Retraction

Retraction: Research on the Application of Network Security Defense Based on Artificial Intelligence (J. Phys.: Conf. Ser. 1992 022077)

Published 9 September 2022

This article has been retracted by IOP Publishing following an allegation that raises concerns this article may have been created, manipulated, and/or sold by a commercial entity. In addition, IOP Publishing has seen no evidence that reliable peer review was conducted on this article, despite the clear standards expected of and communicated to conference organisers.

The authors of the article have been given opportunity to present evidence that they were the original and genuine creators of the work, however at the time of publication of this notice, IOP Publishing has not received any response. IOP Publishing has analysed the article and agrees there are enough indicators to cause serious doubts over the legitimacy of the work and agree this article should be retracted. The authors are encouraged to contact IOP Publishing Limited if they have any comments on this retraction.

Retraction published: 9 September 2022
Research on the Application of Network Security Defense Based on Artificial Intelligence

Yukun Huang1,2,*
1Guangxi Vocational&Technical Institute of Industry, Guangxi, China, 530001
*Corresponding author e-mail: huangyukun@gxic.net

Abstract. With the continuous close relationship between the network and all aspects of people's life, the network security threats that people are facing are also gradually rising, such as the protection of personal privacy information, the protection of enterprise intellectual property rights and core technology, and other aspects are related to the research and utilization of network security defense. The utilization of artificial intelligence in network security defense can greatly improve the protection ability of network security, so it has high research value. Based on this, this paper first analyses the utilization process of artificial intelligence in network security research, and then studies the current situation of network security defense, as well as the specific utilization of network security defense based on artificial intelligence.

Keywords: Artificial Intelligence, Network Security Defense, Application

1. Introduction
With the iterative expansion of computer tech, the modern emerging tech represented by AI has made a significant technical breakthrough and has been widely and deeply applied in many fields. As people's work and life are more and more inseparable from the assistance and help of the Internet, the network security threats that people are facing are also gradually rising, such as the protection of personal privacy information, the protection of enterprise intellectual property rights and core tech, and the protection of national important security domain information, etc., all involve the research and utilization of network security defense. In this context, how to ensure network security under the condition of network information environment has become the focus of attention and research in various fields related to network utilization.

In recent years, with the increasing threat of network security defense, the remediation of network security environment has become more and more severe and urgent [1]. As an important support to ensure the stability and orderly operation of the network environment, network security has become a hot spot in the utilization of many modern technologies represented by AI. Based on the utilization of AI in network security defense, it can greatly improve the protection ability of network security, such as the release of network flexibility and security, and ensure the normal expansion of much utilization in many fields. At present, the real network security threats faced by all walks of life in China can not be ignored. Every year, the network security events will lead to significant losses. Therefore, the utilization of AI tech in network security defense has important practical value.
In addition, AI tech can achieve effective defense of network security through its system integration ability and powerful information analysis ability, and brings new opportunities to the expansion of network security defense, so that it can effectively deal with more and more complex network security threats [2]. In short, as a branch of computer science and tech, the utilization of AI in network security defense can play a great value in the protection of information in the network system. The utilization of AI tech in network security protection plays an important role in promoting network security and enhancing the level of network protection, so as to further enhance the level of network security defense.

2. Utilization of AI in network security research

2.1. Utilization process of AI in network security defense

AI is a set of algorithms based on empirical data to improve the performance of the system itself. It obtains known attributes from a large number of data to solve the problems of classification, clustering, dimension reduction and so on. The utilization of AI in network security defense can effectively solve the problem of network security defense. The general utilization process of AI in network security defense research mainly includes several stages as shown in Figure 1, which are independent and interrelated.

![Figure 1. Utilization process of AI in network security defense.](image)

Among them, security problem abstraction is to map network security defense problems into categories that can be solved by AI [3]. To solve security problems by using AI tech, it is necessary to abstract and define problems, and map network security problems into classification, clustering and dimension reduction problems that AI can solve, as shown in Table 1 below. Through the reasonable abstraction and definition of network security problems, we can make clear how to collect data, and choose the appropriate AI algorithm to build the security problem model.

| Contents                  | Examples                                                                 |
|---------------------------|--------------------------------------------------------------------------|
| Classification            | Trojan detection, base station detection, virtualization security, credit card fraud |
| Clustering                | Identity authentication, abnormal account detection, network intrusion detection |
| Dimension reduction       | Device identity authentication and malicious web page identification     |
2.1.1. Data acquisition
The utilization of AI will produce a large amount of data, so it is necessary to effectively collect the generated data, mainly by collecting data from the system layer, network layer and utilization layer, as shown in Table 2 below.

