ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)
https://doi.org/10.17559/TV-20241009002044
Original scientific paper

Research on Key Technology Algorithms of Communication Network Intrusion Detection and Data Encryption Based on Artificial Intelligence

Wei CAI*, Yingze YE

Abstract: In order to solve the problem of network intrusion detection and data encryption, artificial intelligence is introduced into communication network intrusion detection. Obtain the intrusion data of communication network and analyze the abnormal behavior of communication network: Firstly, the intrusion behavior data is processed based on artificial intelligence algorithm, and the number of network security vulnerabilities and network attacks is screened out. Secondly, an adaptive monitoring method is designed by using reinforcement learning agent to interact with the environment and constantly update the characteristics of the agent. The practical application shows that the method has higher detection stability than the traditional fixed detection method. Finally, on the basis of obtaining the data of communication network nodes by using artificial intelligence technology, the obtained data of communication network nodes is encrypted by using mixed-pool mapping method. The results of design comparison and test show that the proposed artificial intelligence-based network communication data encryption transmission method has higher efficiency, shorter response time and less abnormal node loss, which proves that the proposed method has better encryption transmission performance.

Keywords: artificial intelligence; communication; communication network; communication protocol; data encryption; intrusion detection

1 INTRODUCTION

As an indispensable part of today's social life, the problem of network intrusion security needs to be solved. With the diversified development of network data transmission, network intrusion behavior has also made diversified changes [1]. Under normal circumstances, traditional intrusion detection methods can detect intrusion behaviors in time [2, 3]. However, the detection effect of this method is relatively simple, and the intrusion behavior cannot be detected in real time, which affects the security operation of the network [4]. Based on this, a communication network intrusion detection method is designed to maximize the accuracy of network intrusion detection.

The amount of data to be transmitted in the communication network is increasing [5], and the organization of neighboring structures is becoming more and more demanding. When data transmission is carried out, not only the reliability of data transmission should be considered, but also the efficiency of data transmission should be considered. The response time of adjacent nodes is too long, which is easy to limit the average traffic of one-way data transmission. Related data encryption transmission methods have attracted extensive attention from scholars. Artificial intelligence is a proper term in the field of data information [6], which directly stores the data generated during the operation of the system, and has many advantages such as openness, traceability, maintenance and processing. This data sharing mechanism is a new computer encryption algorithm, which is mainly embodied in distributed information storage. In order to improve the efficiency of data transmission, it is proposed to use wireless communication nodes to build an overall data transmission network. This section describes how to connect some nodes to generate backup data transmission paths based on actual data transmission requirements. In more cases, the planned data transmission path is difficult to play a good transmission effect. On the basis of obtaining node energy characteristics through chaotic parameter modulation and time stamp technology, it is derived from the Bitcoin system, and its essence is a kind of information storage without central identification.

In order to ensure the security and stability of communication network transmission, this paper proposes an artificial intelligence-based communication data encryption transmission method. A hybrid encryption method for network communication data based on improved MD5 (Message-Digest Algorithm 5) algorithm is designed and analyzed. Considering the stability and reliability of the final test results, a specific communication data encryption structure will be constructed under a more rigorous and real environment, combined with the improved MD5 algorithm. At the same time, it is associated with the Internet cloud to form a multimedia computing mechanism, which is more in line with the encryption standards of modern communication data and provides better convenience for data processing. The first chapter is the introduction, the second chapter is related work, and the third chapter is research on communication network intrusion detection algorithm based on artificial intelligence, chapter four is research on encrypted transmission of communication network data, chapter five is simulation verification, and chapter six is conclusion.

2 RELATED WORK

In literature [7], an extreme learning machine based on online serialization is incorporated into the intrusion detection model to reduce the time complexity of the classifier by modifying the bias coefficient. This method uses machine learning methods in the intrusion detection system to improve the classification accuracy and efficiency of the system. However, the combination of accuracy and false positives is not good enough. However, SVM (Support Vector Machine) training is slow [8], and this model is too time-consuming when there is a large amount of data. In literature [9], when faced with a complex network with a large amount of data, model training is limited to manually labeled data, and the detection and recognition rate cannot be guaranteed. Because ELM (Extreme Learning Machine) is a single hidden layer structure, the expression ability is limited, and the feature selection needs to be carried out manually.

In recent years, more and more researchers have applied the increasingly perfect deep confidence network to intrusion detection. Firstly, the nonlinear learning ability of DBN is used to reduce the dimensionality of the original data [10], and then particle swarm optimization is used to optimize the number of nodes in the hidden layer. The experimental results show that this method has good feasibility. The Gauss-Bernoulli constrained Boltzmann machine used for this algorithm uses seven hidden layers [11]. Experiments show that this algorithm can improve the detection rate and false positive rate of the model to a certain extent [12]. However, this algorithm can only be detected in a fixed scene environment, and is not applicable in real-time and changeable scenes, and cannot be used in Marine wireless network scenarios. In literature [13], the data after feature extraction was passed into DNN structure for training, and a good intrusion detection effect was achieved. In addition, using this method for feature extraction can also effectively detect unknown and unforeseeable network attacks. However, the training of both NLP (Natural Language Processing) and DNN (Deep Neural Networks) in this model requires a lot of computational costs, so this model is not suitable for dynamic maritime wireless networks.

Literature [14] proposes an intelligent intrusion detection system that combines statistical analysis and autoencoder. The proposed IDS (Intrusion Detection System) method combines the latest advances in data analysis, statistical techniques, and machine learning theory. In the same year, literature [15] proposed a hybrid deep learning model based on convolutional neural network (CNN) and Weight-dropped Long Short-term Memory network in order to solve the problem of delayed response to intrusion detection in a big data environment.

