Adaptive Incremental Modeling Combined with Hidden Markov Modeling in Cyber Security

Liwen Xu

Business School, Jiangsu Open University, Nanjing, 210000, China
E-mail: liwenxulw@tom.com

Received 25 March 2024; Accepted 19 June 2024

Abstract

This study examines the limitations of traditional CS technology, which relies heavily on labeled data and is unable to detect new types of attacks in real time. It proposes an optimization and improvement of CS technology through the use of hidden Markov models and adaptive incremental models. The research is conducted from three perspectives: the actual collection of security information, the extraction of unknown protocol features, and the development of detection models. Firstly, a unified method of collecting safety information is established, and a safety information database is obtained by combining information filtering, integration, and association analysis. Secondly, the modified hidden Markov model is used to parse the unknown protocol messages and extract the appropriate features. Finally, the extracted information features are applied to the adaptive incremental model for intrusion detection. The experimental results indicated that the average time cost of the data processing method is 25.841 ms, and the identification accuracy of the intrusion detection model for new attack types reaches

Journal of Cyber Security and Mobility, Vol. 13_5, 1149–1172.
doi: 10.13052/jcsm2245-1439.13515

91.15%. The model designed by the research can adapt to the complex and changeable network environment and accurately detect network intrusion while ensuring operational efficiency, which provides a new research direction for the field of CS.

Keywords: Cyber security, hidden Markov models, adaptive, incremental learning, association analysis.

1 Introduction

The exponential growth of information technology can be attributed to the ongoing advancements in big data, cloud computing, and communication technologies, which have led to an increasing number of network devices [1]. The proliferation of network devices and applications, along with the resulting surge in inflated network data, has led to a growing severity of the cyber security (CS) problem [2]. The Internet exposes a tremendous deal of hidden risks, and a cyber-attack might seriously harm the interests of businesses, nations, and people alike [3]. However, existing work mainly relies on empirical knowledge as well as publicly labeled datasets, which does not achieve better network attack detection (NAD) results when facing massive, service-diverse, and rapidly evolving real networks [4, 5]. For this reason, the research utilizes adaptive theory as well as incremental learning (IL) method and hidden Markov model (HMM) to construct a new NAD approach to achieve a more adaptive network intrusion detection (ID) that is more in line with the real network environment. The innovation of the research is to construct an unknown protocol message model based on an improved HMM to parse the protocol and extract more useful information. In the meantime, adaptive theory and the IL solutions are used with ID to enhance the model's capacity for generalization. Conventional cyber secruity detection methods typically employ static data for training, which is challenging to adapt to the dynamic nature of the network environment. Furthermore, during the training process, the detection model relies excessively on manually labeled data, which frequently fails to encompass all potential attack patterns and variants. The research design method employs the adaptive IL method to facilitate the automatic update and enhancement in the evolving environment, thereby enabling the identification of novel attack modes. Furthermore, correlation analysis technology is employed to integrate and correlate diverse safety information, thereby enhancing the precision of detection.

The remainder of this study is structured as follows. The first section is the literature review, which provides an overview of the state of both local and foreign research at the moment. The second part is the method elaboration part, which introduces the research method and design process. The third part contains the description of the experimental analysis part, which investigates the performance of the model of the study design Model through a series of experiments. The fourth part is the conclusion part, which discusses and puts forward the future outlook based on the experimental results.

2 Related Work

The academic community has placed a great deal of emphasis on and a lot of work has been done on machine learning-based computer science research in the past few years. To lower the false alarm rate and raise the real alarm rate in the ID system, Azizan et al. [6] suggested a machine learning-based model for the network ID system. The model analyzed vast amounts of data and identified anomalous traffic using the support vector machine (SVM) technique. According to the findings, the method's average accuracy was 98.74%. A multi-intelligence-based NAD technique was presented by Roy et al. [7] to defend high voltage DC systems' power modulation controller and automatic generation control loop against cyber-attacks. The method employed a single class classifier for wide-area signals and used a support vector regression model to detect and identify attacks based on local information. The results indicated that the research design method performs well during the attack. Li et al. [8] provided technical support for CS strategies for active distribution systems and proposed an adaptive hierarchical NAD and localization method based on waveform analysis for distributed active distribution systems. The method was based on a deep learning model for detecting cyber-attacks and used an improved spectral clustering method for the initial localization of cyber-attacks. Attack detection was difficult because spread launch denial of service attacks and attack techniques are dynamic, as discovered by Nuiaa et al. [9]. They suggested a novel paradigm for attack detection. The model's objective was to choose features using a feature selection model; the features that were chosen were then classified using the K closest neighbor, random forest, and SVM algorithms. The method's accuracy in identifying attacks was 89.59%. AlShahrani [10] identified that cyber attack techniques have been improving in recent years and the methods for defending against the attacks need to be further optimized. In light of these considerations, a deep learning-based NAD classification technique was proposed. The technique employed the AdaBoost regression classifier for attack detection. The results of the performance investigation indicated that, in comparison to current deep learning algorithms, the suggested method demonstrated significantly enhanced performance in terms of NAD.

Learning from new data without forgetting prior knowledge is known as IL which is a crucial problem in machine learning and artificial intelligence research. According to Peng et al. [11] the existing inference techniques for network structures are computationally intensive and too imprecise to represent the variability of network structures. For this reason, they proposed a new network representation method. The method used recursive neural networks as well as an optimization strategy to explore the semantics of nodes in the new rectangular space, and then optimized the framework using the IL method. According to experiments, when the network learns the representation, the technique reduced processing time by more than 200% and the memory footprint by more than 80%. Wu et al. [12] proposed a nonparametric a priori induced hybrid model of depth and log polynomials to detect the cognitive state of pilots by means of a developed brain power map. For every neuron in the network's initial layer, the model inferred latent variables using multi-normal distributions. By extracting additional probability distributions from the brain power map layer by layer, as indicated by experimental data, the approach can achieve improved accuracy in pilot cognitive detection. The HMM can identify the implicit parameters of the process from the observable parameters and utilize them for further analysis. The challenge of predicting intelligent service quality characteristics in the Internet of Things domain was addressed by Sefati et al. [13] with their suggested service quality prediction approach, which is based on HMM and ant colony optimization algorithms. The method first estimated the quality of service parameters using ant colony algorithm and then used HMM for prediction. In their study, Cheng et al. [14] employed the HMM to provide estimation mode information for the control in order to overcome issues with asynchronicity and data loss associated with the asynchronous output feedback control mode of wind power production systems. Using the Lyapunov function approach and linear matrix inequality technique, they established a sufficient condition for the finite-time boundedness of the continuous closed-loop system that rigorously obeys the (U,G,V)-a-dissipative property.

