Research on the Application of Computer Network Technology Under the Background of Artificial Intelligence Cloud Technology

Qingwei Meng*

applied Technology College of Dalian Ocean University, Dalian 116300, China

*Corresponding author: mengqingwei@dlou.edu.cn

Abstract. On the basis of timely processing of network situation information, effective responses to network attacks with dynamic evolution characteristics are the main problems faced by cyberspace security defines mechanisms. The application of artificial intelligence technology can strengthen the intelligent characteristics of this system. This article mainly starts with the related concepts of artificial intelligence technology and cyberspace defines, and explores the application measures and development trends of this technology in cyberspace security defines.

1. Introduction

Artificial intelligence is a frontier issue in the field of computer science. The continuous development of science and technology provides a certain basic guarantee for the application of this technology in people's production and life. Regarding the definition of artificial intelligence, there are still some controversies in academia. Through the analysis of the research status of this issue, it is found that the academic circles strictly distinguish between "strong artificial intelligence" and "weak artificial intelligence". Among them, weak artificial intelligence is defined by scholars as machine learning algorithms based on mathematical techniques. In the application process of this algorithm, the programmer first needs to predict the possible situations in the application process, and then use the computer to determine the feasibility of the solution. Strong artificial intelligence has strict requirements on the thinking characteristics of programs. It requires a computer program to make autonomous decisions based on a correct understanding of external things, and make certain instructions and operations like a human. The computer network has obvious openness, so the virus can spread at a very fast speed, and it is easy to cause very serious economic losses to users or even paralyze the entire network system. Data mining technology is mainly to extract unknown data from large, noisy, and crowded spaces. These data are all useful potential information. Traditional data mining technology has certain limitations. With the rapid development of Internet technology, the network data mining technology produced by combining traditional data mining with the Internet has been widely used in computer virus defines systems to improve the security of computer networks and ensure stable operation of computer networks [1].
2. Related concepts of cyberspace define

2.1. Cyberspace
Cyberspace is a global domain in the information environment, that is, the space formed by the interconnection of information technology infrastructures, which include the Internet, communication networks, computer systems, and embedded processors and controllers. From the perspective of agents in the artificial intelligence discipline, cyberspace is the environment where all forces in cyberspace operations are located. Compared with the traditional environmental concepts in artificial intelligence, cyberspace has its own unique characteristics, including the part of the environment. Perceptual, dynamic, discrete, extremely complex and intensely confrontational. The cyberspace is extremely antagonistic. Both the enemy and the enemy coexist in the cyberspace. They not only have to face intelligent offensive and defensive technology, but also face traditional threats from firewalls, intrusion detection systems, and intrusion prevention systems [2].

2.2. Offensive cyber operations
Offensive cyber operations are military operations and activities such as computer network attacks (CNA) and computer network spying (CNE) against enemy information systems and networks in the field of cyberspace. CNA is a malicious behaviour directed at computer system or network data, software, or hardware. This behaviour has the characteristics of destructiveness, disruptiveness, degradability, and denial of access. CNE refers to the act of collecting intelligence, which invades the computer system in a covert way to obtain the required data.

2.3. Cyber defines
Computer Network Défense (CND) refers to measures to protect information, computers, and networks from being disrupted or destroyed. The main actions include monitoring, detecting and responding to illegally authorized computer actions. Commonly used technologies include passive information protection, active deception, and network Space conflict avoidance technology and intrusion detection technology, etc.

3. Intrusion detection methods

3.1. Methods based on statistical analysis
The anomaly detector first observes the behaviour of the target, and then generates a frame from it. This framework does not require too much space for storage and can be updated efficiently and regularly. With the continuous update of statistical data, the system periodically generates a data to represent its abnormality. This value is a function of the sub-abnormalities generated by some independent methods, which are obtained by the system according to user behaviour. There are usually the following detection methods:

3.1.1. Activity Intensity Measure. This method detects sudden abnormalities in behavioural activities, especially those that are more frequent than normal. It will not bring great anomalies to the long-term average, but it will be found in the short-term, such as frequent visits within one minute.

3.1.2. Audit Record Distribution Measures. This method detects the distribution of activity types, and can find anomalies in the short-term behaviour type distribution for specific users. For example, a large number of accesses to a file in a short period of time, or high-frequency I/O operations [3].

3.1.3. Categorical Measures. This method detects anomalies in the distribution of all activities of the entire system. For example, the number of logins in a certain place, the total number of email visits.

3.1.4. Ordinal Measures. This method detects anomalies in which the output result is a number, such as the number of CPU utilization I/O operations. The most recent user behaviour data is recorded and
compared and summarized with the previous data every other cycle. Abnormal behaviour is obtained through this comparison.