Reference [16] - To ensure end-to-end encryption, one of the most recommended solutions is to use associative data authentication encryption, but when the number of nodes increases, this scheme requires an adaptive key management center; if the key management center is not specially designed, it will increase the cost in disguise. The MQTT-TTS scalable protocol is proposed to enhance object-to-object security. Its advantage is that it is easy to expand [17, 18], but the data resides in the buffer for a long time, and the accumulation in the buffer will lead to transmission delay, which is relatively low in the overall transmission efficiency of the system. In the future, there will be many Internet of Things communication agents in the cloud, and the centralized way is not easy to expand, and multiple agents are required to achieve distributed deployment, combining algorithms, services and edge computing. It is proposed that the tree-organized agent distribution architecture can be used to improve the protocol [19], which has improved performance in terms of delay and robustness to faults, but it is still necessary to further consider the problems of message flooding and routing complexity. The distributed Qqos aware MQTT middleware [20] is proposed through the edge computing application, and the intermediary plug-in continuously monitors the network QoS and coordinates the MQTT protocol proxy network, thus significantly reducing the end-to-end latency; however, this plug-in can only demonstrate its advantages in the scenario of edge computing. A resource management framework for edge computing system based on MQTT is proposed [21, 22]. The introduction of edge computing is to enhance the scalability, efficiency and privacy of the Internet of Things system, but it affects the overall transmission efficiency of the Internet of Things system and increases the complexity of the authentication connection between the client and proxy server. The management of keys and certificates will also increase the cost [23, 24]. There is a risk of interception in the process of session key negotiation, and there is a threat at the impersonation attack level.

This paper uses the underlying P2P network, and sets each node in the communication network as the component of the wireless network, so that each component becomes the same node in the wireless network, and ensures that each component enjoys the same rights and responsibilities. Learn about other nodes in the wireless network in time and synchronize them. When a new node attempts to join a wireless network, it will make a complete access request to a node in the wireless network, and when the access request appears, the wireless network will transmit the message to the central node of the wireless network [25, 26]. At the same time, when a node attempts to enter the wireless network, during this period of time, all node data related to its work will be transmitted to the monitoring center, and then judged whether the node is missing data, if it is, at this time the node's data is abnormal, and the request for access communication is rejected. The abbreviation is as shown in Tab. 1.

Table 1 Abbreviation

Abbreviation	Full name
MD5	Message-Digest Algorithm 5
SVM	Support Vector Machine
ELM	Extreme Learning Machine
NLP	Natural Language Processing
DNN	Deep Neural Networks
IDS	Intrusion Detection System

3 RESEARCH ON COMMUNICATION NETWORK INTRUSION DETECTION ALGORITHM BASED ON ARTIFICIAL INTELLIGENCE

3.1 Characteristics of Communication Network Intrusion Detection Data are Extracted

The data features are divided within the feasible region, and all data features are fixed point values to ensure the accuracy of data feature extraction.

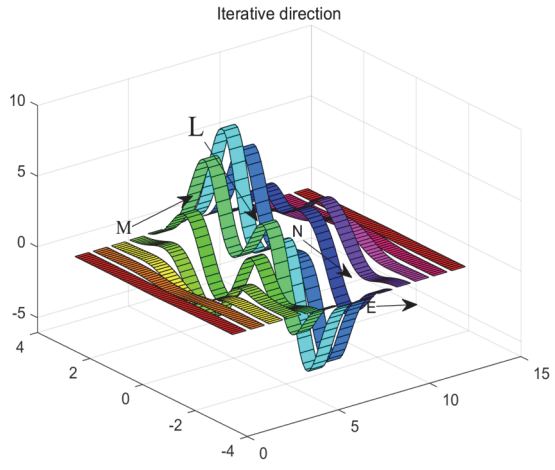

Figure 1 Schematic diagram of gradient descent optimization features

Considering the specific data division mode of communication network intrusion behavior, this paper has few data types and large randomness of data extraction, which makes it impossible to extract the optimal data effectively. Therefore, this paper adopts the method of multiple calculation and iteration to get the best eigenvalue of the communication network intrusion data, as shown in Fig. 1 below.

As shown in Fig. 1, *m*, *l*, and *n* are the local optimal solutions of features, and e is the global optimal solution of features. From the iterative process of M-E, local optimal solutions such as m, l and n at different times are found respectively, and then global optimal solutions are extracted according to the eigenvalues of *a*, *b* and *c*, so as to understand the characteristics of network intrusion behavior at different times.

3.2 Research on Accurate Identification of Artificial Intelligence Communication Network Intrusions for Multi-Class Attacks

With the pursuit of accurate identification of multi-class attacks in ETCN intrusion detection as the core goal, the overall research process is shown in Fig. 2. Firstly, a sample construction method based on spatiotemporal traces is designed to represent spatiotemporal traces contained in ETCN intrusion dataset in the form of spatial samples and time series. Secondly, three space-based learners and time-based learners are designed in CNN to capture the spatial and temporal traces of network attacks. At the same time, a transfer strategy based on transfer learning is designed and applied in a space-based learner to transfer the sample spatial information across data domains. Thirdly, an integrated structure and an integrated algorithm are designed to integrate the learning results of the six base detectors to achieve the final high-precision detection. Finally, the methods in this chapter are fully evaluated and verified through multi-angle experiments.

