacy: Comprehensive review and analysis. Complex Intell Syst, vol. 7, no. 5, pp. 2157-2177, October 2021.

[10] A. A. Mugha, "Well-architected wireless network security," Journal of Humanities and Applied Science Research, vol. 5, no. 1, pp. 32-42, December 2022.

[11] H. Yang, Z. Zhang, L. Xie, and L. Zhang, "Network security situation assessment with network attack behavior classification," Int J of Intelligent Sys, vol. 37, no. 10, pp. 6909-6927, March 2022.

[12] A. R. Alharbi, M. Hijji, and A. Aljaedi, "Enhancing topic clustering for Arabic security news based on k-means and topic modelling," IET Networks, vol. 10, no. 6, pp. 278-294, March 2021.

[13] J. Zhu, L. Huo, M. D. Ansari, and M. A. Ikbal, "Research on data security detection algorithm in IoT based on K-means," SCPE, vol. 22, no. 2, pp. 149-159, October 2021.

[14] D. Stiawan, M. E. Suryani, S. Susanto, Y. Idris, M. N. Aldalaien, N. Alsharif, and R. Budiarto, "Ping flood attack pattern recognition using a K-means algorithm in an Internet of Things (IoT) network," IEEE Access, vol. 9, pp. 116475-116484, January 2021.

[15] J. Xu, D. Han, K. C. Li, and J. Hai, "A K-means algorithm based on characteristics of density applied to network intrusion detection," Comput Sci Inf Syst, vol. 17, no. 2, pp. 665-687, January 2020.

[16] Y. K. Saheed, M. O. Arowolo, and A. U. Tosho, "An efficient hybridization of K-means and genetic algorithm based on support vector machine for cyber intrusion detection system," International Journal on Electrical Engineering and Informatics, vol. 14, no. 2, pp. 426-442, June 2022.

[17] N. Liao and X. Li, "Traffic anomaly detection model using K-means and active learning method," Int J Fuzzy Syst, vol. 24, no. 5, pp. 2264- 2282, March 2022.

[18] S. Gu, B. Kelly, and D. Xiu, "Autoencoder asset pricing models," J ECONOMETRICS, vol. 222, no. 1, pp. 429-450, May 2021.

[19] K. Zhang, J. Zhang, X. Ma, C. Yao, L. Zhang, Y. Yang, J. Wang, J. Yao, and H. Zhao, "History matching of naturally fractured reservoirs using a deep sparse autoencoder," SPE Journal, vol. 26, no. 04, pp. 1700-1721, August 2021.

[20] Q. Ni, J. C. Ji, and K. Feng, "Data-driven prognostic scheme for bearings based on a novel health indicator and gated recurrent unit network," IEEE T Ind Inform, vol. 19, no. 2, pp. 1301-1311, April 2022.

[21] P. Preethi and H. R. Mamatha, "Region-Based convolutional neural network for segmenting text in epigraphical images," AIA. vol. 1, no. 2, pp. 119-127, September 2023.