Hindawi
Mobile Information Systems
Volume 2022, Article ID 7302623, 9 pages
https://doi.org/10.1155/2022/7302623

Research Article

Construction of Early Warning Mechanism of University Education Network Based on the Markov Model

Lianghai You

Shangqiu Institute of Technology, Shangqiu 476000, China

Correspondence should be addressed to Lianghai You; 1350007007@sqgxy.edu.cn

Received 21 May 2022; Revised 23 June 2022; Accepted 27 June 2022; Published 31 July 2022

Academic Editor: Liping Zhang

This paper proposes and builds an early warning mechanism model of the college education network using the Markov model. This paper proposes a method to determine the observation value of Markov model based on the flow control principle and TCP/IP model in an effort to address the issue that the observation value of Markov model is challenging to determine when it is applied to intrusion detection. The detection model also employs an adaptive sliding detection window algorithm to further increase the system's detection rate. The mechanism developed in this paper is compared to other early warning mechanisms in order to confirm the validity and applicability of the educational network early warning mechanism. The experimental results demonstrate that the accuracy of the educational network early warning mechanism in this paper is higher than that of the conventional early warning mechanism, which is 9.87 percent, at up to 95.02 percent. The proposed model, however, clearly excels in terms of early warning adaptability, model fitting level, and information overload processing effectiveness. In general, this paper successfully applies the Markov model to the early warning system of the college education network. For the study of the college education network's early warning system, it has some reference value.

1. Introduction

In order for the network to offer people convenient services, network security must be in place. Network security issues are being put to progressively more difficult tests as network attack methods diversify [1]. The college education network system has gradually evolved into a professional and interactive information exchange carrier in tandem with the rapid development of information technology. In order to efficiently share instructional resources, the college education network makes use of cutting-edge computer technology and network communication capabilities. The network platform is currently a common teaching tool in classrooms and has taken the place of other methods as the primary way to enhance teaching quality. The network security of a university still has some unrecognised risks, though [2]. The campus network is attacked by malicious software and infected by foreign viruses as a result of the openness of the educational network system connections and the variety of information resources, which has a serious negative impact on the design of the educational network in higher education institutions. Traditional security defenses are incapable of handling complex network attacks because they lack initiative and dynamics, always employ a "slow beat" defensive strategy, and lack the ability to take initiative. The security of a higher education institution's network is now a top priority for the institution [3]. The campus management of institutions of higher learning has fully embraced network technology, but the network security issue has significantly impacted how these institutions are run on a daily basis. Determining the risk level through vulnerability detection is the conventional risk assessment method for college education network security [4]. The current vulnerability detection tools primarily focus on the security performance of a single device; however, they have limited capability to evaluate the security performance of the entire network. The vulnerabilities and flaws in the university network system are getting worse by the day due to the ongoing development of hacker technology. A link that institutions of higher learning currently need to focus more

on is how to ensure the security of the network system for higher education and promote its practicability into full play [5]. The hidden risks associated with educational networks in higher education institutions can be further reduced by information technology, which can also support the long-term growth of network platforms in these institutions.

Early warning systems for network security can accurately identify risks before an attack and offer technical assistance for implementing network active defense and ensuring network security [6]. However, at the moment, early warning technology research primarily focuses on attack behavior, and the complexity and diversity of network attacks frequently cause issues with these early warning technologies, such as state space explosion [7]. As a result, early warning technology based on attack behavior has some implementation limitations. A probabilistic model with parameters, the Markov model, is used to describe random process statistics. The next state of a process depends on the current state, not the previous state, according to the Markov model. The initial state of the entire process has nothing to do with the previous Markov process, but there is a probability in a Markov process that can be calculated from the previous state in the transition process between every two states [8]. The Markov model can obtain the corresponding Markov model by using the gathered training samples for adaptive learning. Its algorithm is established and effective, and it has frequently been applied to intrusion detection research [9]. The intrusion detection system based on the Markov model has good real-time due to the intrusion detection model's characteristics of small amount of data generated by the model and simple detection rules. In other words, Markov chain is a Markov process with discrete state and time parameters [10]. Markov chain is a special case of the Markov random process. Based on the analysis of the existing network security early warning technologies, this paper puts forward and constructs an early warning mechanism model of college education network by combining compound attack, attack intention, and Markov model. The main contributions of this paper are as follows:

(1) Aiming at the problem that the observation value of Markov model is difficult to determine when it is applied to intrusion detection, this paper proposes a method to determine the observation value of Markov model based on the flow control principle and TCP/IP model. At the same time, it is proposed to improve the training time efficiency by constraining the initial parameter matrix of the model before training. Through the experiment, it can be found that this method significantly reduces the scale of observation set and shortens the training time, effectively improving the time efficiency of training.

(2) When constructing the early warning mechanism of college education network, the network intrusion detection mode based on anomaly is adopted, and the changing rules of the flag bits and port numbers of network protocols under normal network conditions are analyzed. In this early warning technology, the forward algorithm is used to calculate the probability of the Markov model of compound attack generating an alarm information sequence, and the improved Viterbi algorithm is used to identify the attacker's attack intention. Finally, the two methods are combined to predict the attacker's next attack. Experiments show that the detection rate of network attacks in this paper has been greatly improved, and it can better warn a large number of network attacks.