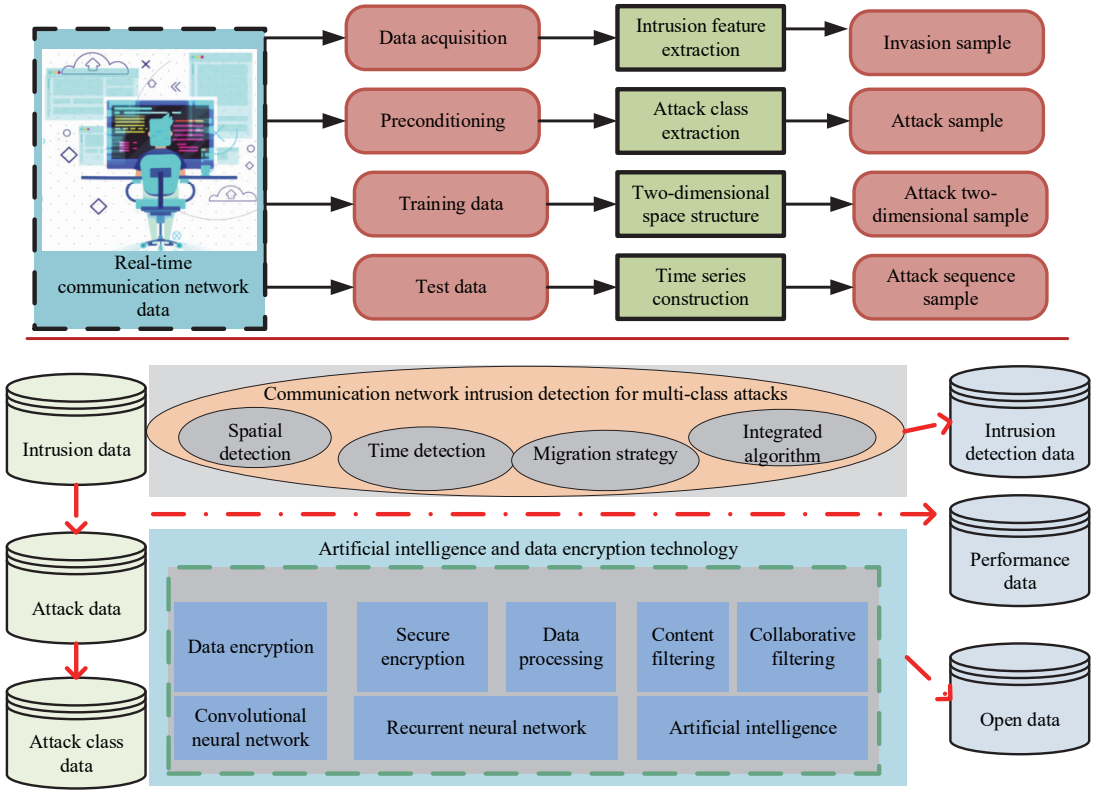

Figure 2 Communication network intrusion detection algorithm framework for multi-class attacks

In the process of data processing, inconsistent data are mainly processed, multiple data are integrated into a data set, data feature extraction and processing are re-performed, and data conflict and redundancy are reduced. The difference of values of numerical variables directly leads to the disadvantage of behavior data being dominated by characteristic data. Therefore, this paper adopts a normalized method to process intrusion behavior data, and the formula is as follows:

$$M' = \frac{M - M_{\max}}{M_{\max} - M_{\min}} \tag{1}$$

M represents the subsequent intrusion behavior; M is the initial eigenvalue; $M_{\min}$ is the minimum transformation result of intrusion behavior. $M_{\max}$ is the maximum transformation result of the intrusion behavior. After the normalization of intrusion behavior data, there is a correlation between different data. In this paper, the normalized data is unified into the same numerical interval to shorten the data processing time. For intrusion detection event, this paper defines it as exception attribute set A. In this paper, the label set of intrusion implicit condition is B, and the interval range of the label set is $O - 1$. Where 0 is the implicit condition of the intrusion event and 1 is the

session that contains the offensive nature of the intrusion event, the intrusion data processing principle is as follows.

$$R = A\frac{C_n}{A_1A_2.....A_m}\frac{D_n}{B_1B_2.....B_m} \tag{2}$$

R is the principle of intrusion data processing; *A* is the set of exception attributes; *C* is the normal feature category; *D* is the abnormal feature category; *B* is the set of intrusion implicit condition tags; *B* is the implied vector of the label set interval at different intrusion times. After processing the hidden vector in the feature vector, network security vulnerability can be analyzed. The formula is as follows:

$$T = R\frac{C_n}{m}\times\frac{D_n}{m} \tag{3}$$

Step 1. Before the calculation, the feature transformation method is used to numeralize and normalize the features of all samples, also, for category labels, map them to decimal values in order, starting from 0.

Step 2. The total number of samples is h and the feature dimension is M_i. Pearson correlation coefficient:

$$p_{MM'} = \frac{\sum_{i=1}^{n}(M_i-\overline{M})(M'_i-\overline{M}')}{\sqrt{\sum_{i=1}^{n}(M_i-\overline{M})^2(M'_i-\overline{M}')^2}} \tag{4}$$

The matrix contains the Pearson correlation coefficient between any two features in the data set (the diagonal of the matrix is the correlation coefficient between a feature and itself, so it is always 1), which can be formalized as follows:

$$R_p = \begin{bmatrix} p_{11}, p_{12}.....p_{1m} \\ p_{21}, p_{22}.....p_{2m} \\ .... \\ p_{m1}, p_{m2}.....p_{mm} \end{bmatrix} \tag{5}$$

Calculate the degree of linear redundancy between *K*-dimensional features and other features:

$$r_p(k) = \lambda * \sum_{i=1}^{m} p_{kl} \tag{6}$$

Step 3. Calculate Pearson correlation coefficient between all features and category labels.

Step 4. For the nonlinear correlation part, the distance correlation coefficient between features is computed through traversal. Distance covariance:

$$d_{Cov(M,M')} = \frac{1}{m^2\sum_{i,j=1}^{n}A_{ij}B_{ij}} \tag{7}$$

Step 5. Calculate the distance correlation coefficient between all features and category labels.

Step 6. In accordance with the principle of "maximum correlation minimum redundancy", that is, to make the correlation between the features of ETON intrusion data set and the category labels as large as possible, and to make the redundancy between the features as small as possible, a comprehensive formula is designed to weigh the results of the linear part and the non-linear part. The formula is as follows:

$$v(k) = \lambda * (d_{Cov(M,M')} - r_p(k)) * (1-\lambda)(R_p - r_p(k)) \tag{8}$$

Step 7. Rank the comprehensive measurement coefficients of all features of ETCN network data from large to small. The larger the value of *v*, the more important the *K*-dimension features are.

3.3 Research on Accurate Identification Method of Communication Network Intrusion by Adding Adaptive Module to the Model

In order to enable the model to monitor intrusion behavior in dynamic environment, an adaptive module is added to the module. 20% of the real-time communication data collected in the information storage module will be passed into the adaptive update module, which will process this part of the data as label data and use to dynamically train the DBN network. The model of the adaptive module is shown in Fig. 3.