In recent years, the application of generative adversarial networks (GANs) in the field of cyber secruity has attracted significant interest. GANs can generate realistic network traffic data, which can be used to train more robust network ID systems. Arafah M. et al. [15] proposed a GAN-based detection model in response to the increasing speed and type of cyber attacks on information systems and communication infrastructure. This model enhanced the capabilities of GAN through a bidirectional structure, enabling the classification and detection of network intrusion. Furthermore, transfer learning techniques for deep learning models had garnered significant interest. Transfer learning leverages knowledge acquired in other tasks to accelerate learning in new tasks. In their study, Ullah F. et al. [16] proposed a network traffic ID system based on transformer transfer learning. This system was designed to address the challenges of identifying specific attacks due to the complexity and imbalance of data in current network ID. The system employed transfer learning methods to learn the feature interactions between network feature representations and unbalanced data.

When the aforementioned literature is considered collectively, it becomes evident that empirical knowledge and publicly accessible datasets represent the principal sources of data utilized in contemporary computer science research. Nevertheless, as scientific and technological advancements continue, it becomes increasingly challenging to apply the methodologies currently employed in practical settings [17, 18]. For this reason, the study collects CS data, performs feature extraction, and then uses adaptive theory and IL methods to detect attack events.

3 Network Attack Detection Model Based on HMM and Adaptive Increments

With the popularization of Internet technology, people can easily access the network and carry out various network activities. However, this also leads to an increasing number of security threats to the network environment. For this reason, the study constructs a new NAD approach using the HMM and adaptive incremental approach.

3.1 Cyber Security Data Collection and Pre-processing

Obtaining effective security information from a huge amount of network data is difficult due to the uncountable amount of security information in the network in real network environments farm office [19–21]. In an ordinary network attack may generate a large amount of data in a medium-sized network environment. For this reason, the study collects, processes, correlates, and manages security information in the network to provide more realistic

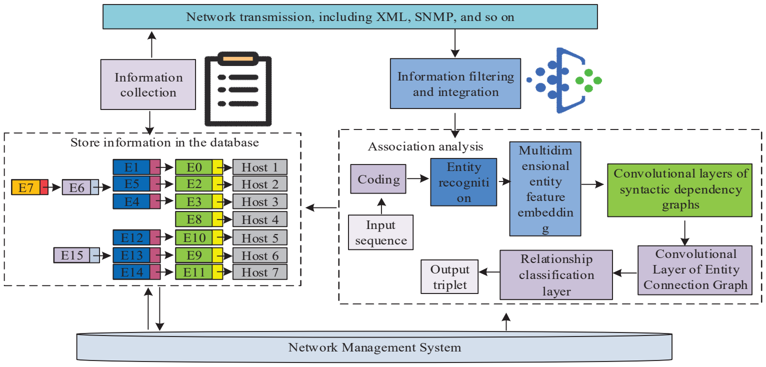

Network transmission, including XML, SNMP, and so on
Information collection
Information filtering and integration
Store information in the database
E7
E6
E1
E5
E4
E12
E13
E14
E15
E0
E2
E3
E8
E10
E9
E11
Host 1
Host 2
Host 3
Host 4
Host 5
Host 6
Host 7
Association analysis
Coding
Input sequence
Entity recogniti on
Multidim ensional entity feature embeddin g
Convolutional layers of syntactic dependency graphs
Convolutional Layer of Entity Connection Graph
Relationship classification layer
Output triplet
Network Management System

Figure 1 Data collection process designed by the research.

CS data for subsequent research and analysis. The data collection process designed by the study is shown in Figure 1.

To ensure the accuracy of the subsequent analysis, the study filters the security information and deals with the error bias present in it, thus improving the quality of the information for the subsequent analysis. The information filtering criterion determined by the study is shown in Equation (1).

$$|a_p - H| < \delta \tag{1}$$

In Equation (1), a is the safety message and a_p is the parameter of the safety message. H is the normal value and δ is the deviation size. In the actual network environment, there is duplication of functions of many security nodes, and the same security behavior may form a large number of security events. When encountering large-scale network traffic attacks, the redundant information generated is very large, which not only far exceeds the actual needs of analysis, but also seriously affects the processing efficiency. For this reason, the study integrates and processes the collected information as a way to shrink the amount of security information and reduce the resources it occupies. Events generated by actors usually contain multiple basic features, and if the basic features of an event belong to the dominant or subordinate features simultaneously, it is said to be of concern. If the basic features of the event do not belong to the dominant or subordinate features, then the event needs to be ignored. For this purpose, the similarity between events needs to be calculated first, and the calculation method is shown in Equation (2).

$$S(e, e') = \begin{cases} 1 & v_{ej} = v_{e'j}, \forall j \in [1, n] \\ 0 & v_{ej} \neq v_{e'j}, \exists j \in [1, n] \end{cases} \tag{2}$$

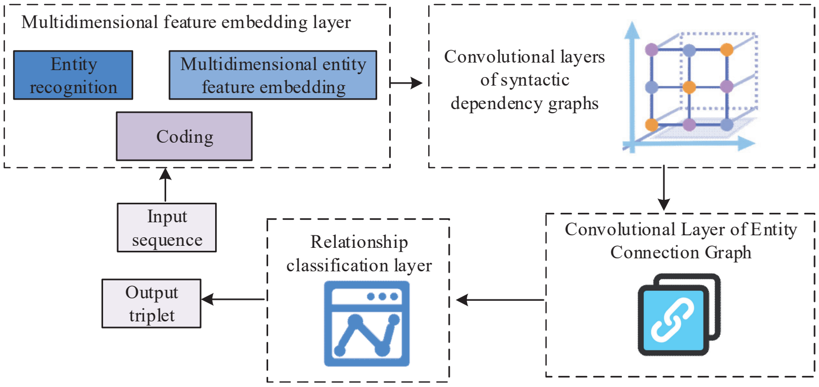

Multidimensional feature embedding layer
Entity recognition
Multidimensional entity feature embedding
Coding
Convolutional layers of syntactic dependency graphs
Input sequence
Relationship classification layer
Convolutional Layer of Entity Connection Graph
Output triplet

Figure 2 Design of the security event relationship extraction model process.