2. Related Work

Compound attack has become one of the main forms of network intrusion. How to detect and predict compound attack is a difficult point in network early warning technology. Early warning technology lays the foundation for realizing active defense of network security, and it is one of the research hotspots nowadays.

In order to accurately assess network security risks in real time, Granjal et al. proposed a Markov model-based network security risk assessment method. This method models the target network based on the Markov model [11]. Daniel-Ioan proposed a new security risk assessment model for university education network based on simulated attack [12]. Mekki et al. introduced the relevant security risks in the educational network of institution of higher learning and discussed the important influence of computer technology in campus network security; at the same time, they explored how to use computer technology in campus network security [13]. Beck proposed a compound attack modeling method based on attack intent [14]. This method regards attack purpose as attack intent and understands compound attack from the perspective of active defense. The advantages of composite attack representation based on attack intent are analyzed from the perspective of being beneficial to attack early warning and active defense. Einy et al. designed an intrusion detection algorithm based on the theory of Markov model and BP neural network [15]. The algorithm effectively improves the detection rate. Liu et al. performed risk assessment of target network based on Bayesian attack graph [16]. The model combines intrusion detection information to dynamically update the generated Bayesian attack graph to evaluate network security risks in real time; however, the impact of network node correlation on network security risks is not considered in the evaluation process. Wu explored the construction of an intrusion detection system based on the Markov model and proposed an adaptive sliding detection window algorithm in the intrusion detection system [17]. Experiments show that the implementation of the algorithm can greatly improve the detection rate of the intrusion detection system. Carnimeo et al. proposed an optimized real-time cybersecurity risk assessment method [18]. This method reduces the scale of input parameters in the evaluation process, but in the evaluation process, the overall risk of the network is quantified by adding the risks of the hosts, and the importance of the hosts in the network is not considered, which is inconsistent with the actual situation of the network.

This paper proposes and builds an early warning mechanism model of the college education network using the Markov model, based on in-depth research and discussion on the relevant literature of predecessors. This paper proposes a method to calculate the observation value of the Markov model based on the flow control principle and the TCP/IP model in order to address the issue that the observation value is challenging to determine when the Markov model is applied in the field of intrusion detection. The initial parameter matrix of the model is suggested to be constrained prior to training in order to reduce training time. The improved Viterbi algorithm is used to determine the attacker's attack intention, and the early warning technology calculates the likelihood that the compound attack's Markov model will generate the alarm information sequence through the forward algorithm. The two calculations are then combined to predict the attacker's next move. The early warning mechanism model presented in this paper has strong generalised early warning capability, accurate dynamic early warning, and high efficiency in predicting the change trend of risk management and control, according to experiments.

3. Methodology

3.1. Network Security Early Warning Technology. The security risk of educational network in institution of higher learning refers to some potential security problems; for example, the users of campus network unconsciously or consciously use the vulnerability of information system and its management system to destroy, steal, and spread some sensitive information and destroy the network operation. Network attack is a common problem in the network security of higher education, and foreign attackers are generally hackers with network information technology. Network attacks are a serious threat to the security of the network. Predicting network attacks has become an important part of active defense research. Intrusion detection is the discovery of intrusion behavior, which is the combination of software and hardware of intrusion detection. Intrusion detection is an active security technology, which has the functions of identifying intrusion behaviors, preventing the occurrence and expansion of intrusion events, etc. Intrusion detection technology is an important security detection technology. By extracting the key information in the current network, this technology detects whether the key information violates the security policy of the security rule base, so as to detect whether there is a network attack in the current network and give an early warning to the network attack. Intrusion detection is a reasonable complement to firewall, which helps the system to deal with network attacks, expands the security management ability of system administrators, and improves the integrity of information security infrastructure. It collects information from a number of key points in the computer network system [19, 20] and analyzes this information. The biggest difference from other security products is that intrusion detection systems are more intelligent. Anomaly detection is to model the normal behavior characteristics of the system. In the process of detection, whether the system deviates from the normal behavior model is monitored. When the deviation is too large, it is considered that an intrusion occurs. A complete intrusion detection system includes the following parts: attack detection, attack response, record of attack behavior and extraction of attack evidence, and evaluation of loss after attack. In a complete attack process, every attack is generally an exploitation of a certain system vulnerability or weakness. A successful attack process often includes several scattered attack steps. If each attack step is regarded as an independent attack, the attack process is composed of them.