The principle of sparse coding is to decompose the input sample set to obtain a linear combination of multiple primions. The features of the input sample are represented by the coefficient of the basis. The specific decomposition formula is shown as follows:

$$M = \sum_{i=1}^{m}\lambda_i m_i \tag{9}$$

As shown in Fig. 3, the main points of the improved model can be summarized as follows: Based on the negative gradient and the previous term distribution algorithm, the parameters and weights of the basic decision tree are iteratively fitted in order. With the progress of the fitting process, the discriminant ability of the model is gradually improved, and the iteration is completed when the number of iterations reaches the preset upper limit *M*. The final improved model is obtained by combining all the basic decision trees together in a weighted linear manner. In this process, the model establishes the boundary of normal and aggressive decision behavior in the decision tree by means of binary splitting. Theoretically, a more accurate boundary of decision behavior can be built with each new decision tree established. When the model is faced with the tested sample after training, it can determine its positive and negative attributes through the boundary of decision behavior. Even in the face of unknown attacks that are not involved in training, the model can determine whether a sample is normal or an attack by determining which side of the decision behavior boundary the mapping position of the sample is in the feature space.

Step 1. First, randomly shuffle all samples (to avoid subsequent calculations falling into local space);

Step 2. For the *I*-type feature of the *K* th sample, calculate the average value of the sample label of the first *k* samples as the statistical value $x_{k,i}$ of the target variable of the feature. At the same time, add prior knowledge in the calculation to smooth it to avoid overfitting.

$$m_{k,i} = \frac{\sum_{j=1}^{k} y_j + \lambda p}{\sum_{j=1}^{k} m_j + \lambda} \tag{10}$$

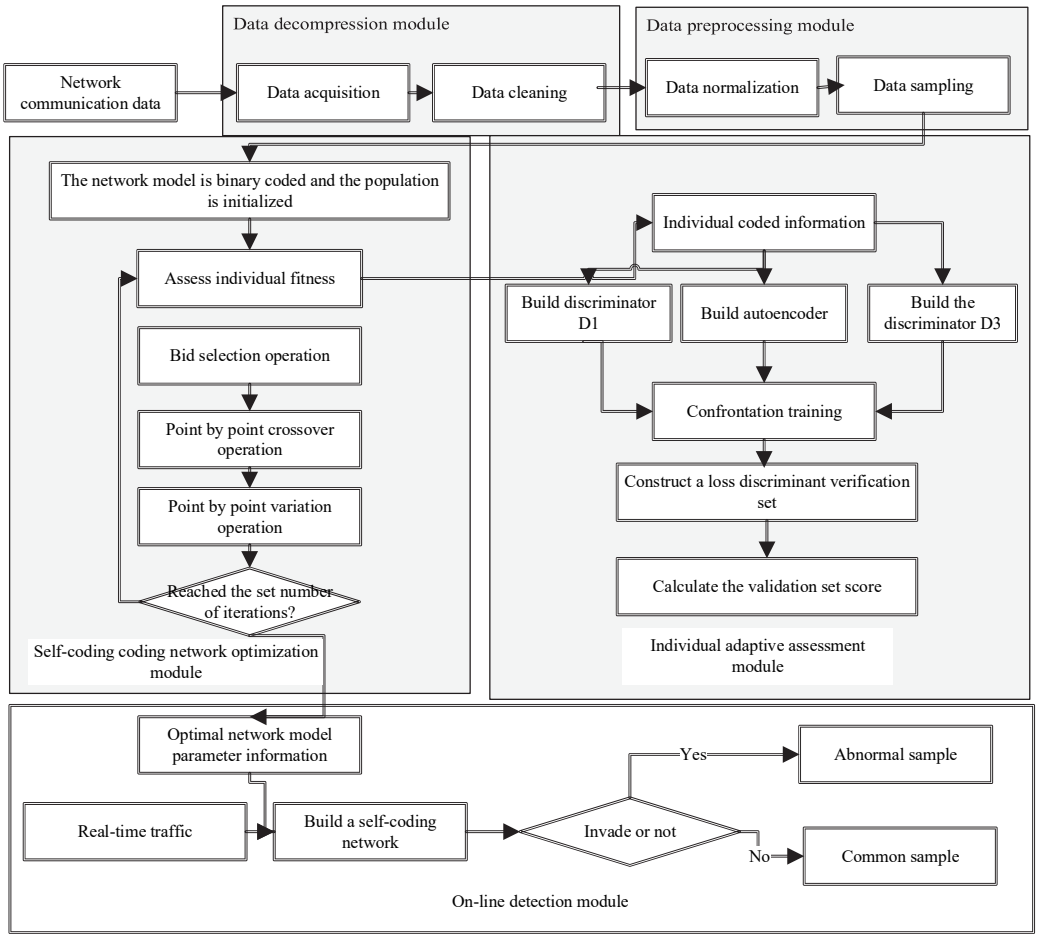

Figure 3 Adaptive artificial intelligence communication network intrusion algorithm diagram

3.4 Research on Adaptive Communication Network Intrusion Methods Based on Reinforcement Learning

The implementation framework of the proposed communication network intrusion adaptive online monitoring method is shown in Fig. 4. The data in the sample database is updated according to the latest communication network transmission data, and reinforcement learning agents are trained to maintain the adaptability of the intelligence to the communication network transmission changes.

(1) According to the actual intrusion detection, the environment state and return function are determined.

(2) The dynamic sample database is first composed of historical data samples transmitted by the communication network. After the actual test, part of the actual test data is randomly selected to be added to the sample database, and an equal amount of historical data is removed to realize the dynamic update and adjustment of the sample database.

(3) The trained mature agent is continuously used for intrusion detection of data transmitted by the latest communication network.

The training agent stage refers to the training of the agent using the historical data of the problem to be solved. The essence of training is to optimize and improve the agent's action strategy, mainly by updating the action state function, which can be expressed as:

$$R(m,m',a) = \lambda \sum_{m'} p(m') \max R(m',a) \tag{11}$$

In the action decision process, in order to avoid the tendency of the agent to "only use", the agent strategy based on the two-one greedy strategy is constructed to transform the agent strategy. The action strategy implemented after the transformation can be expressed as:

$$\omega(m) = \begin{cases} w(m') \\ A \end{cases} \tag{12}$$

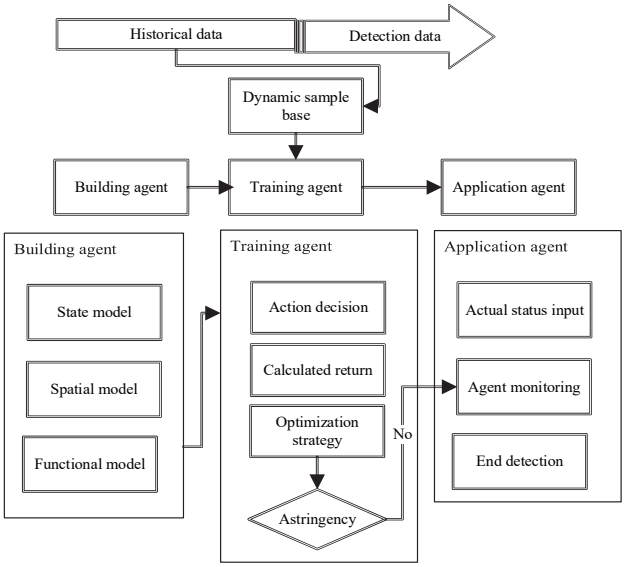

Figure 4 Adaptive intrusion detection implementation framework

In the return calculation step, the agent will calculate the return value according to the preset return Eq. (4) according to the change of the environment state, and update the action state function value, such as Number of implicit elements, Number of elements, Learning rate, Attenuation factor, Sparse punishment and Maximum iterations. The model parameters are shown in Tab. 2.

Table 2 Parameter table of Adaptive communication network intrusion detection model

Parameter	Value
Number of implicit elements	60
Number of elements	51
Learning rate	0.0001
Attenuation factor	0.001
Sparse punishment	6
Maximum iterations	600

4 RESEARCH ON ENCRYPTED TRANSMISSION OF COMMUNICATION NETWORK DATA

4.1 Data Encryption for Communication Network Security Protection Based on Machine Learning

With a complete communication network security protection process data encryption structure can be a more complete grasp of the real-time status of encrypted information. It mainly applies security protection means in the data cloud, and lacks the initiative of data encryption. In this paper, the whole data encryption process structure is established, in which the communication network security protection process is divided into two parts: secret key management and anomaly detection. The encryption structure is shown in Fig. 5.

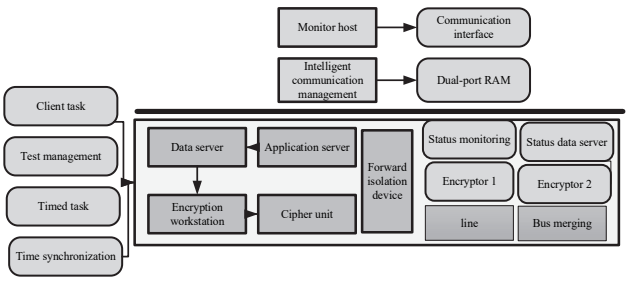

Figure 5 Encryption structure

In this paper, a key with a length of 80 bits is applied for encryption. When the starting value of the round key of the machine learning algorithm is 80 bits, each iteration calculation can be described by cat mapping. Assuming that the initial round key string of 90 blt is $m - m_1m_2$. m_{80}, after the first iteration of the key, two key sequences can be obtained as:

$$\begin{cases} l_1 = m_1 m_2 ... m_{40} \\ l_2 = m_{41} m_{42} ... m_{80} \end{cases} \tag{13}$$

After the generation, it can be extended to a set key length of 160 bit on the basis of meeting the security requirements of the communication network autonomous defense data encryption method.

The autonomous defense against sensitive data of the communication network encrypted by machine learning algorithm is mainly divided into three parts: First, the XOR operation of the round key is performed on the plain text information of the sensitive data. The expression is as follows:

$$\omega_\lambda = \omega_\lambda + m_\lambda^j \tag{14}$$

In the formula, w is the intermediate change state in the process of autonomous defense of sensitive data encryption by the communication network, and the state remains 64 bit, then the wheel key used is m. Then, the intermediate state of sensitive data encryption after a round of key XOR operation is divided into 16 states, each state is 4 . The 80 bit round key only needs 16 nonlinear S-boxes for substitution operations, and each S-box has the same 4 bit input and output. The above 16 communication network autonomous defense sensitive data encryption intermediate state w_{16}. After the S-box substitution operation of w_1, S_{16} can be obtained, and the operation results can be obtained according to Tab. 3.

Table 3 S-box substitution operation table in machine learning algorithm

Input	Output
1	D
2	6
3	C
4	7
5	E

After nonlinear S-box replacement, the communication network autonomous defense sensitive data encryption intermediate state:

$$\begin{cases} \omega_r = \omega_{4*r} \\ \omega_{r+16} = \omega_{4*r+1} \\ \omega_{r+32} = \omega_{4*r+2} \end{cases} \tag{15}$$

When using machine learning algorithm to encrypt communication network autonomous defense sensitive data, after 28 rounds of replacement, it is also necessary to carry out 32 rounds of key XOR operation to get the final communication network autonomous defense sensitive data ciphertext information. In order to ensure the balance between the encryption effect and the encryption efficiency

of this method, the update of the round key is realized through the synchronous application of the round key generation module and nonlinear S-box. In summary, the key components are the data to be encrypted, the round key and the number of encryption iterations when using machine learning algorithms to encrypt communication networks to defend sensitive data independently. Therefore, the decrypted plaintext information can be obtained by reversing the encryption process of the sensitive data of the communication network autonomous defense.

4.2 Mixed Encryption Model of MD5 Network Communication Data Based on Machine Learning Algorithm

According to the transmission path and coverage area of network communication data, basic encryption nodes can be set first. Such nodes are basic core nodes, which have strong master control and are the core of the encryption level. The refined MD5 algorithm is used to calculate the fine granularity of the encryption core node.

At this time, the fine-grained nodes arranged before are formed into the encryption correlation degree, and the sliding window is segmented by the improved MD5 algorithm to realize multi-directional encryption and form a more powerful sliding homomorphic hybrid encryption model to enhance the corresponding encryption effect. The default unit of the derived encryption instruction needs to be prepared first, as shown in Tab. 4.

