ISSN: 1813-4890

Research on Application of Artificial Intelligence Technology in Cyberspace Security Defense

Yukun Li

Guangdong University of Science and Technology, 523083, Dongguan, Guangdong, China

Abstract

With the rapid development of Internet technology, a variety of new applications and new technologies, network space environment increasingly complex, endless loopholes, threats, the scale and complexity of the attack surface is expanding, the traditional defense means is difficult to do comprehensive, entire network, full-time defense, artificial intelligence technology as a new technology industry, has been widely used in various fields, also to network space security provides a new defense ideas and means. By means of artificial intelligence related technologies, all aspects of chip, system hardware, physical environment, system software and other aspects, can be used to quickly generate defense countermeasures and provide more accurate decision-making basis for management.

Keywords

Artificial intelligence technology; cyberspace; security and defense

1. Introduction

Artificial intelligence technology is an important branch in the field of computer, which is called artificial intelligence technology because of its humanized processing ability[1], Its core technologies mainly include machine learning, natural language processing, computer vision, robotics, and biometric identification technology. Artificial intelligence technology should be widely applied in many industries due to its unique intelligent learning ability. The introduction of artificial intelligence technology in cyberspace defense can greatly enhance the security of cyberspace. Cyberspace security involves all kinds of communication systems, electronic devices, real-time data in cyberspace, namely, device layer security, system layer security, data layer security and application layer security. Among them, the security of equipment layer shall address the security problems of the information system itself in cyberspace, including physical security, environmental security and equipment security; system security, including data security, identity security in network space, and the security problems in the information application process, including content security and application security.

Current network space security defense technology mainly firewall technology, encryption technology, network security situation early warning, intrusion detection, network lure, security, etc., with the increasingly complex network space environment, the traditional static defense technology is far from meet the demand of defense, only to further improve the level of security defense, to the greatest extent to reduce the network security problems.

2. Advantages of Artificial Intelligence Technology in Handling Security Problems in Cyberspace

In the traditional cyberspace defense structure, the deployment of targets is mostly static, homogeneous and determined. Equipment or system maintains some fixed combination for a long time, and mostly have the same model, version or status, function and characteristics are relatively certain; single defense point, usually based on an attack point or part of the attack

ISSN: 1813-4890

point, with hysteresis, most of the experience-based, repair way; universal, for the software or hardware of the same vulnerabilities, basically in other entities, so vulnerabilities can be batch replication, once a device threatened, can quickly affect other devices in a short time. The cyberspace security and defense technology based on artificial intelligence technology can better solve the above problems, and its advantages are mainly reflected in four aspects:

1. More powerful nonlinear processing ability, can be better for network structure processing. At present, most of the cyberspace structure is a non-linear topological structure, which is much higher than the general linear network structure, which leads to the higher difficulty coefficient of cyberspace security defense system. For the traditional cyberspace security defense system, there are more vulnerabilities in the complex topological network structure, but fewer vulnerabilities can be found and take defensive measures, and the security degree of cyberspace is lower. Artificial intelligence technology performs well in handling non-linear structure. Using artificial intelligence technology to deal with complex network problems can maintain the time consumption of network environment security and reduce the time consumption of topological network computing, accelerate the response speed of the system to network intrusion, so as to maintain the security and stability of cyberspace[2]；

2. The processing of fuzzy information is more accurate. On the basis of accurate analysis of the existing and known information, it can make more accurate predictions of the unknown problems that have not yet appeared. For the cyberspace security defense system, the monitoring function of network intrusion information is the most difficult but the best in the defense test. Whenever network intrusion occurs in network space, the monitoring system timely discovers the intention of network intrusion, which can well realize the killing of network intrusion. However, the monitoring of network intrusion information has certain requirements for accuracy, which is embodied in the accuracy of information prediction by the security defense system, and the judgment of information circulation in the network space based on experience learning, so as to realize the accurate judgment of intrusion information[3]. Traditional cyberspace security defense monitoring technology is not perfect, affected by massive data processing and monitoring index is difficult, the traditional system in the monitoring and early warning function has not been a breakthrough, and artificial intelligence technology when processing of fuzzy information, can with the help of natural language processing technology, can deeply analyze to unknown fuzzy information, and then in artificial intelligence technology of data processing technology, the batch information packaging and computing operations, such as artificial intelligence security defense application scenarios;