With the increasing types of intrusions, coupled with many attacks that have been prepared for a long time, they are carried out through online collaboration. Faced with this situation, it is very important to share this kind of attack information between different functional components of intrusion detection system and different IDS. To carry out intrusion detection on network attacks, it is necessary to deeply understand the generation principle, attack methods, and attack process of existing network attacks. When establishing an intrusion detection model, it is necessary to comprehensively consider the characteristics of a complete network attack and abstract the above useful characteristics. Only in this way can an effective intrusion detection model be designed. Network security early warning mainly finds intrusion signs according to abnormal network traffic, abnormal network behaviors, virus threats, etc. When the attacker's ultimate goal has not yet been achieved, it matches the intrusion process through a prebuilt attack model, judges the attacker's next possible attack behavior, and evaluates the impact of the attack on the network and the threat it will pose soon. In anomaly detection, it is first necessary to build a behavior model of normal behavior through normal data. The basic idea of the model construction is that there are differences between intrusion behavior and normal behavior. The training data used to train the normal model can be system audit records, network data, system call sequences or system call parameters, etc. In the actual running network environment, the change of node state accords with the law of Markov model. The special logical relationship between nodes, such as control relationship and access relationship, will have a certain impact on the results of network security risk assessment. Different nodes have different positions in the network, and the security risks brought by attacks are different. The problem of host-based intrusion detection system is that it requires high reliability of the system. In order to extract intrusion information, it requires that the system should have reasonable settings in addition to its basic security functions. Use the trained normal behavior model to distinguish normal behavior from abnormal behavior. All behaviors that are not within the scope of normal behavior patterns are considered abnormal. The intrusion detection model built by Markov model has the characteristics of small amount of data generated by the model and simple detection rules, so the intrusion detection system based on Markov model has good real-time.

3.2. Markov Model. A statistical analysis model called a Markov model was created using the Markov chain as its foundation. The next state in the future is only related to the current state, but not to any previous states, giving rise to the Markov chain's characteristic of having no aftereffect [21]. The observed value and the state in the Markov chain model are one to one. The observer can determine the value's state by observing the observed value. The observed values and states in the Markov model, however, do not line up one after the other. The observer can only directly perceive the observed value, not the state, and can only infer the state's existence and properties through a random process. Every transition between two states in a Markov process is subject to a probability. Although it is possible to calculate this probability from the previous state, the initial state of the entire process has nothing to do with the preceding Markov process. Two stochastic processes are present in the Markov model, one of which is the fundamental stochastic process of state transition and the other of which is used to describe the statistical relationship between state and observation. The Markov model's internal state is hidden from the observer, who can only see the observed values. However, the observer can determine the existence and characteristics of the internal state from the sequence of external observations. A double stochastic process with two parts is the Markov model. The first is the Markov chain, which uses the concept of transition probability to describe the change in state. The probability of observation values describes one general stochastic process, which describes the relationship between states and observation sequences. The observation value can be obtained by observation when building a state and observation model in a Markov model, but the state value cannot be obtained directly and must instead be calculated using the observation value as a parameter. To train the most likely state transition and determine the corresponding output probability, use the typical system call sequence as the known observation sequence. This is the classic Markov model problem. The training of the Markov model is the most crucial link when solving real-world issues. It is equivalent to creating an optimal model because the parameters of a given model should be changed until they are optimal in accordance with the observational sequence. Markov model is shown in Figure 1.

The Markov model is essentially a finite state automaton of a double random process. The underlying Markov chain cannot be directly observed but can only be obtained through the sequence of observations. When an initial, unoptimized Markov model is constructed, it is necessary to use the training algorithm of the Markov model to optimize the parameter values in the Markov model $\lambda = \{A, B, \pi\}$, so that the $p(o|\lambda)$ value can achieve the maximum value. The research object of Markov model is a data sequence, and each value of the sequence is called an observation value. Markov model thinks that there is another sequence hidden behind the sequence. This sequence represents a series of states, and each observed value occurs in a certain state. The changes of the observed value and state are stipulated by the probability model, but the state sequence cannot be observed, and it is hidden behind the observed value. Decoding is trying to find the hidden part of Markov model, that is, to find a correct state sequence. In practical applications, this kind of problem is usually solved only by finding the optimal sequence. At present, Markov model has been widely used in all walks of life. Markov model is widely used in intrusion detection field. Using the characteristics of Markov model, we can infer the probability of the next system call from the current system call. When the probability of the next system call is lower than the threshold, it means that there is an exception. When several consecutive system calls are abnormal, it is judged that an intrusion has occurred.

3.3. Construction of Early Warning Mechanism of Educational Network in Institution of Higher Learning. Attackers use different attack methods to achieve their attack intentions, but their attack intentions are often concealed, and the attack intentions are hidden in various complex attacks. The current intrusion detection system can only generate different alarm information for various attacks, but the attacker's attack intention is often submerged in a large amount of alarm information. In this chapter, aiming at the current security risks of college education network, we construct the early warning mechanism model of college education network based on Markov model. When constructing the Markov model, the training of the Markov model can build a feature library with high detection rate without a large number of data sets. If the data mining algorithm is used to build the model, a large amount of data is needed, so the use of Markov model greatly speeds up the modeling speed. In a computer, a system call refers to a program asking the operating system kernel for a service that needs higher authority to run. System call provides the interface between application and operating system. The early warning mechanism of college education network based on Markov model proposed in this paper is different from other early warning mechanisms. It is shown in the following aspects: (1) The detection effect is better and the abnormal detection rate is improved. (2) The contour database is reduced and the storage space of the system is saved. (3) The convergence speed is fast. (4) The accuracy of early warning is higher. (5) It is real-time. The process of model training and attack detection is shown in Figure 2.

