10.18686/frim.v2i5.4517

Research on Network Intrusion Detection Technology Based on Artificial Intelligence

Hongxia Yin, Zhang Li, Liyao Fu, Chen Tao

Shandong Vocational Animal Science and Veterinary College, Weifang, Shandong 261061

Abstract: As network intrusion becomes more and more complicated and network characteristics become more and more diverse, the traditional network intrusion detection technology has some problems such as high false alarm rate, poor adaptability and low detection rate. The article provides an in-depth analysis of network intrusion detection techniques based on artificial intelligence to better solve these problems. In recent years, we have been witnessing great progress in image recognition, speech recognition, and natural language processing. The powerful advantage of artificial intelligence in processing large-scale and complex data provides new ideas for the processing of multi-attribute intrusion data. The introduction of AI technology in network intrusion detection can effectively improve the detection accuracy and reduce the false alarm rate and omission rate. Based on this, the article analyses the artificial intelligence network intrusion detection technology and discusses the network security management based on artificial intelligence for the reference of related personnel.

Keywords: Artificial intelligence; Network intrusion detection; Technology research

Introduction

The increasing sophistication of network intrusion means makes it difficult for traditional machine learning methods to identify them effectively. Therefore, modern information technology should be introduced to improve the level of network intrusion detection technology. In recent years, with the rapid development of artificial intelligence technology, people process a large amount of data efficiently and use new methods to deal with multi-attribute intrusion data, providing key technical support for natural language processing, speech recognition, image recognition and so on. Therefore, the introduction of artificial intelligence into network intrusion detection can effectively improve the accuracy of detection.

1. Artificial Intelligence Based Network Intrusion Detection Techniques

1.1 Intrusion detection

Traditional network intrusion detection techniques usually use pre-determined detection rules. However, the method has some drawbacks, such as artificial rules, difficult to maintain, and difficult to cope with new attacks. However, AI-based network intrusion detection technique is a machine learning-based method, which has the advantages of high efficiency, accuracy, and adaptivity. Intrusion detection is the monitoring of data streams to determine whether there is an attack or not, in order to achieve real-time protection of the network. And the data streams are categorised for better analysis and processing. In recent years, methods such as Neural Networks, Support Vector Machines, and Decision Trees have become a new area of research. A classification modelling is proposed based on the analysis and study of historical data, which is used to model new data streams. By using artificial intelligence methods, intrusion activities are categorized and analyzed through methods such as cluster analysis and association rule mining, so as to achieve the purpose of analyzing and warning intrusion activities and improve the security of the defence system.

1.2 Network intrusion detection system

The computer automatic identification technology based on intelligent technology includes functions such as data acquisition, pre-processing, feature extraction, classifier and alarm. Specifically, in the pre-processing stage, the pre-processing of groupings is completed, a large number of duplicate groupings are removed, and irrelevant groupings are filtered. In the feature extraction part, the corresponding feature vectors is obtained by preprocessing the samples, which provide the basis for subsequent category learning and classification. The classifier identifies network anomalies and attacks by learning and classifying the feature vectors. The early warning module mainly generates warning messages by analysing the warning data, prompting the managers to take appropriate measures.

1.3 Artificial intelligence detection algorithms

The introduction of artificial intelligence techniques into the field of network intrusion detection, which is widely used in the field of data mining and machine learning. Data mining can help network administrators to understand network data and identify useful information in it. Machine learning (machine learning) is an intrusion detection technique based on network data. Currently, a neural network based intrusion detection technique is proposed to address the problems in intelligent networks. Among them, neural networks are computer models used to simulate the structure and function of biological nervous systems. The advantage of these two methods is that it enables adaptive learning and training for nonlinear problems. The decision tree method adopts a hierarchical structure, which can express the decision-making process graphically and is simple to understand. Support vector machine is a binary classification method based on statistical learning, which not only has strong generalisation ability, but also has strong robustness. For different applications and different data characteristics, different methods are used for identification. In the case of a small number of samples and significant characteristics, the decision tree method can be used; for the characteristics of large data size and complex characteristics, the improved methods of neural networks and support vector machines can be selected. In addition, multiple detection methods can be combined to improve the detection accuracy and robustness.

2. Artificial Intelligence based network security management

2.1 Discovering and handling abnormal events

Artificial neural network system is a class of intelligences with high recognition, which can accurately determine the intrusion behaviour and have good adaptability to attacks. Due to the strong learning ability of the artificial neural network system, it is able to rapidly classify the data and store it, thus improving the quality and efficiency of detection. Using fuzzy detection system to quickly locate the hidden viruses in the system and respond to the system, it can quickly find the potential viruses lurking in the system and respond to them accordingly, thus ensuring the safety of the network system. In case of an attack on the network system, different methods can be used to provide early warning. The network system includes a number of security devices, which are alerted by means of alarm lights, window alarm lights, etc., and the alarm data is automatically stored in a database.

2.2 Intelligent Detection of Data Traffic

Data traffic is determined by the volume, whether it is uploaded or downloaded, there are fluctuations in traffic. When the data volume is large, the communication volume will also be large. Artificial intelligence technology makes full use of the correlation between data traffic and volume to intelligently detect data traffic and add the corresponding security metrics. Viruses often lurk in the data, and users downloading data containing viruses can cause significant traffic loss. In the event that abnormal data flow is detected, the intelligent system will interrupt the data transmission and send a request to the database to retrieve the contents and compare the data to determine whether the downloaded data is safe or not. In the process of processing risk data, it is uploaded into a database by analysing the source, content and characteristics of the data. Some network terminals are open, so viruses do not need authorisation to connect to the network and engage in nefarious acts. Viruses can be detected through terminal devices such as mice, keyboards and touch devices, which are connected to the network and consume a lot of traffic.

2.3 Intelligent Isolation and Control

With predefined security countermeasures, AI is able to monitor the internal and external networks of the firewall. The artificial intelligence firewall, consists of three parts: authentication, state monitoring, and packet filtering. For example, packet filtering is designed to screen packets at the network layer, with reference to the working state of the system, and predefine filtering logic, thus enhancing the security of packet content. Email has become a widely used tool for information transfer, and intelligent firewalls are used to monitor emails, check the content of the information in the emails, and detect viruses. And once a possible virus is detected, it should be isolated and controlled in a timely manner to ensure the security of information on the network.

3. Conclusion

In summary, artificial intelligence has significant advantages and values, including the ability to autonomously analyse network intrusions, establish a diversified protection system, comprehensively identify network security risks, and isolate and control malicious intrusions. With the development of AI, the security of the network has been greatly improved, and unknown or known threats can be quickly discovered and dealt with. In the future development process, the intelligence degree of network intrusion detection technology will be further improved to achieve rapid identification and response to unknown and known threats, so as to better cope with potential network intrusion.

References

[1] Shen Sol. Design of computer network intrusion detection technology based on artificial intelligence technology[J]. Yangtze River Information and Communication, 2023, 36(05):127-129.

[2] Zhen Tao. Research on network intrusion detection technology based on artificial intelligence[J]. Information and Computer (Theoretical Edition), 2023, 35(07):237-239.

[3] Wang Xia. Research on network intrusion detection technology based on artificial intelligence[J]. Jiangxi Communication Science and Technology, 2022, (03):46-48+51.

[4] Jiang Yuting. Research on network intrusion detection technology based on artificial intelligence[J]. Information Communication, 2019, (12):70-72.

[5] Liu Yubiao. Application of artificial intelligence technology in computer network intrusion detection[J]. Science and technology wind, 2019, (32):94+97.