3.2. Method based on matching

3.2.1. Simple pattern matching. It encodes known intrusion characteristics into a pattern consistent with audit records. This mode cannot conflict with other modes, and at the same time it must be able to identify its variants. When a new audit event is generated, this method will search for a known intrusion pattern that matches it; when the audited event matches a known intrusion event pattern, it is called an alarm. Patterns can be added or deleted at will without affecting existing pattern matching. At the same time, there is no need to establish any dependencies. At present, pattern matching based on feature description is widely used. This method has a high accuracy rate of prediction and detection, but it is powerless for intrusions and attacks without experience knowledge. Simple pattern matching may lose the sequence of intrusion behaviour [4].

3.2.2. Graphics-based intrusion detection system. The system can construct a graph of the hosts it detects and the activities of the hosts. Take a worm invasion as an example, as shown in Figure 1. The worm first starts from host A, and then it attacks hosts B and C. The establishment of these two links is reported to Grids, and Grids records these two links in the form of graphs. If there is no movement of hosts A, B, and C for a long time in the following period, then this picture will automatically disappear. If the worm spreads to D, E and other hosts soon, then this link will also be recorded in the structure map. A series of parameters such as the generation time of these links will be recorded. If the timestamp shows that these links are very close in time, then they are more likely to be intrusions. Such a picture is stored in the database. When such a picture appears again, it may be considered a worm. Other attacks are also defined as a picture and the corresponding parameters on the picture. In addition to time, other information such as target address and port is also used in the representation of other types of intrusions. Both the attributes of graph nodes and edges can be used to represent specific information. The characteristic structure of the intrusion behaviour graph becomes the condition of judgment at this time.

![Characteristic diagram of worm attack](image)

**Figure 1.** Characteristic diagram of worm attack

4. Basic characteristics of Agent technology

Software Agent technology has become a hot topic and active field of artificial intelligence research in the 1990s. Its main background is the popularization and application of the Internet; people urgently require software that is integrated on heterogeneous hardware and software platforms and is semantically incompatible. Improve their reusability. At present, there is no unified definition of Agent. Generally speaking, Agent is a software entity that can actively execute and automatically process information. After summarizing the opinions of many scholars: Wooldridge and Jennings proposed to It is regarded as a software system with the following basic characteristics: Autonomy: refers to the
ability to operate on its own without the intervention of humans and other software systems, and has certain control over its own actions and internal state. Social ability: refers to the ability to interact with other software agents and people through a certain agent communication language, also called communication ability. Responsiveness: refers to the ability to perceive the environment, such as the physical world, users using graphical interactive interfaces, other agents, networks, and combinations of these factors, and can respond to changes in the environment in time. Proactiveness: The ability to demonstrate targeted behaviour through active initiatives, rather than simply adapting to the environment. Software Agents should satisfy the above-mentioned basic characteristics. They are software entities controlled by themselves and executed concurrently. They can save the current environment and user status and knowledge, and can communicate with each other, so they are a natural extension of object-oriented technology [5].

From the perspective of the characteristics of distributed network attacks, the use of automated means to attack network service systems has become a new feature of distributed attacks. The construction of an agent network security system based on FIPAOS technology can judge distributed network attacks in a coordinated manner based on deploying agents in different network environments. The application of the DECIDE project has enabled agent technology to be applied in the cyberspace security exercise platform.

5. Target detection and recognition technology

Target detection and recognition refers to finding a target from a scene (picture), including two processes: detection (where) and recognition (what). The difficulty of the task lies in the extraction and identification of candidates for the area to be detected, so the general framework of the task is: first establish a model for extracting candidate areas from the scene, then identify the classification model of the candidate area, and finally fine-tune the parameters of the classification model and the effective candidate frame. The location is refined [6].

At present, target detection and recognition technologies are mainly divided into two categories: one is target detection and recognition algorithms based on traditional image processing and machine learning algorithms, and the other is target detection and recognition algorithms based on deep learning. Based on traditional image processing and machine learning algorithms for target detection and recognition algorithms, target detection and recognition methods can be mainly expressed as: target feature extraction → target recognition → target positioning. The features used here are all artificially designed, such as SIFT (Scale Invariant Feature Transform), HOG (Histogram of Oriented Gradient), SURF (Speeded Up Robust Features), etc. Identify the target through these characteristics, and then locate the target in combination with corresponding strategies. The main focus of the video image content security technology is the target detection and recognition algorithm based on region recommendations, such as R-CNN, Fast-R-CNN and Faster-R-CNN. The basic workflow of R-CNN is shown in Figure 2, and the specific description is as follows:

![Figure 2. Schematic diagram of R-CNN algorithm principle](image-url)
(1) Receive an image and use Selective Search to select about 2000 candidate regions that are irrelevant from top to bottom (proposal); (2) Convert the extracted candidate regions into a uniform size picture (zoom/compression, etc.), use the CNN model to extract the fixed-length features of each candidate region; (3) Use a specific class of linear SVM classifier to classify each candidate region; (4) Bounding Box regression.