Compound attacks frequently consist of several distinct attack steps, each of which is reflected by the corresponding alarm information. Each attack step in a compound attack depends on the output of the previous attack step. The relationship between attack steps and between attack steps and alarm information can be well described by a Markov model. The primary function of Internet Control Message Protocol, a member of the TCP/IP family, is to provide error reporting. Its specific use cases include testing connectivity and speed between routers, between hosts and routes, and between hosts. The ICMP report information is accessible if the router is taking too long to respond or the target host cannot be reached. The data processing module, data training module, intrusion detection module, and early warning module make up the majority of the model. The intrusion detection module is the heart of the model. The

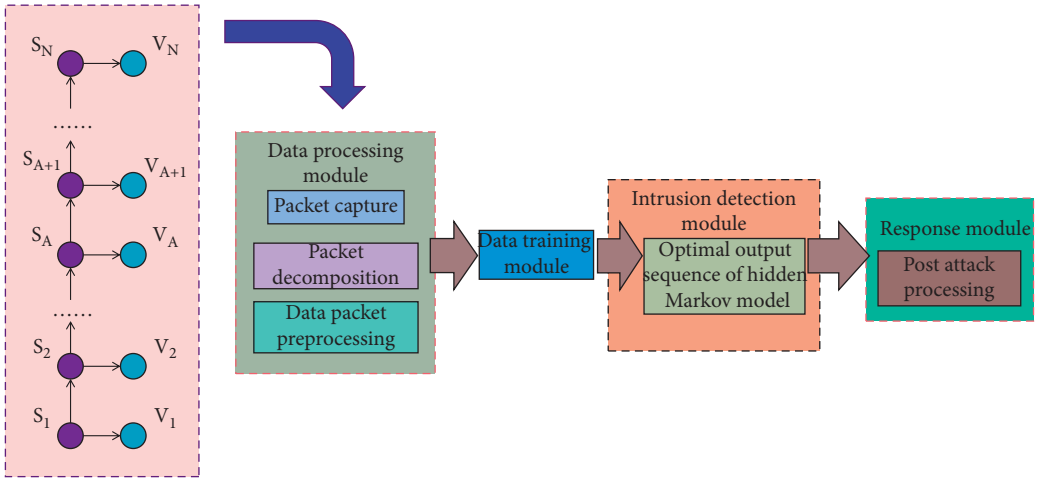

Figure 1: Markov model.

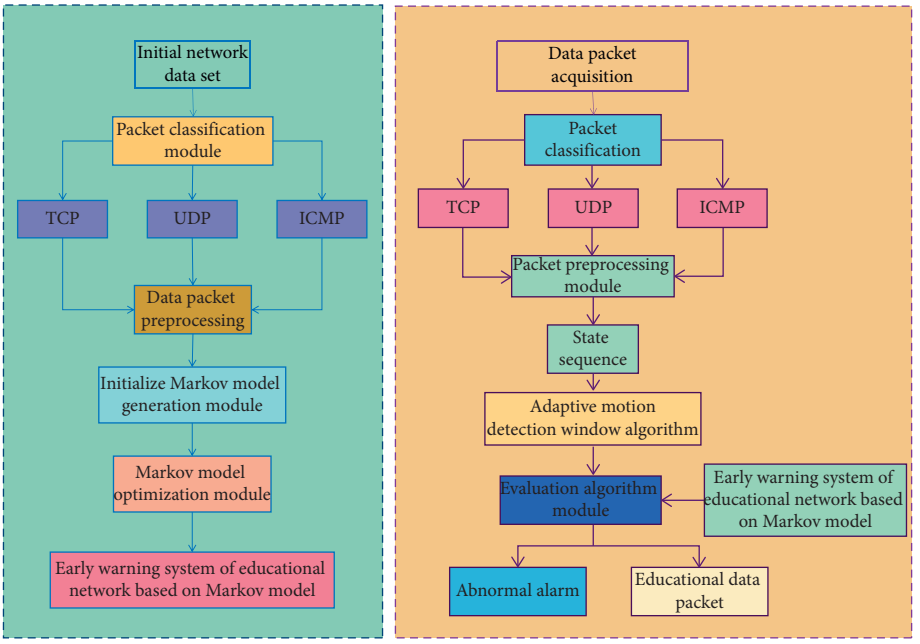

Figure 2: Model training and attack detection process.