In Equation (2), e and e' are two different security events, v_{ej} and $v_{e'j}$ are the basic characteristics of the two events, and $S(e, e')$ is the similarity of the two security events. If the value of $S(e, e')$ is 1, it means that the two security events are similar and the two cannot be integrated. If the value of $S(e, e')$ is 0, it means that the two security events do not belong to a unified actor and cannot be integrated. Similar security events are considered duplicates if they occur no less often than in the dependent feature set. The event duplicates can then be directly processed by integrating the coverage. In the heterogeneous network environment, security events on each security node are not isolated, and security events generated by the same network behavior are similar to each other. Event correlation analysis security events generated by the same behavior by calculating the dissimilarity degree of the events to form a correlated security event set, which provides a more complete security information flow for subsequent security analysis. The research-designed security event relationship extraction model is presented in Figure 2.

There are two main types of security events characterized by numerical features and character types. Therefore the corresponding dissimilarity measure needs to be targeted. The dissimilarity measure of character features of any two events in the set is calculated as shown in Equation (3).

$$D^s(e_i, e_j) = \sum_{l=1}^{p} \left(\frac{1}{n_{f_{il}}} + \frac{1}{n_{f_{jl}}} \right) \sigma(f_{il}, f_{jl}) \tag{3}$$

In Equation (3), $n_{f_{il}}$ and $n_{f_{jl}}$ are the number of practice shared features taking values f_{il} and f_{jl}, respectively, and $\sigma(\cdot)$ is a function taking values 0 or 1. Similarly, the dissimilarity of numerical features is calculated as shown in Equation (4).

$$D^N(e_i, e_j) = \sum_{l=1}^{p} (f_{il} - f_{jl})^2 \tag{4}$$

The dissimilarity of arbitrary confounding security events is jointly determined by the character dissimilarity and numerical dissimilarity, which is calculated as shown in Equation (5).

$$D(e_i, e_j) = \left(\frac{D^N(e_i, e_j)^2 + D^s(e_i, e_j)^2}{D^N(e_i, e_j) + D^s(e_i, e_j)} \right)^{\frac{1}{2}} \tag{5}$$

Event correlation aggregates and merges the current security event to be detected with existing similar security events based on their dissimilarity.

3.2 Cyber Security Feature Selection

In real networks, more and more cyber-attacks are adopting new approaches and techniques, resulting in the difficulty for existing research to extract and obtain effective features from cyber-attack data and use them for security detection in the absence of empirical knowledge. For this reason, the research proposes to utilize HMM to parse text and binary protocol message formats to provide support for extracting features of actual traffic [22–24]. There are four common protocol message formats, which are text-based protocols, binary-based protocols, TLV-based protocols, and pointer-based protocols. In order to facilitate the subsequent testing, the study utilizes the message grouping method to collect and group the test protocol message data. Due to the large variation of field contents in TLV and pointer-type protocols, it is necessary to analyze the semantic information of the fields with the help of protocol state machines, which has a high computational cost. For this reason, the research mainly focuses on protocols of text type and binary type. In the field of CS, it is very important to master the network protocol specification, which needs to be utilized for feature extraction and type recognition. The security access control also needs to utilize the protocol specification to formulate the corresponding security access rules according to the features in the protocol. Moreover, unknown protocols have a wider application in military, commercial, and some civil scenarios, although they can improve the communication efficiency and security. Unknown protocols are those network protocols that are not widely recognized or defined by a standardization organization. Due to their non-standard and secretive nature, they are often

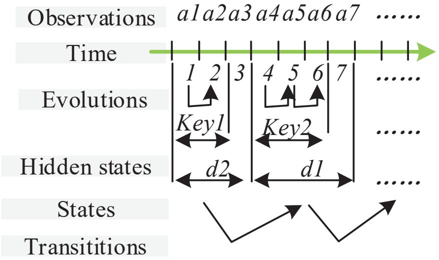


Figure 3 Unknown protocol message model based on HsMM.

used as tools by cyber attackers to increase the complexity and concealment of attacks. However, if these networks receive malicious attacks, it is difficult to detect such threats effectively. Due to the lack of a priori knowledge of the unknown protocols, it is not possible to determine the specific type of message format, so there is a need to propose a generalized message segmentation method that is compatible with existing formats. HMM is a probabilistic statistical model with the ability to simulate temporal data, for this reason, the research utilizes it to construct the unknown protocol message model as a way to analyze the information related to the keywords and fields of the message. To further optimize the feature extraction process, the study uses an extended form of HMM, which is a hidden semi-Markov model (HsMM). It constructs the unknown message model of HsMM according to the common format of the message, as illustrated in Figure 3.