Table 4 Derived encryption instruction default unit table

Derived unit	Primary encryption	Advanced encryption
Data coverage ratio	1.45	1.64
Communication key distance	1.24	15.7
Mixed correlation coefficient	2.78	1.87

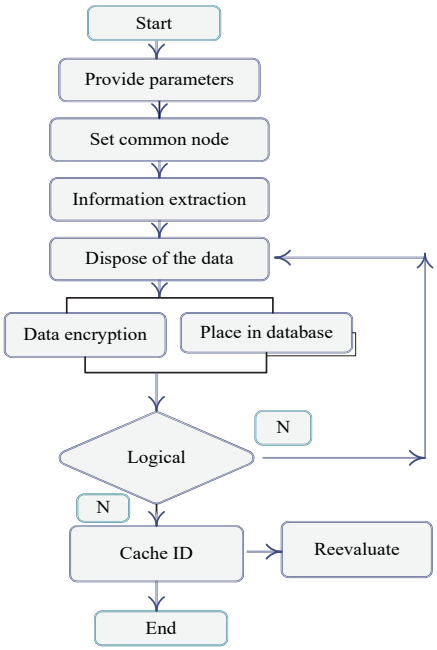

Figure 6 Machine learning MD5 data cache encryption process

The cached data in the process of communication network security protection is the final embodiment in the Internet server terminal, and the final information encryption and transmission will be realized in the storage process. The data cache encryption process of MD5 communication network security protection based on machine learning is shown in Fig. 6.

The whole machine learning MD5 mobile communication network data exchange privacy steganographic encryption algorithm mainly consists of four steps.

1) Initialization phase.

Through the key formation algorithm in the relevant prior knowledge, a key pair needs to be formed for each node L, that is:

$$pk_i = v_i, sk_i = m_i \tag{16}$$

2) Coding and signing.

After the terminal awareness node collects the big data mobile communication network, it simplifies the operation process.

3) Data fusion.

Different processing methods are used to process and analyze each part of the data packet, and addition operation is used for the data part, that is:

$$\lambda_{avg} = \sum_i m_i \tag{17}$$

4) Data encryption:

Combine them, get a new piece of data, and send it to the network base station.

$$m_i^{'} = index(m_i) \bmod 2^k \tag{18}$$

5 SIMULATION VERIFICATION

The training data in this paper are a mixture of the UNSW-NB15 dataset and the CSE-CIC-IDS2017 dataset. In addition, in order to better fit the communication environment of the actual maritime wireless network, the communication data of part of the VDES system is collected and combined with other data sets. Due to the large overall data set, this paper randomly selected part of the data as training samples, as shown in Tab. 5.

Table 5 Distribution of UNSW-NB 15 intrusion detection data types

Attack type	No.	Percent
Normal	1,58,567	87.94%
Exploits	38,322	1.50%
DoS	13,818	0.43%
Backdoor	1,569	0.19%
Analysis	2,139	0.19%
Fuzzers	19,568	0.78%
Generic	177,398	7.42%
Reconnaissance	13,571	1.49%
Shellcode	10,451	0.04%
Worms	128	0.02%
Total	2,116,001	100 %

Tab. 6 shows the attack types and data distribution contained in the CSE-CIC-IDS2017 dataset.

Comparing the accuracy of the model proposed in this paper with the SA-AE algorithm and the CNN-WDLSTM algorithm in the environment of small sample training data, the results obtained are shown in Fig. 7.

Table 6 CSE-CIC-IDS2017 Intrusion detection training and test data distribution

Attack type	Number of training sets	Number of test sets
Benign	1,378,596	967,538
DDoS	76,764	51,639
Port Scan	94,234	53,475
Bof	11,549	587
Infilteration	10,458	16
Web Attack	1,794	794
FTP-Pataor	4,684	3,263
SSH-Pataor	3,479	2,467
DoS Goldeneye	6,064	4,342
DoS Hulk	139,769	92,673
DoS Slowhttptest	2,047	2,749

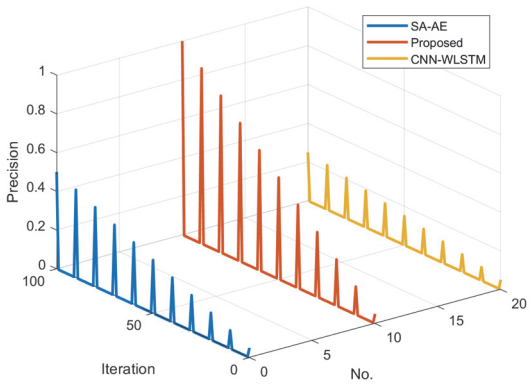

Figure 7 Comparison of model accuracy

Fig. 7 shows how the accuracy of the model changes as the number of iterations increases. Due to the combination of statistical technology and self-coding technology, SA-AE algorithm can achieve a certain accuracy in the early stage of iteration. However, due to the use of small samples in training, SA-AE algorithm falls into local optimization and quickly converges to a low accuracy, indicating that the algorithm is not suitable for the scene of small sample training data. The design of CNN-WDLSTM algorithm obviously only considers the situation in the background of big data. Although it can gradually improve the accuracy after several iterations, the final accuracy is still low and cannot meet well the requirements in the scenario of small sample training data. The algorithm proposed in this chapter can obtain a stable accuracy in the first 20 to 30 iterations, and the accuracy of the model is above 95%, which is well adapted to the environment of small sample data.

In addition, the network IP address is scanned, the normal access TCP port is identified, and the network access protocol is initially analyzed. In the process of SYN scanning in the mall, it is found that the C port in the server is open, and a confirmation command is sent to the server, and it is obtained that the C port is open normally and there is no abnormal data. After TCP detection, fraudulent data is found, and TCP is used to flag the vulnerability of the flag area. After scanning, it is found that there are many open proxy servers in the TCP tag, which are carrying out real-time attacks on the network. At this time, the network intrusion detection situation is shown in Fig. 8.

As shown in Fig. 8, before 25 min, the LOF value is still in the normal range, and after 30 min, the LOF value begins to rise rapidly. It can be seen that 0 min - 30 min is the normal behavior of the network. After 35 minutes, the network becomes abnormal. According to the real-time environment of the network, this paper determines that the abnormal behavior of the network is that the online data of the shopping mall users has been invaded. The data distribution after encryption is shown in Fig. 9, Fig. 10 and Fig. 11.