observation layer is the top layer of a Markov warning model. The observation sequence is based on the alarm information in each attack intention, which allows the observer to infer the attack intention and, at the same time, predict the attacker's next move. The hidden layer, which contains the abstract attack intentions for each attack step of compound attacks and makes up the second layer of the Markov warning model. We can compare the model's local optimal probability, which was obtained by training a Markov model, to assess its accuracy. This means that starting from the point where the implicit state number is set as the distinct system call number, the local optimal probability determined by the experiment will go through a process of first increasing and then decreasing, and the implicit state number when the local optimal probability is the largest is the best, i.e., the variety of programme states. To solve the parameter estimation problem of Markov model, an observation sequence is given:

$$O = \{O_1, O_2, O_3, \ldots, O_T\}. \tag{1}$$

The Baum-Welch algorithm can determine $\lambda = \{p, A, B\}$ that maximizes $P(O|\lambda)$ definition:

$$\xi_t(i, j) = P\left(O, q_t = \theta_i, q_{t+1} = \theta_j | \lambda\right). \tag{2}$$

It is deduced that

$$\xi_t(i, j) = \frac{\left[a_t(i) a_{ij} b_j(O_{t+1}) \beta_{t+1}(j)\right]}{P(O|\lambda)}. \tag{3}$$

Then, the probability that the t Markov chain is in the θ_i state at the moment can be expressed as

$$\begin{aligned}\theta_i \xi_t(i) &= P(O, q_t = \theta_i|\lambda),\\ &= \sum_{j=1}^{N} \xi_t(i,j),\\ &= \frac{a_t(i)\beta_t(i)}{P(O|\lambda)}.\end{aligned} \tag{4}$$

Thus, if $\sum_{t=1}^{T-1}\xi_t(i)$ represents the expected number of transitions from the θ_i state, $\sum_{t=1}^{T-1}\xi_t(i,j)$ represents the expected number of transitions from the θ_i state to the θ_j state. The revaluation formula in the Baum-Welch algorithm can be derived:

$$\begin{aligned}\overline{\pi}_i &= \xi_1(i),\\ \overline{a}_{ij} &= \frac{\sum_{t=1}^{T-1}\xi_t(i,j)}{\sum_{t=1}^{T-1}\xi_t(i)},\\ \overline{b}_{jk} &= \frac{\sum_{t=1,O_t=V_K}^{T-1}\xi_t(i)}{\sum_{t=1}^{T}\xi_t(i)}.\end{aligned} \tag{5}$$

The calculation process is repeated, and the parameters of the model are gradually improved until $P(O|\overline{\lambda})$ converges. At this time, $\overline{\lambda}$ is the required model. Assume that the risk value of a node with a correlation relationship with node k at time t is denoted as

$$r_{k_l}(t,j) \quad 1 \le l \le m\, 1 \le j \le n. \tag{6}$$

The risk impact value of the node k with the correlation relationship on the node is recorded as

$$\Delta r_{k_l}(t,j) \quad 1 \le l \le m\, 1 \le j \le n. \tag{7}$$

It can be calculated by the quantitative value of correlation and the risk value of related nodes. The specific calculation formula is as follows:

$$\Delta r_{k_l}(t,j) = W_{k_{l,k} r_{k_l}}(t,j). \tag{8}$$

The indirect risk of node k is brought about by the special access relationship between nodes. Therefore, the value of indirect risk can be obtained through the superposition of risk impact values, namely:

$$\begin{aligned}IR_k(t,j) &= \sum_{l=1}^{M} \Delta r_{k_l}(t,j),\\ &= \sum_{l=1}^{M} \left\{ W_{k_{l,k} r_{k_l}}(t,j) \right\}.\end{aligned} \tag{9}$$

The creation of the feature database for the intrusion detection model is crucial because it affects the detection rate of the entire detection model. In the process of intrusion detection, it is necessary to compare the feature information in the current network packet with the information in the feature database. Whether the attack is successful or unsuccessful, the intrusion detection system's alarm information reveals the attacker's attack capability and system knowledge from one side, which creates a foundation for further determining the attacker's attack intention. In this study, the Markov model is trained using the data processed by the data processing module, and the trained model is then applied to the detection of intrusion and abnormal behavior. Different node positions in the network have different effects on the network's overall risk in the real-world network environment. Obviously, a core node attack has a bigger impact on network security than an edge node attack. Process behavior is the monitored object in anomaly detection based on system call. Even though the process behaves in a series of system calls, system calls are typically how the intrusion intention is carried out. The associated program's functionality, on the other hand, is fundamentally what defines the process behavior. The change model of the network packet protocol flag bit is established under typical network conditions in order to construct a network early warning model with strong real-time performance and high detection rate. This model can describe the characteristics of the network under normal conditions in detail, and all behaviors that violate the current detection model are considered as network attacks. Because the detection model is based on anomaly, it has a high detection rate.

4. Result Analysis and Discussion

In the process of prototype system realization, the key modules are compound attack scene judgment, attack intention recognition, and attack prediction, among which the compound attack Markov model is involved. In order to verify the theoretical conception of this paper, several groups of experiments are designed in this chapter. The experiment is carried out according to the preset number of hidden states. The validity of the early warning mechanism model of college education network is verified by experiments, and the validity of the model is measured by the detection rate of network attacks in the experiments. The host hardware environment used in the experiment is a PC with good performance. The alarm information table in this model mainly stores the basic data of alarm information. The fields and meanings contained in the alarm table are shown in Table 1.