After obtaining the message model of the unknown protocol, the study extracts keywords and field information based on the maximum likelihood criterion to segment the message segments. Finally, a feature extraction method based on message segmentation is proposed to check whether each keyword or its subsequence occurs frequently or not, and if the number of occurrences exceeds a predefined threshold, it is identified as a feature. After extracting the features, the study utilizes elephant herding optimization (EHO) to filter the features with large contributions. A novel population intelligence optimization technique called EHO is designed to solve global unconstrained optimization issues. The clan update operation is the first step in the algorithmic optimization search procedure, and the male elephant separation operation is the second. Throughout the investigation, it is discovered that the conventional EHO is devoid of a functional mutation mechanism, which causes individuals to become quickly drawn to local extremes and results in premature convergence. For this reason, the study introduced the Levy flight strategy into the algorithm. The original position update operation

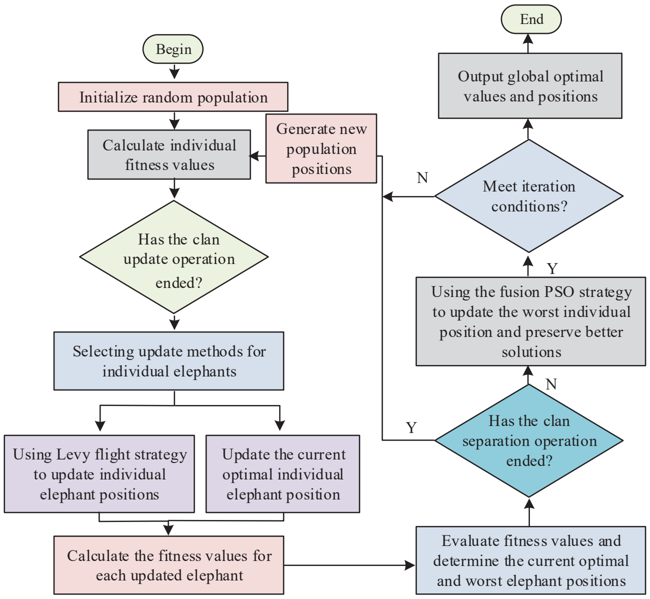

Begin
Initialize random population
Calculate individual fitness values
Generate new population positions
Has the clan update operation ended?
Selecting update methods for individual elephants
Using Levy flight strategy to update individual elephant positions
Update the current optimal individual elephant position
Calculate the fitness values for each updated elephant
Evaluate fitness values and determine the current optimal and worst elephant positions
Has the clan separation operation ended?
Y
N
Using the fusion PSO strategy to update the worst individual position and preserve better solutions
Y
Meet iteration conditions?
N
Output global optimal values and positions
End

Figure 4 Improved image group optimization algorithm flow.

is replaced with Equation (6).

$$x_{new,ci,j} = x_{ci,j} + Levy(\lambda) + \alpha \cdot (x_{best,ci} - x_{ci,j}) \cdot r \tag{6}$$

In Equation (6), $x_{new,ci,j}$ is the updated position and $x_{ci,j}$ is the individual elephant. $Levy(\lambda)$ is the random search path, λ is a parameter, and α is a scale factor to control the step size. $x_{best,ci}$ is the best-positioned matriarch in the clan, and r is a random number used to increase the random number of population diversity. To address the issue of randomness in the removal of male elephants that are not well suited for the elephant herd separation process, the study employs a particle swarm optimization technique. This strategy involves calculating the fitness function value of each individual particle. The improved EHO process is shown in Figure 4.

3.3 Construction of Network Attack Detection Model

Existing network ID models are generally over-reliant on well-labeled security datasets, but new classes of attacks often emerge in real-world scenarios. For this reason, the research applies adaptive class IL methods to ID. As mentioned above, this study uses HMM and HsMM to model and analyze

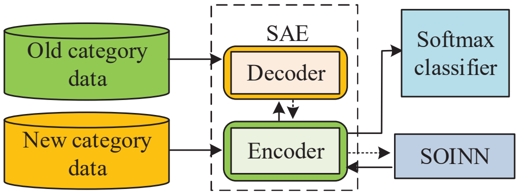


Figure 5 A framework of cyber attack detection model based on adaptive incremental learning.

unknown protocol messages and extract key feature information. The filtered features are input into the adaptive class IL ID model. The study combines stacked auto-encoder (SAE) and self organizing incremental neural networks (SOINN) to sparsely encode high-dimensional data, while the extracted features are mapped into the topological space, and indirectly constrained according to the topological update rules and defined topological constraint functions weight changes in the encoder and thus realize IL. To enhance the adaptability of the model and its ability to cope with new types of attacks, an adaptive class IL method is introduced, which combines SAE and SOINN. The method involves stacking multiple autoencoders layer by layer, whereby SAE extracts the features of the data layer by layer, and finally obtains a low-dimensional feature representation. SOINN is then able to establish topological relationships between features and perform IL based on the topological relationships, by mapping features into topological spaces. In the process of IL, SOINN dynamically adjusts the weight and topology of the network based on new input data to adapt to new categories of attacks. To combine SAE and SOINN effectively, a topology update rule and a defined topology constraint function are introduced. By studying these rules and functions, weight changes in encoders are indirectly constrained. The aforementioned methodologies have been employed to construct a NAD model with adaptive and IL capabilities, thereby enabling effective response to novel attack types and changes. The framework of the adaptive IL based NAD model designed in this study is illustrated in Figure 5.

Following the implementation of CS data collection, pre-processing, and feature selection as outlined in the preceding section, the study employs SAE to construct a feature extractor and inputs the extracted features of the old category data into SOINN, which then completes the initialization in accordance with the topology update rules. This is followed by the IL phase. When a new category of samples is to be trained, the new category samples are input into SOINN through the SSAE encoder, and SOINN generates a new local topology adaptively according to the topology update rule. At the same time, the change of the weights of the old nodes is constrained, and the weights of the encoder are constrained by error calculation and backpropagation. The study introduces the KL discretization to assess the similarity between the average activation output of each hidden layer node and the sparsity, which is determined as stated in Equation (7). The sparsification of multiple selfencoders results in a stacked bisected SAE.

$$\begin{cases} KL(\rho||\hat{\rho}_j) = \rho \log_{a'} \dfrac{\rho}{\hat{\rho}_j} + (1-\rho) \log_{a'} \dfrac{1-\rho}{1-\hat{\rho}_j} \\ \hat{\rho}_j = \dfrac{1}{m} \sum\limits_{i=1}^{m} [a_j'^2 x^i] \end{cases} \tag{7}$$