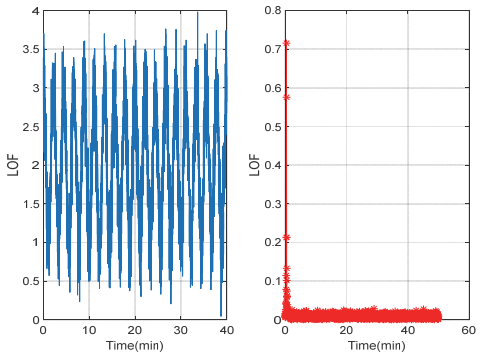

Figure 8 Abnormal network behavior detection

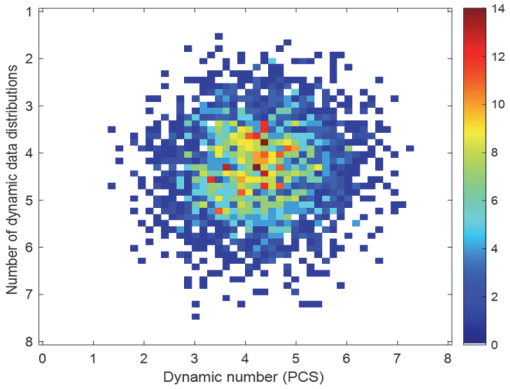

Figure 9 Encryption distribution of machine learning MD5 communication data 1

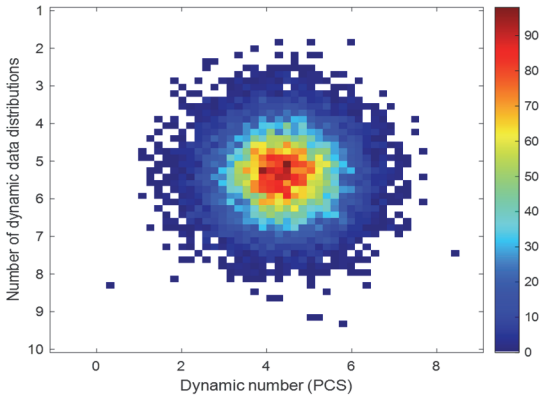

Figure 10 Encryption distribution of machine learning MD5 communication data 2

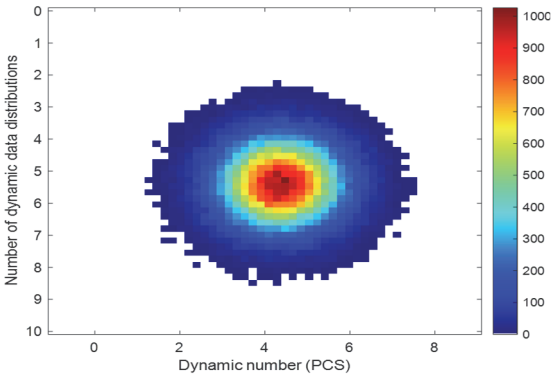

Figure 11 Encryption distribution of machine learning MD5 communication data 3

The data encryption method of communication network security protection based on machine learning has the best encryption effect. As shown in Fig. 9, Fig. 10 and Fig. 11, it can be seen that the encryption method proposed in this paper gradually has a strong information coverage ability after different training, and the data covered is relatively dense, and the communication data has a good hiding ability after introducing the encryption method proposed in this paper.

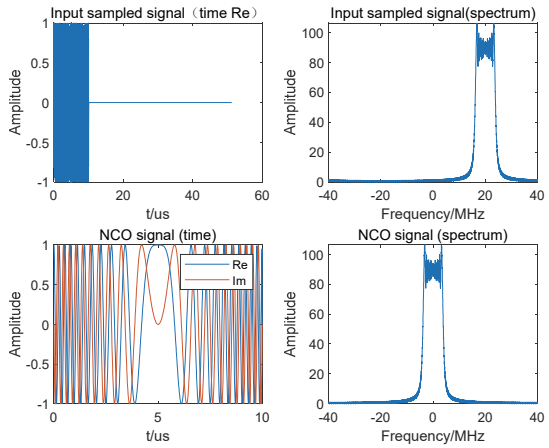

Figure 12 Data encryption output

The analysis of Fig. 12 shows that with the increase of sampling frequency, the amplitude of time-domain waveform of communication network data fluctuates between 1 kB/s and −1 kB/s, and the peak value fluctuates between 0 and 100. It can be seen that the steganographic ability of the proposed method for data encryption in communication networks is good, and the amplitude can be maintained relatively stable under the multi-channel transmission of communication network data.

Table 7 Encryption performance comparison

Method	Leak probability	Deciphering bit length	Recognition / %	Time overhead /s
Proposed method	0.026	1.56	97.44	0.44
SA-AE method	0.058	9.75	86.48	0.97
CNN-WDLSTM method	0.086	12.65	91.25	1.53

The analysis of Tab. 7 shows that the leakage probability of the proposed method is 0.026, the decoding bit length is 1.56 kbit, the recognition degree is 97.44%, and the time cost is 0.44s. Compared with other methods, the proposed method takes less time and has less probability of leakage and higher recognition when decoding bits with short length.

6 CONCLUSION

This paper studies the design of communication network intrusion detection method based on artificial intelligence algorithm. Based on the acquisition and processing of abnormal behavior data, a detection model is constructed to detect network intrusion accurately, and an adaptive detection method for communication network intrusion is proposed. This method can dynamically adjust the sample base, constantly train the detection agent, make it keep adaptability to the communication network intrusion detection, and effectively support the current communication. The next step will be the encryption transmission method of wireless network communication data based on blockchain technology, encrypt the communication data obtained by using blockchain technology, and realize the encryption transmission of wireless network communication data by unifying the communication data transmission format and designing the communication architecture.

7 REFERENCES

[1] Yang, C. Y., Ling, Y., & Li, X. (2021). Research on Information Encryption Algorithm under the Power Network Communication Security Model. *Journal of Physics: Conference Series, 1852*(3), 32007-32014. https://doi.org/10.1088/1742-6596/1852/3/032007

[2] Yao, J. & Liu, J. (2021). Research on Computer Network Technology System Based on Artificial Intelligence Technology. *Journal of Physics: Conference Series, 1802*(4), 42028-42034. https://doi.org/10.1088/1742-6596/1802/4/042028.