Observe the changing trend of the local optimal probability of the final model under different state numbers to prove the hypothesis proposed in this paper. In this group of experiments, the initialization of the matrix is random, and the corresponding training time is recorded. Figure 3 shows the model training results over time.

During the experiment, the function of adaptive sliding detection window is turned off at first, and the fixed sliding window is used for detection. In the experiment, the sliding window size will be 1–30 for network attack detection test. In order to objectively show the influence of different time windows on the detection rate, different time windows will be tested several times in the experiment. Experiments show that the detection rates of network attacks with different sliding window sizes are shown in Figure 4.

It can be seen that the larger the sliding window, the higher the detection rate. This is because the larger the

Table 1: The fields and meanings of the alarm information table.

Field	Description of corresponding field
MessageClassID	Message type
AlertID	Alarm information sign
ResponsePriority	Response priority level
Time-stamp	Time stamp
CreateTime	Generation time of alarm information
EndTime	End time of alarm information
Classification	Attack category
SourceIP	Source host address
SourcePort	Source port number
TargetIP	Destination host address
TargetPort	Destination port number

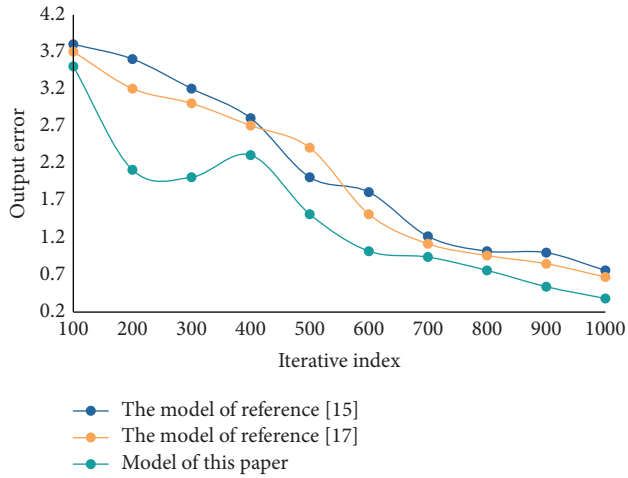

Figure 3: Model training results.

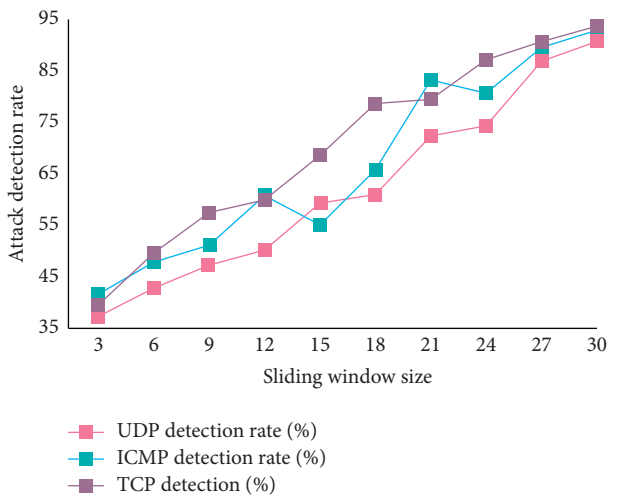

Figure 4: Detection rate of network attacks with different sliding window sizes.

sliding window, the lower the conditional entropy of the sequence to be detected in the sliding window. The decrease of the conditional entropy indicates that the uncertainty of the sequence to be detected in the sliding window is smaller, and the sequence with small uncertainty is convenient for Markov model to process. The early warning model assumes that the future evolution of the system has nothing to do with the past in the known state of the system. Attack is the exploitation of vulnerabilities, the system is fixed under certain conditions, and the attack process is the transition process among a limited number of states, which is stable for the whole attack process. As the computational complexity is linearly related to the sliding window size, the computational complexity increases with the increase of the sliding window length, so the sliding window length must have a suitable value space. Figure 5 shows the detection rate when the adaptive sliding detection window function is enabled.

It can be seen that the detection rate can be kept at a high level when the adaptive sliding detection window function is enabled. It not only ensures that the intrusion detection system has a high detection rate, but also ensures the real-time performance of the detection system. The experiment calculates the local optimal probability of the model obtained by training under a given number of hidden states. The greater the local probability, the more accurate the model. The smaller the local probability, the lower the accuracy of the model. Table 2 shows the local optimal probability value when the observation length is 40.

When an attacker attacks a network, he can use different attack methods to achieve the same attack intention, and each different attack method will trigger the intrusion detection system to generate different alarm information. Different alarm information may correspond to the same attack state and attack intention, and these alarm information sets corresponding to the same attack intention are called the observed values of the model. Figure 6 shows the detection rate of the early warning model in the actual network environment.

As can be seen from Figure 6, the attack detection rate of this model keeps above 90%, which can meet the needs of daily network attack detection. The execution state of the program is invisible, but people can observe the system calls associated with a certain state. It can be seen that the behavior process has the characteristics of Markov process. Anomaly detection based on system call attempts to establish a normal model of process behavior through the observed system call sequence and then infer the possibility that the current system call sequence comes from this model. The accuracy of the educational network early warning mechanism in this paper is shown in Figure 7.