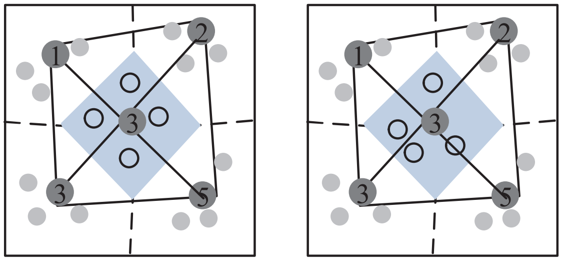
In Equation (7), $\hat{\rho}_j$ is the average activation output of each hidden layer node, ρ is the set sparsity, and $a_j'^2 x^i$ is the response output of the jth node in the hidden layer to the ith sample. Based on the discretization, after the encoder extracts the features from the data, the study utilizes a random initialization method to initialize the SOINN. The neuron set, node weights are initialized first. Then input the new sample corresponding to the features, both Euclidean distance to find the nearest neuron node and the second closest node in the neuron set. The calculation method is shown in Equation (8).

$$\begin{cases} s_1 = \arg\min \|\xi - W_c\|, \quad c \in A \\ s_2 = \arg\min \|\xi - W_c\|, \quad c \in A \backslash \{s_1\} \end{cases} \tag{8}$$

In Equation (8), A is the set of neurons and ζ is the feature corresponding to the input new sample. W_c is the node weights, c is the initial node, and s_1 and $s_2 s_2$ are the closest and second closest nodes to node c. If two nodes satisfy Equation (8), a new node is inserted for the new feature and the node weights are updated. In the IL phase, in order to maintain the original topology, a loss function needs to be designed for its changes to maintain the stability of the topology by limiting the movement of nodes. Equation (9) displays the loss function calculation.

$$l_a = \sum_{v \in V^t, x \in D^t} (\hat{v} - v)^T \Lambda^{-1} (\hat{v} - v), \hat{v} = f(x) \tag{9}$$

In Equation (9), t is the number of current stages, l_a is the loss value, and $\hat{v}$ and v are the node weight vectors of the current and previous stages,



(a) Node distribution aggregation

(b) Scattered node distribution

Figure 6 Differences in node distribution.

respectively. Λ is the diagonal matrix consisting of the variance of v in each dimension, and $f(\cdot)$ is the SAE encoder function. Considering the large variance of some node dimensions, there may be a situation where the distinction between old and new nodes is not obvious. The node distribution variance is shown in Figure 6.

In order to ensure that the Euclidean distance between newly inserted nodes and different neighboring nodes in SOINN is greater than a certain value, the study optimizes the loss function and the optimization result is shown in Equation (10).

$$l_d = \sum_{c_j, x \in D^t} d(f(x), v_j) - \sum_{c_i \neq y} min(0, d(v_i, v_j) - d_{min}) \tag{10}$$

In Equation (10), c is the sample label, y is the t moment category label, and $d_{\min}$ is the minimum distance threshold. If $d(v_i, v_j)$ is greater than $d_{\min}$, then the distance is considered to be large enough not to require a limit, at which point the item is eliminated and the maximum value is chosen to be the value of the hyperparameter $d_{\min}$. In the IL phase, the study uses a small batch gradient descent algorithm to train the SAE encoder and SOINN, and the error is back propagated into the encoder for fine-tuning based on the calculated loss. The synthesis of the above realizes the detection of network intrusion. To enhance the capacity of the research design model to discern intricate patterns, this study employs deep learning methods to refine it. Building upon the original SOINN, this study introduces the concept of deep learning to construct a Deep-SOINN model. The model is constituted by a series of stacked SOINN layers, each of which performs feature extraction and classification on the input data, and then transmits the outcomes to the subsequent layer of SOINN as input. In this manner, Deep-SOINN is capable of learning more intricate data patterns and enhancing its detection accuracy.

4 Performance Analysis of Network Attack Detection Model

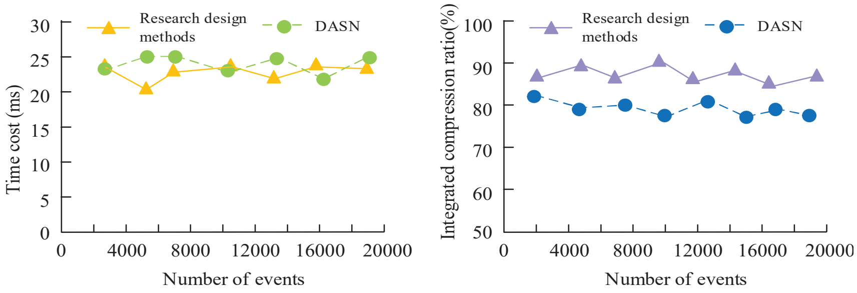
4.1 Experimental Configuration

In order to evaluate the performance of the designed network ID model, the KDD Cup 99 dataset is used for testing. This dataset is a widely used benchmark for evaluating the performance of network ID systems and contains data on multiple types of network attacks and normal network traffic. Each record in the data set contains several characteristics, such as duration, protocol type, service type, number of source bytes, number of destination bytes, and so on. The experiment was conducted in the Python environment. In order to provide a comprehensive evaluation of the model's performance, the research team employed a range of evaluation indicators, including accuracy, precision, recall, F1 score, and detection coverage. These indicators are selected to provide a comprehensive assessment of the model's performance.

4.2 Performance Analysis of Network Intrusion Detection Methods Based on HMM and Adaptive Incremental Model

To evaluate the effectiveness of information filtering as well as integration, experiments were conducted to determine and compare the information collection and processing methods designed by the research with the DASN event management model. The distributed denial-of-service (DoS) attack is simulated mainly by PureSecure, and the generated attack events are utilized as a test set to compare the system time overhead with or without information processing and the compression ratio metrics after information processing. Figure 7 presents the comparison results.