3. Stronger collaboration ability, which can better cooperate with multiple and multi-level technologies used in cyberspace security, so as to achieve stronger security defense effect. Cyberspace in its structure is complex, the traditional network space security defense system, from hardware to software, from the system to the network, the model, function, configuration, long communication cycle between the equipment, system, once the network space is attacked, the system is difficult to coordinate organize effective countermeasures, this will lead to network space in a short period of time will bear large attacks, once beyond the threshold of security defense system, will bring to predict the adverse consequences of cyberspace. The management mode of artificial intelligence technology has the characteristics of hierarchy, can strengthen the cooperation ability between systems, when the cyberspace is invaded, can maximize the role of the entire security defense response in a short time, the sudden network invasion can be blocked and stopped in time;

4. The control algorithm can do a relatively fast, accurate and low-cost one-time calculation of the obtained information[4]。

ISSN: 1813-4890

3. Deficiency of Artificial Intelligence Technology in Dealing with Cyberspace Security Problems

Although artificial intelligence technology has many advantages in dealing with cyberspace security issues, there are also some deficiencies that cannot be ignored. First, AI technology relies on data quality, and high-quality data is often difficult to obtain, which affects the accuracy of threat detection. Second, integrating AI technology into an existing cybersecurity infrastructure can require a lot of time and resources, which can be a huge challenge for many organizations. Moreover, while AI technology can process large amounts of data and information, it has never able to replace human decisions or provide personalized advice. In addition, artificial intelligence technology is affected by many factors in dealing with the security problems in cyberspace. For example, the size of the neural network and the decision defined for filtering, and the number of iterations required to achieve the predefined error rate, such as a three-layer decision tree, each layer has multiple nodes for each decision path. Although the matrix is very simple, it also requires a lot of computation. Therefore, the limitation of the system resources may compromise the intelligence of the solution. In addition, the lack of available processing resources in the hardware also makes the AI statistical weighted matrix, once trained, usually not updated in the service, resulting in the existence of some vulnerabilities. To this end, a lot of resources need to be invested in training AI to cope with the emerging cyber threats.

Therefore, when using artificial intelligence technology, we need to fully consider its advantages and disadvantages, combined with other technical means to carry out comprehensive prevention, to ensure the security of cyberspace.

4. Typical Application of Artificial Intelligence Technology in Security Defense in Cyberspace

4.1. Smart firewall

Network threats emerge in an endless stream. In addition to viruses and Trojan horses in the traditional sense, the advanced persistent threats represented by APT are constantly evolving, showing the characteristics of diversified means, concealment and faster diffusion speed. Firewall based on artificial intelligence, introduced the intelligent detection engine, through massive sample training threat detection model, and can according to the real-time traffic data for continuous optimization, detection threat ability is stronger, can based on signature threat detection, support intelligent detection APT advanced unknown threat, have higher detection force, need to invest operations time shorter. This kind of firewall generally configuration AI chip, AI chips provide powerful computing power for intelligent firewall, AI chip also known as AI accelerator or computing card, is specialized in processing AI application a large number of matrix multiplication and addition module, mainly divided into GPU, FPGA, ASIC, etc., can meet the performance requirements of the massive data, fast and efficient huge amounts of data processing capacity is one of the advantages of intelligent firewall. AI engine provides flexible computing method for intelligent firewall. AI engine is a complex system, including the whole process of machine learning processing, such as data acquisition, data cleaning, feature analysis, feature analysis, feature extraction, model training, model verification, prediction, etc.; including machine learning algorithms such as supervised learning, unsupervised learning, semi-supervised learning, reinforcement learning; including data processing technologies such as traffic analysis, image processing, natural language processing, graph data processing; supporting baseline learning, classification, clustering, regression, and interactive learning scenarios. Therefore, the intelligent firewall integrated with the AI engine can effectively deal with the many security problems faced in the network.