In order to verify the reliability and practicability of the educational network early warning mechanism in this paper, this chapter compares this mechanism with other early warning mechanisms. The experimental results show that the accuracy of the educational network early warning mechanism in this paper is as high as 95.02%, which is higher than that of the traditional early warning mechanism of 9.87%. In this paper, Markov model is applied to the early warning mechanism of college education network, and good results have been achieved.

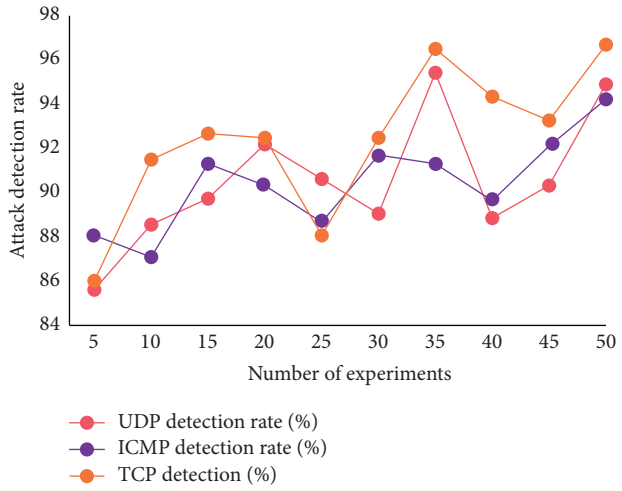

Figure 5: Detection rate when the adaptive sliding detection window function is enabled.

Table 2: Local optimal probability value when the observation length is 40.

Number of experiments	Local optimal probability value
1	78.46
2	77.98
3	79.61
4	78.15
5	78.94
6	79.21
7	80.35
8	81.23

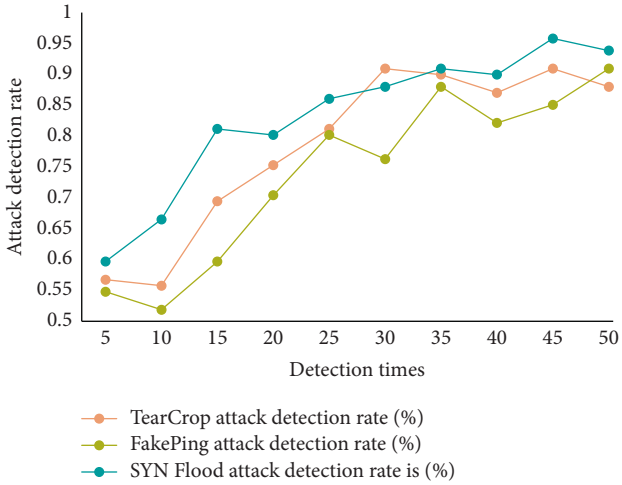

Figure 6: Detection rate of early warning model in actual network environment.

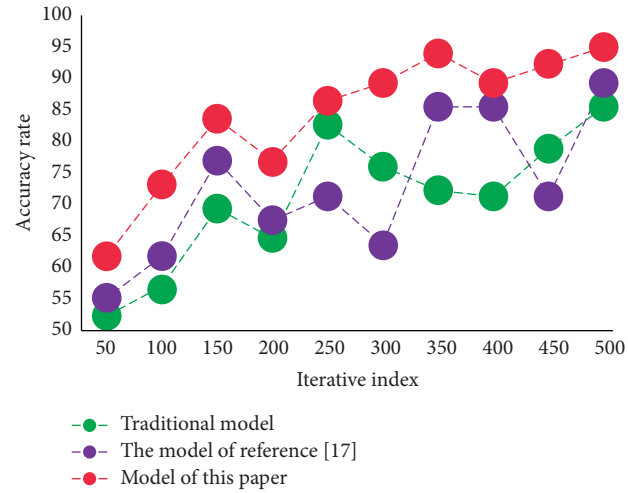

Figure 7: Comparison of the accuracy of the early warning mechanism of education network.

5. Conclusions

Construction on campuses and the growth of teaching initiatives are both key factors in how smoothly the educational network system operates in institutions of higher learning. This study suggests a Markov model-based early warning mechanism for the college education network in an effort to address the current security risks of the network. The model takes into account both the possibility of network attack and the vulnerability of a single machine. The attack behaviors, potential routes, and security state changes brought about by attackers invading the network are identified, and the potential threat's location is assessed using the generated attack state diagram and the original risk value. In addition, both the direct and indirect risks brought on by correlation are used to measure the nodes' security risks. The overall security risks of the target network are quantified after taking into account the significance of each node in the network and combining this information with each node's security risks. The initial parameter matrix of the model is constrained in this paper before training, which also increases the training time efficiency. Furthermore, compared to the traditional early warning mechanism's accuracy of 9.87 percent, the experimental results demonstrate that the educational network early warning mechanism in this paper has an accuracy of up to 95.02 percent. The early warning system of the college education network is applied to the Markov model in this paper, and positive outcomes are obtained. For the study of early warning systems in the college education network, it has a certain reference value. Although this research has certain

value and achievements, there are still some shortcomings. This paper only does a little work on the application of Markov model in anomaly detection. This is far from enough for the application of anomaly detection in practice. In the future, more research work is needed to achieve this goal.