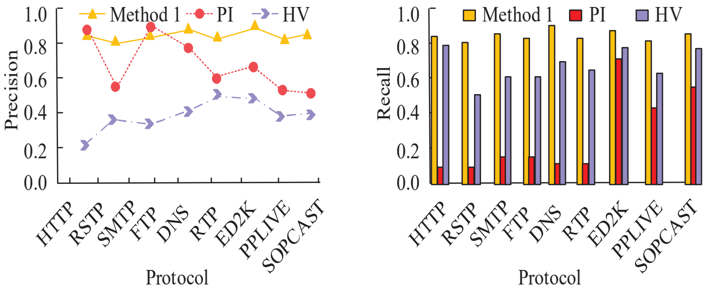
In Figure 7(a), the research-designed data processing method imposes a higher time overhead than DASN, but the difference is not significant. The average time overhead of the research-designed method is 25.841 ms, while the average time overhead of DASN is 14.125 ms. In Figure 7(b), the compression ratio achieved by the research-designed method is higher than 87% when the number of events is 2000, and the compression ratio starts to decrease gradually as the number of events increases, but it is always higher than 80%. The compression ratio of DASN floats around 80%. Taken together, the method proposed in this paper is able to reduce the security



(a) Time cost

(a) Integrated compression ratio

Figure 7 Comparison of time cost and compression ratio indicators.



(a) Precision

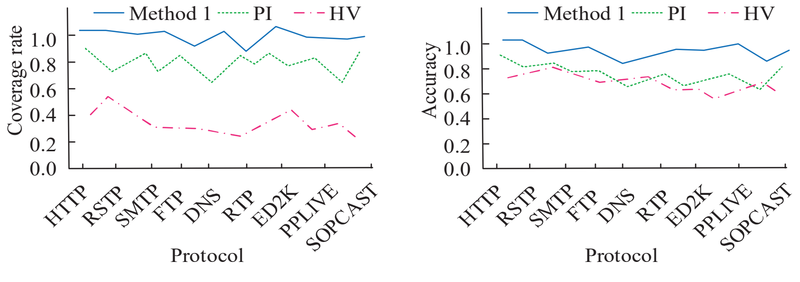
(b) Recall

Figure 8 Comparison results of precision and recall rate.

event information and maintain a relatively good processing efficiency while reducing the space overhead of security events.

To assess the efficacy of the message protocol parsing method (Method 1) developed in the study, the study compares its performance with that of more popular methods for parsing messages of unknown protocols. The comparison methods include protocol informatics (PI) project method [25]. a parsing method based on binary protocol (HV) [26]. The comparison metrics include precision and recall. The comparison results are shown in Figure 8.

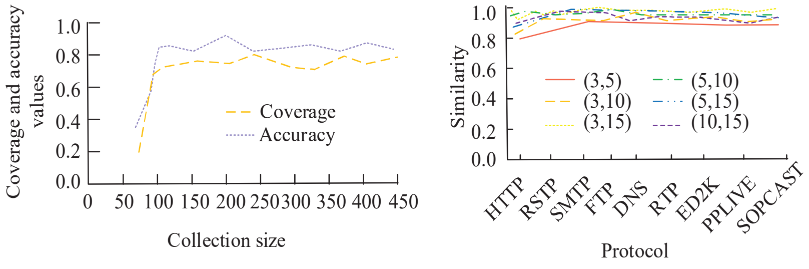
In Figure 8(a), it is visible that Method 1 achieved higher accuracy than HV on all protocol data sets. Method 1 also has higher accuracy than PI on all protocol sets except HTTP and FTP, and the average accuracy of Method 1 is 80.15%. In Figure 8(b), Method 1 has the best Recall value with an average of 85.45%, which is significantly higher than the other two methods. In order to further examine the performance of the protocol parsing methods designed in the study, the experiment continues to introduce coverage and accuracy as



(a) Coverage rate

(b) Accuracy

Figure 9 Comparative results of the coverage and accuracy of the three methods.



(a)The impact of collection size

(b) Similarity

Figure 10 Performance analysis of method 1 under the same influencing factors.

evaluation metrics, and the comparison results of these two performances of the three methods are illustrated in Figure 9.

In Figure 9(a), the coverage results obtained by method 1 on the protocols HTTP and ED2K are 100%, and the coverage on the other protocols is over 84%, while none of the other two methods exceeds 85%, and the minimum coverage appears to be below 50%. In Figure 9(b), the accuracy of the three methods do not differ much, but Method 1 has the best stability, which basically stays around 90%. In order to assess the impact on the performance of method 1 under different parameters, the study randomly extracted subsets of different sizes and different numbers of states from the traffic collection for testing, and the test results are shown in Figure 10.

In Figure 10(a), the coverage and accuracy of method 1 gradually increase with the growth of the set size, and when the set size exceeds 50, method 1 remains stable, and both the coverage and accuracy remain above 80% and 90%. In Figure 10(b), the similarity of several states basically exceeds 90% when the number of compared states is 3, 5, 10, and 15, which indicates that Method 1 is less affected by the number of states. In order to examine the

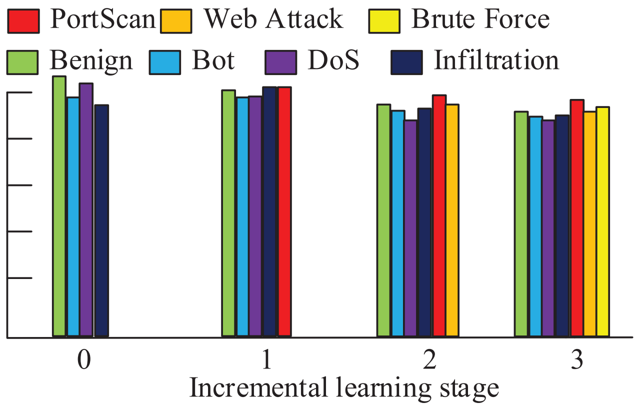


Figure 11 The change of the detection accuracy of the model for different types of attacks.