6. Feature extraction technology

Before statistical feature analysis was used in face recognition, the automatic face recognition system ignored what kind of facial features played the most important role in face recognition, and only assumed some pre-set people. The measurement of face parts and the measurement of the relationship between the parts are effective and sufficient to reflect the differences between different faces. This assumption is obviously unreasonable. But it gives us an important enlightenment: the human face can be encoded and decoded from the perspective of information theory, so as to emphasize some important global and local features. The features extracted by this method may be different from the usual intuitive features. Principal component analysis is used for face recognition mainly from two aspects: First, from the perspective of information theory, we need to extract as much relevant information of the face image as possible from the face image, and then combine this information with the face in the face database Comparing the information, the face recognition is completed. Second, from a mathematical point of view, we hope to find the main features of the face distribution, that is, the feature vector of a set of face image correlation matrix. This set of feature vectors can be seen as Cheng captures the characteristics of face image changes. In this method, each face image can be accurately represented by the linear operation of the feature vector. The number of feature vectors is equal to the number of face images participating in the training. You can also choose some eigenvectors with the largest eigenvalues to approximate the representation [7].

Given an n dimensional random vector \( x \), it can be expanded into a linear combination of \( n \) wiki vectors \( (\varphi_1, \varphi_2, \cdots, \varphi_n) \)

\[
x = \sum_{i=1}^{n} \alpha_i \varphi_i = \Phi \alpha
\]  

(1)

In the formula, \( \alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n) \) is the random coefficient vector. \( \Phi \) is \( n \times n \) a matrix of dimensions, namely

\[
\Phi = (\varphi_1, \varphi_2, \cdots, \varphi_n)
\]

(2)

Here, \( \Phi \) actually defines a linear transformation from \( x \) to \( \alpha \). K-T transformation requires that the components in the transformed random coefficient vector \( \alpha \) are mutually orthogonal, so that the specific form of \( \Phi \) can be determined.

Thus, if the autocorrelation matrix \( R \) of \( x \) is known, then there is

\[
R = xx^T = \Phi \alpha \alpha^T = \Phi \alpha \alpha^T \Phi^T = \Phi D \Phi^T
\]

(3)

If \( \Phi \) is further required to be a normalized orthogonal matrix, namely

\[
\Phi^T \Phi = I
\]

(4)

Where \( I \) is the unit matrix, we can get

\[
R \Phi = \Phi D \Phi
\]

(5)
This is the characteristic equation of $R$, with

$$R \varphi_i = \lambda_i \varphi_i \quad (6)$$

Among them, $\lambda_i$ is an eigenvalue of $R$, and $\varphi_i$ is the eigenvector corresponding to $\lambda_i$. Therefore, the transformation matrix $\Phi$ can be formed by the eigenvectors of the autocorrelation matrix $R$ of $x$. Since $H$ is a real symmetric and non-negative definite matrix, it can meet the above requirements for $\Phi$, and all its eigenvalues are non-negative.

7. Conclusion

The construction of cyberspace security defines system is an important measure to ensure the consistency, credibility and availability of information resources in computer systems. The complexity of information systems and the diversity of network security threat factors are the main problems faced in the development of computer technology. Adaptability and multi-modality are the main characteristics of the cyberspace security defines system based on artificial intelligence technology. With the continuous development of computer technology and artificial intelligence technology, the effectiveness of this technology in the development of cyberspace security defines work will be more fully displayed.

References

[1] Diego Inácio Patríciaa, & Riederb, R. Computer vision and artificial intelligence in precision agriculture for grain crops: a systematic review. Computers and Electronics in Agriculture, 15(3) (2018) 69-81.

[2] Song, H., Bai, J., Yi, Y., Wu, J., & Liu, L. Artificial intelligence enabled internet of things: network architecture and spectrum access. IEEE Computational Intelligence Magazine, 15(1) (2020) 44-51.

[3] Zhao, Q., & Zhang, Y. Ensemble method of feature selection and reverse construction of gene logical network based on information entropy. International Journal of Pattern Recognition and Artificial Intelligence, 34(2) (2020) 487-500.

[4] Jian, G., & Mengfei, Y. Evolutionary fault tolerance method based on virtual reconfigurable circuit with neural network architecture. IEEE transactions on evolutionary computation, 22(6) (2018)949-960.

[5] Liu, Z., Zheng, Q., Ji, Z., & Zhao, W. Sparse self-represented network map: a fast representative-based clustering method for large dataset and data stream. Engineering Applications of Artificial Intelligence, 68(2) (2018) 121-130.

[6] Yang, Y. J., & Bang, C. S. Application of artificial intelligence in gastroenterology. World Journal of Gastroenterology, 25(4) (2019) 31-48.

[7] Szczepanski, P. L., Michalak, T. P., & Rahwan, T. Efficient algorithms for game-theoretic betweenness centrality. Artificial Intelligence, 231(2) (2016) 39-63.