[3] Sun, Q. (2021). Key Research on Recommendation Algorithms Based on Spatio-temporal Relationships in Location Social Networks. *International Conference on Artificial Intelligence, Big Data and Algorithms (CAIBDA),* 2021, 133-136. https://doi.org/10.1109/CAIBDA53561.2021.00035

[4] Wang, Q. & Lu, P. (2019). Research on Application of Artificial Intelligence in Computer Network Technology. *International Journal of Pattern Recognition and Artificial Intelligence, 33*(5), 1959015.1-1959015.12. https://doi.org/10.1142/S0218001419590158

[5] Liu, Q. & Ma, X. (2021). Security Model and Design of Network Communication System Based on Data Encryption Algorithm. *International Journal of Autonomous and Adaptive Communications Systems, 14*(1/2), 159-173. https://doi.org/10.1504/IJAACS.2021.10033793

[6] Zhang, Z., Cao, Y., & Cui, Z. (2021). A Many-Objective Optimization Based Intelligent Intrusion Detection Algorithm for Enhancing Security of Vehicular Networks in 6G. *IEEE Transactions on Vehicular Technology, 3*(9), 87-96. https://doi.org/10.1109/TVT.2021.3057074

[7] Subramani, S. & Selvi, M. (2023). Multi-objective PSO based feature selection for intrusion detection in IoT based wireless sensor networks. *Optik, 273*, 170419-170428. https://doi.org/10.1016/j.ijleo.2022.170419

[8] Yuan, Y., Xu, H., & Wang, B. (2023). A New Dominance Relation-Based Evolutionary Algorithm for Many-Objective Optimization. *IEEE Transactions on Evolutionary Computation, 20*(1), 16-37. https://doi.org/10.1109/TEVC.2015.2420112

[9] Ramakrishnan, M., Dhas, C. S. G., & Sikamani, K. T. (2021). A Novel Multi Optimization Based Genetic Algorithm for Network Security. *Journal of computational and theoretical nanoscience, 2021*(3), 18-32.

[10] Mansour, R. F. (2023). Artificial intelligence based optimization with deep learning model for blockchain enabled intrusion detection in CPS environment. *Scientific Reports., 11*(3), 59-76.

[11] Shitharth, S. & Prince, W. D. (2021). An enhanced optimization based algorithm for intrusion detection in SCADA network. *Computers & Security, 70*(sep.), 16-26. https://doi.org/10.1016/j.cose.2017.04.012

[12] Zhou, X., Li, B., & Qi, Y. (2020). Mimic Encryption Box for Network Multimedia Data Security. *Security and Communication Networks, 2020*(2), 1-24.

https://doi.org/10.1155/2020/8868672
[13] Kohout, J., Komarek, T., & Cchc, P. (2020). Learning communication patterns for malware discovery in HTTPs data. *Expert Systems with Applications, 101*(JUL.), 129-142. https://doi.org/10.1016/j.eswa.2018.02.010
[14] Pan, Q. & Zhang, H. (2019). Key Algorithms of Video Target Detection and Recognition in Intelligent Transportation Systems. *International Journal of Pattern Recognition and Artificial Intelligence, 2019*(4), 1653-1668.
[15] Alimi, O. A., Ouahada, K., & Abu-Mahfouz, A. M. (2021). A Review of Research Works on Supervised Learning Algorithms for SCADA Intrusion Detection and Classification. *Sustainability, 2021*(17), 173-189. https://doi.org/10.3390/SU13179597
[16] Meng, Q., Zhang, Y., & Wu, F. (2020). Network Intrusion Detection Model Based on Artificial Intelligence. *Journal of Physics Conference Series, 1617*, 12082-12098. https://doi.org/10.1088/1742-6596/1617/1/012082
[17] Li, Y., Liu, R., & Liu, X. (2021). Research on Information Security Risk Analysis and Prevention Technology of Network Communication Based on Cloud Computing Algorithm. *Journal of Physics: Conference Series, 1982*(1), 12129-12138. https://doi.org/10.1088/1742-6596/1982/1/012129
[18] Li, J., Wang, R., & Wang, J. (2020). Analysis and forecasting of the oil consumption in China based on combination models optimized by artificial intelligence algorithms. *Energy, 144*, 243-264. https://doi.org/10.1016/j.energy.2017.12.042
[19] Liao, X. & Xie, J. (2021). Research on Network Intrusion Detection Method Based on Deep Learning Algorithm. *Journal of Physics: Conference Series, 1982*(1), 12121-12136. https://doi.org/10.1088/1742-6596/1982/1/012121
[20] Fu, N. & Zhang, D. (2021). Research on Application Technology of Computer Communication and Network Development Based on Data Mining Technology. *Journal of Physics: Conference Series, 1982*(1), 12132-12143. https://doi.org/10.1088/1742-6596/1982/1/012132
[21] Xu, H., Chen, X., & Zhou, J. (2021). Research on Basic Problems of Cognitive Network Intrusion Prevention. *Lecture Notes in Electrical Engineering, 2013*, 514-517. https://doi.org/10.1007/978-3-642-40618-8_86
[22] Huang, C. (2021). Forest management and resource monitoring based on AMI intrusion detection algorithm and artificial intelligence. *Journal of Ambient Intelligence and Humanized Computing, 2021*(4), 3211-3224. https://doi.org/10.1007/s12652-021-03211-y
[23] Choudhary, D. & Pahuja, R. (2022). Deep Learning Approach for Encryption Techniques in Vehicular Networks. *Wireless Personal Communications, 125*(1), 1-27. https://doi.org/10.1007/s11277-022-09538-9
[24] Yuanzhe, L., Chaowei, W., & Yue, Z. (2020). Research on an improved approach for network security detection based on data mining and prefixspan algorithm simulation experiment. *International Journal for Engineering Modelling, 31*(1), 184-193.
[25] Daming, L. Z. (2020). Information security model of block chain based on intrusion sensing in the IoT environment. *Cluster Computing, 22*(1), 451-468. https://doi.org/10.1007/s10586-018-2516-1
[26] Zou, S., Zhong, F., & Han, B. (2021). Network intrusion detection method based on deep learning. *Journal of Physics: Conference Series, 1966*(1), 12051-12056. https://doi.org/10.1088/1742-6596/1966/1/012051

Contact information:

Wei CAI
(Corresponding author)
School of Intelligent Manufacturing,
Jianghan University,
Wuhan, 430056, China
E-mail: a471520511@163.com

Yingze YE
Information Technology Center,
Huazhong Agricultural University,
Wuhan, 430070, China