Table 1 Comparison of the performance indicators of the three models in different stages

	Old Category Data			New Category Data		
Project	Accuracy	Recall	F1 score	Accuracy	Recall	F1 score
Model 1	0.945	0.954	0.942	0.875	0.885	0.868
KNN-SVM	0.921	0.925	0.918	0.772	0.751	0.764
mCNN	0.905	0.897	0.900	0.701	0.698	0.710

performance of the NAD model (Model 1) designed by the study, the study selects three categories of attacks, PortScan, Web Attack, and Brute Force, as the new category data, and four categories of data, Benign, Bost, Dos, and Infiltration, as the old category data. For this purpose, the study records the change in attack detection accuracy of the model under different phases and the results are shown in Figure 11.

In Figure 11, with the addition of the new category attack samples in the IL phase, the attack detection rate of the old category data shows a decreasing trend, but its recognition accuracy is still above 80% after the completion of the third phase of training. In addition, the recognition accuracy of the new categories are 89.45%, 91.23%, and 90.88%, respectively. To further explore the performance of Model 1, the study uses it to compare with the attack detection method based on K-nearest neighbor-support vector machine (KNN-SVM), and the multi-convolutional neural network (mCNN). The comparison results are shown in Table 1.

In Table 1, both KNN-SVM and mCNN produce a large decline in detection performance for new types of attacks after IL, with recognition accuracy below 0.8. In contrast, Model 1 has an attack detection accuracy

Table 2 Comparison of detection results under different scales and complexities

Model	Resource Utilization	Detection Accuracy	Response Time (s)	Scalability
Model 1	0.92	0.91	0.25	High
Model 2	0.90	0.89	0.30	Medium
Model 3	0.80	0.87	0.28	Low
Model 4	0.88	0.85	0.27	Medium
Model 5	0.86	0.82	0.32	High

of more than 0.8% for both old and new categories of data, and its average detection accuracy is 91.15%.

To further validate the model, the study initially employs the existing category data for the initial training of the model and records its performance on the test set. Thereafter, the new category data is introduced incrementally, the model is updated through IL, and the performance of the model on the old and new category data is evaluated at each stage. In the initial stage, the model achieved an accuracy of 94.5%, a recall of 95.4%, and an F1 score of 94.2%. Following the introduction of the new category data, the accuracy of the model on the old category data exhibited a slight decline, yet remained above 80%, indicating a robust stability of the model. Concurrently, the accuracy of the model reached 87.5% on the new category data.

To further validate the generalizability of the model in a variety of different situations, research selected several datasets of more complex network attacks for testing. These datasets cover many different types of attacks, such as DDoS attacks, XSS attacks, SQL injection, and contain network traffic data of varying sizes and complexity. At the same time, a wider range of performance metrics are used to further test the model's performance, including: resource utilization, detection accuracy, response time, and scalability. A comparison of the existing advanced technology analysis with the comparison model is presented. The comparison model includes: based on improved noise reduction coding model ID model (model 2), based on cattle optimization and improve the regularization of limit learning machine network ID model (model 3), based on grey wolf algorithm network ID (model 4), based on internal and external convolution network ID (model 5). The test results are shown in Table 2.

Table 2 indicates that Model 1 exhibits superior performance in terms of resource utilization, detection accuracy, response time, and scalability across a range of networks, with varying sizes and complexities of network traffic data. Compared to Models 2, 3, 4, and 5, Model 1 demonstrates an advantage in detection accuracy, attributed to its IL-based design that effectively handles the introduction of new classes of data. In addition, the resource utilization of Model 1 is relatively low, indicating its efficacy in actual deployment. With regard to response time, Model 1 demonstrates satisfactory performance and is able to rapidly complete the detection of network attacks. Furthermore, Model 1 exhibits high scalability, enabling it to accommodate network traffic data of varying sizes and complexities. The practical significance of the proposed model is that it can accurately detect new and old types of network attacks, which is of great significance for real-time monitoring of network environments and timely detection and response to potential threats. Furthermore, the research design model can adapt to new cyber attacks through IL, reducing the dependence on a large number of security devices and professionals. The research model has a fast response speed and can improve the safety processing efficiency. Furthermore, the findings of the study illustrate the substantial potential of IL in the domain of CS and contribute to the advancement of CS technology.

5 Conclusion

In the field of computer science, traditional security technologies may appear inefficient and outdated. To address this issue, this study proposes a method for acquiring and processing security information, which is then applied in subsequent analyses. Additionally, an improved HMM and adaptive IL methods are used to construct a network ID model. The experimental results revealed that the average time overhead of the data processing methods designed for the study is 25.841 ms and the compression ratio is always higher than 80% with the increase in the number of events. The coverage results obtained by method 1 on protocols HTTP and ED2K were 100%, and the coverage on other protocols was more than 84%, while the coverage of the other two methods did not exceed 85%. In the case of comparing the number of states as 3, 5, 10 and 15, the similarity of several states basically exceeded 90%, which indicates that Method 1 is less affected by the number of states. The detection accuracy of Model 1 for the new category of attacks was 89.45%, 91.23%, and 90.88%, respectively, in the process of performing IL. It can be concluded that the CS detection model based on HMM and adaptive increment designed by the research can realize the accurate identification of newly generated attacks in the real network environment, and adapt to the characteristics of the network environment, which is characterized by the huge amount of data, diversified services and rapid evolution. In the actual network environment, network traffic and attack patterns may change dynamically over time. While the proposed model employs IL methods to accommodate the introduction of new category data, further research is necessary to elucidate more effective strategies for responding to changes in the dynamic network environment.

References

[1] Asgupta D, Akhtar Z, Sen S. Machine learning in cybersecurity: a comprehensive survey. The Journal of Defense Modeling and Simulation, 2022, 19(1): 57–106.

[2] Pamarthi S, Narmadha R. Literature review on network security in Wireless Mobile Ad-hoc Network for IoT applications: network attacks and detection mechanisms. International Journal of Intelligent Unmanned Systems, 2022, 10(4): 482–506.

[3] Wazid M, Das A K, Chamola V, Park Y. Uniting cyber security and machine learning: Advantages, challenges and future research. ICT Express, 2022, 8(3): 313–321.