Data Availability

The data used to support the findings of this study are available from the author upon request.

Conflicts of Interest

The author does not have any possible conflicts of interest.

References

[1] K. Salah, J. A. Calero, and S. Zeadally, "Using cloud computing to implement a security overlay network," *IEEE Security & Privacy*, vol. 11, no. 1, pp. 44–53, 2013.

[2] A. Arghavani, M. Arghavani, M. Ahmadi, and P. Crane, "Attacker-Manager Game Tree (AMGT): a new framework for visualizing and analysing the interactions between attacker and network security manager," *Computer Networks*, vol. 133, no. 1, pp. 42–58, 2018.

[3] M. Pathmika and F. Khan, "Dynamic process fault detection and diagnosis based on a combined approach of hidden Markov and Bayesian network model," *Chemical Engineering Science*, vol. 201, pp. 82–96, 2019.

[4] Y. Yao and Y. Cao, "A Neural network enhanced hidden Markov model for tourism demand forecasting," *Applied Soft Computing*, vol. 94, Article ID 106465, 2020.

[5] S. Wang and L. Zhu, "A Markov game model of network security in information system based on copula theory," *Boletin Tecnico/Technical Bulletin*, vol. 55, no. 12, pp. 227–232, 2017.

[6] F. Al-Ayed, C. Hu, and H. Liu, "An efficient practice of privacy implementation: kerberos and Markov chain to secure file transfer sessions[J]," *International Journal on Network Security*, vol. 20, no. 4, pp. 655–663, 2018.

[7] M. Korczynski, A. Hamieh, J. H. Huh, H. Holm, S. R. Rajagopalan, and N. H. Fefferman, "Hive oversight for network intrusion early warning using DIAMoND: a bee-inspired method for fully distributed cyber defense," *IEEE Communications Magazine*, vol. 54, no. 6, pp. 60–67, 2016.

[8] V. Y. Guleva, "The combination of topology and nodes' states dynamics as an early-warning signal of critical transition in a banking network model," *Procedia Computer Science*, vol. 80, pp. 1755–1764, 2016.

[9] B. Alomair and R. Poovendran, "Efficient authentication for mobile and pervasive computing," *IEEE Transactions on Mobile Computing*, vol. 13, no. 3, pp. 469–481, 2014.

[10] L. You, H. Jiang, J. Hu et al., "GPU-accelerated Faster Mean Shift with euclidean distance metrics," *Arxiv*, vol. 2112, 2021.

[11] J. Granjal, E. Monteiro, and J. S. Silva, "Network-layer security for the Internet of things using TinyOS and BLIP," *International Journal of Communication Systems*, vol. 27, no. 10, pp. 1938–1963, 2014.

[12] C. Daniel-Ioan, "Wireless sensor network security enhancement using directional antennas: state of the art and research challenges[J]," *Sensors*, vol. 16, no. 4, p. 488, 2016.

[13] K. Mekki, A. Zouinkhi, and M. N. Abdelkrim, "Fault-tolerant and QoS based network layer for security management," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 11, no. 2, pp. 363–372, 2013.

[14] E. A. Beck, "How zero-trust network security can enable recovery from cyberattacks[J]," *ISACA journal*, vol. 6, pp. 14–18, 2014.

[15] S. Einy, C. Oz, and Y. D. Navaei, "The anomaly- and signature-based IDS for network security using hybrid inference systems," *Mathematical Problems in Engineering*, vol. 2021, no. 9, pp. 1–10, 2021.

[16] Y. Liu, J. Wang, and H. He, "Identifying important nodes affecting network security in complex networks," *International Journal of Distributed Sensor Networks*, vol. 17, no. 2, pp. 1560–1571, 2021.

[17] W. Wu, "Ship communication network intrusion signal identification based on hidden markov model," *Journal of Coastal Research*, vol. 83, no. 1, pp. 868–871, 2019.

[18] L. Carnimeo, D. Foti, and S. Ivorra, "On modeling an innovative monitoring network for protecting and managing cultural heritage from risk events," *Key Engineering Materials*, vol. 628, pp. 243–249, 2014.

[19] F. Cheng, Y. Huang, B. Tanpure, P. Sawalani, L. Cheng, and C. Liu, "Cost-aware job scheduling for cloud instances using deep reinforcement learning," *Cluster Computing*, vol. 25, no. 1, pp. 619–631, 2022.

[20] J. Li, Z. Chen, L. Cheng, and X. Liu, "Energy data generation with wasserstein deep convolutional generative adversarial networks," *Energy*, vol. 257, Article ID 124694, 2022.

[21] S. M. Mirmohseni, C. Tang, and A. Javadpour, "Using markov learning utilization model for resource allocation in cloud of thing network[J]," *Wireless Personal Communications*, vol. 115, no. 1, pp. 1–25, 2020.