ISSN: 1813-4890

4.2. Intelligent intrusion detection technology

Intrusion detection technology (IDS) is a network security technology that proactively protects the system from attacks. Can form a complementary and firewall, coordinated response to network attacks. Its principle is to determine that the system behavior is normal or abnormal according to the host generated data or network traffic data. The general process of machine learning is applied in network intrusion detection: first, use the public data set or use packet tools such as Wireshark and Snort to collect data and conduct data preprocessing; then extract intrusion features, such as packet serial number, sender, receiver IP address, protocol type, and then select the appropriate machine learning algorithm, such as ANN, SVM, decision tree, clustering algorithm, build the network intrusion detection classifier, identify the test data after training, and then determine whether its behavior is normal. At this stage, deep learning-based techniques have been widely used in IDS, showing some effectiveness in detecting intrusion behavior.

4.3. Spam mail detection technology

Although there are many types of spam, false information, phishing sites, Macau gambling, financial promotion, they have one thing in common, that is, they have nothing to do with the needs of the recipient. Traditional static rules can achieve partial filtering, but there are often misoperations, so it needs to be optimized in filtering technology and algorithm.

Artificial intelligence technology has a natural advantage in spam, such as can use circular neural network (RNN):one of the representatives of deep learning technology, through huge amounts of mail samples, training can accurately identify spam spam recognition model, using machine learning model to spam identification lies in the recognition of the new junk content judgment, so can have a stronger defense ability.

4.4. Application of neural networks

The increasingly complex network environment, Making the traditional defenses inadequate, It is difficult to form an active defense system for cyber security, Neural network is an intelligent artificial algorithm technology with adaptive, self-organization and self-learning ability, The network relies on the complexity of the system, By adjusting the interconnections between a large number of nodes within, To achieve the purpose of processing information, Its architecture is generally divided into three categories: feedforward network, feedback network, graph network, Neural networks due to their characteristic nonlinear adaptive information-processing capabilities, Perfect for the complex and changeable cyberspace environment, Together with the existing defenses, Change contingency is taken as an active defense, And then to build up a set of intelligent defense system.

4.5. Malware analysis, automated response

Artificial intelligence technology can provide effective identification and classification of malware by analyzing the code, behavior mode and transmission route of malware. This can help security experts identify and respond to new malware variants in time. Meanwhile, AI technology can automatically respond to security incidents, such as automatically isolating attacked systems and automatically generating emergency response plans. This can improve response speed and efficiency and reduce the risk due to human error or delay.

6. Data encryption and privacy protection, zero-trust security model

Artificial intelligence technology can be used to encrypt and decrypt data to protect users' privacy and security. This may include the application of advanced encryption algorithms, as well as dynamic encryption and decryption based on the user's behavior patterns and habits. The zero-trust security model is a security framework based on authentication and authorization, and artificial intelligence technology can be used to achieve more detailed

ISSN: 1813-4890

authentication and authorization control. For example, by analyzing the user's behavior patterns and identity characteristics, the user's permission level can be dynamically adjusted to achieve stricter security control.

7. Network security risk assessment and management

Artificial intelligence technology can provide a comprehensive assessment of the network security situation by analyzing the security situation and risks of the network system. This can help the security team to better understand the security situation of the network and take targeted defense measures.

5. Conclusion

Era of artificial intelligence, the construction of network space security defense, need to "wisdom", make full use of artificial intelligence technology automation and response to higher efficiency, self learning ability, build a more secure, more intelligent dynamic cyberspace defense system, and build a more harmonious cyberspace.

Acknowledgements

This paper is the phased outcome of 2022 Guangdong University of Science and Technology scientific research project: Research on the Application of Artificial Intelligence Technology in Cyberspace Security Defense, Project Number:GKY-2022KYYBK-20.

References

[1] Zhou Dongming. Application of artificial intelligence technology in cyberspace [J]. Computer Products and Circulation, 2019, (9): 56-57.

[2] Sun Shutong. Application of artificial intelligence technology in cyberspace [J]. Wireless Internet Technology, 2019,16 (23): 130-131.

[3] Zhao Binghua, Yang Guorui, Jia Zhe. An AI-based defense technology in cyberspace [J]. Computer and Networks, 2021,47 (12): 57-60.

[4] Feng Xin rain. Application of artificial intelligence technology in cyberspace [J]. Electronic Technology and Software Engineering, 2018, (15): 244.