[4] Sarker I H, Khan A I, Abushark Y B, Alsolami F. Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions. Mobile Networks and Applications, 2023, 28(1): 296–312.

[5] Ferrag M A, Shu L, Friha O, Yang X. Cyber security intrusion detection for agriculture 4.0: Machine learning-based solutions, datasets, and future directions. IEEE/CAA Journal of Automatica Sinica, 2021, 9(3): 407–436.

[6] Azizan A H, Mostafa S A, Mustapha A, Foozy C F M, Wahab M H A, Mohammed M A, Khalaf B A. A machine learning approach for improving the performance of network intrusion detection systems. Annals of Emerging Technologies in Computing (AETiC), 2021, 5(5): 201–208.

[7] Roy S D, Debbarma S, Guerrero J M. Machine learning based multiagent system for detecting and neutralizing unseen cyber-attacks in AGC and HVDC systems. IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 2022, 12(1): 182–193.

[8] Li Q, Zhang J, Zhao J, Ye J, Song W, Li F. Adaptive hierarchical cyber attack detection and localization in active distribution systems. IEEE transactions on smart grid, 2022, 13(3): 2369–2380.

[9] Nuiaa R R, Manickam S, Alsaeedi A H, Alomari E S. A new proactive feature selection model based on the enhanced optimization algorithms

to detect DRDoS attacks. Int. J. Electr. Comput. Eng, 2022, 12(2): 1869–1880.

[10] AlShahrani B M M. Classification of cyber-attack using Adaboost regression classifier and securing the network. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 2021, 12(10): 1215–1223.

[11] Peng H, Yang R, Wang Z, Li J, He L, Philip S Y, Ranjan R. Lime: Low-cost and incremental learning for dynamic heterogeneous information networks. IEEE Transactions on Computers, 2021, 71(3): 628–642.

[12] Wu E Q, Lin C T, Zhu L M, Tang Z R, Jie Y W, Zhou G R. Fatigue detection of pilots' brain through brains cognitive map and multilayer latent incremental learning model. IEEE Transactions on Cybernetics, 2021, 52(11): 12302–12314.

[13] Sefati S, Navimipour N J. A qos-aware service composition mechanism in the internet of things using a hidden-markov-model-based optimization algorithm. IEEE Internet of Things Journal, 2021, 8(20): 15620–15627.

[14] Cheng P, Wang H, Stojanovic V, Liu F, He S, Shi K. Dissipativity-based finite-time asynchronous output feedback control for wind turbine system via a hidden Markov model. International Journal of Systems Science, 2022, 53(15): 3177–3189.

[15] Arafah M, Phillips I, Adnane A. Evaluating the impact of generative adversarial models on the performance of anomaly intrusion detection. IET Networks, 2024, 13(1): 28–44.

[16] Ullah F, Ullah S, Srivastava G, Lin J C W. IDS-INT: Intrusion detection system using transformer-based transfer learning for imbalanced network traffic. Digital Communications and Networks, 2024, 10(1): 190–204.

[17] Wang H, Li X. Optimization of Network Security Intelligent Early Warning System Based on Image Matching Technology of Partial Differential Equation. Journal of Cyber Security and Mobility, 2024: 461–488.

[18] Dawson J K, Twum F, Acquah J B H, Missah Y. M Cryptographic Solutions for Data Security in Cloud Computing: A Run Time Trend-based Comparison of NCS, ERSA, and EHS[J]. Journal of Cyber Security and Mobility, 2024: 265–282.

[19] Zhan D, xing H. A fast kriging-assisted evolutionary algorithm based on incremental learning. IEEE Transactions on Evolutionary Computation, 2021, 25(5): 941–955.

[20] Bansiwala R, Gosavi P, Gaikwad R. Continual Learning for Food Recognition Using Class Incremental Extreme and Online Clustering Method: Self-Organizing Incremental Neural Network. International Journal, 2021, 6(10): 36–40.

[21] Zhiyong G, Jiwu L, Rongxi W. Prognostics uncertainty reduction by right-time prediction of remaining useful life based on hidden Markov model and proportional hazard model. Eksploatacja i Niezawodność, 2021, 23(1): 154–164.

[22] Wang Z, Chen C, Dong D. Lifelong incremental reinforcement learning with online Bayesian inference. IEEE Transactions on Neural Networks and Learning Systems, 2021, 33(8): 4003–4016.

[23] Conners M G, Michelot T, Heywood E I, Orben R A, Phillips R A, Vyssotski A L, Thorne L H. Hidden Markov models identify major movement modes in accelerometer and magnetometer data from four albatross species. Movement ecology, 2021, 9(1): 1–16.

[24] Aryavalli S N G, Kumar G H. Futuristic Vigilance: Empowering Chipko Movement with Cyber-Savvy IoT to Safeguard Forests. Archives of Advanced Engineering Science, 2023, 1(8): 1–16.

[25] Graveto V, Cruz T, Simões P. A network intrusion detection system for building automation and control systems. IEEE Access, 2023, 11(2): 7968–7983.

[26] Senier A. Tutorial: The End of Binary Protocol Parser Vulnerabilities: Using RecordFlux and SPARK to implement formally-verified binary formats and communication protocols. IEEE Secure Development Conference (SecDev). IEEE, 2023, 2023(2): 5–6.

Biography

Liwen Xu, was born in Jiangsu Province, JS, CHN in 1986. She received her bachelor's degree in law from Nanjing University of Finance and Economics, Jiangsu, China, in 2009, and her master's degree in law from Southeast University, Jiangsu, China, in 2018.

From 2009 to 2019, she worked as a counsellor in the School of Business of the Open University of Jiangsu, China. Since 2020, she has been working as a deputy director of the experiment training center of the School of Business of Jiangsu Open University, Jiangsu, China, and a lab technician Intermediate title. During her tenure, she has obtained one computer software copyright and published 24 papers in public. Her research interests include basic computer technology, experimental practice teaching, education informatization technology, laboratory construction and management.