**Table 2. Generated data collection from the system layer.**

| Layers          | Data                                                                 | Examples                                           |
|-----------------|----------------------------------------------------------------------|----------------------------------------------------|
| System layer    | Chip information, device information, status information             | Location information, SMS log                      |
| Network layer   | Network packet data or network stream data                           | Protocol classification and anomaly detection of TCP stream data |
| Utilization layer | Data generated and stored by various utilization software           | Software security testing, network public opinion analysis |

2.1.2. Data pre-processing and feature extraction
The collected original data often has some typical problems such as data missing, so it is necessary to process the collected data before feature extraction, mainly including data normalization, discretization and unbalanced processing, as shown in Table 3 below.

**Table 3. Data pre-processing and feature extraction process.**

| Layers                     | Objective                                           | Examples                                                   |
|----------------------------|-----------------------------------------------------|------------------------------------------------------------|
| Data pre-processing        | Improving the quality of data                       | TCP stream data collected from within the enterprise       |
| Processing of data outliers| Improving the model effect                          | Fixed value filling, mean filling, upper and lower data filling |
| Processing of unbalanced data | Increase the sample size to balance the data set | Bootstrapping and replication                              |
| Data set segmentation      | Data set preparation                                | Training set, verification set and test set                |
| Feature extraction         | Extract the most essential attributes               | Host information characteristics, static link relationship |

2.1.3. Model construction, validation and effect evaluation
First of all, in the construction level of the model, as the core of the utilization of AI in network security defense, the model construction includes two aspects: algorithm selection and parameter optimization, so as to complete the key process of network security defense [4]. Secondly, in the verification level of the model, the validity of the model is evaluated through verification. The process includes the verification of the accuracy of the model and features, and the representativeness of the data. If the preferential model is not good, other learning algorithms are selected to adjust the parameters. In addition, the learning effect and generalization ability of the model are evaluated.

2.2. Utilization of AI in network security defense
First of all, in the chip security detection layer of network security defense system, mainly including poor chip detection, hardware Trojan horse detection and PUF attack. Secondly, in the aspect of system hardware and physical environment security, it mainly includes device identity authentication of network equipment, physical layer side channel attack response, pseudo base station detection, vulnerability analysis and mining, malicious code analysis, user identity authentication and virtualization security. In addition, the utilization of AI in the network security defense is mainly conducive to the technical advantages of AI to effectively protect the network system security, which includes hardware security defense and software security defense. For the hardware level, the main
protection methods are identity authentication and identity recognition. In the software layer, the physical layer is used to protect the network security effectively.

3. Utilization of network security defense based on AI

3.1. Current situation of network security defense
First of all, in the network security defense environment, the network security policy environment and industrial ecology have been continuously optimized, and the national level has continuously strengthened the formulation and improvement of relevant laws and regulations in the field of network security. Secondly, at the level of refining the safety requirements of important industries and emerging fields, the vigorous expansion of emerging industries and technologies represented by AI constantly drives the innovation and reform of security [5]. The emergence of new technologies and new formats often brings new security risks and challenges, and the integration and innovation of emerging technologies and network security is constantly driving the upgrading of security defense capabilities, and the abuse of emerging technologies is also constantly pushing the improvement of network security protection capabilities.

In addition, the current network security situation is still grim, data leakage, malicious attacks and so on emerge in an endless stream, such as the frequent leakage of personal information and important data, the high incidence of DDoS attacks on important websites, serious threats to network security, frequent targeted attacks launched by phishing mails, and serious threats to information security, which have brought serious losses and influence. With the deepening of people's attention to network security, the current investment in network security is also growing. Figure 2 shows the breakdown of global network security investment in 2019. And with the continuous growth of network security investment, network security defense has gradually transformed to service flower, and with the continuous improvement of policy, policy assistance, network security related industries will achieve further expansion.

![Figure 2. Network information security market structure.](image)

3.2. Utilization advantages of AI tech
First of all, AI tech has strong learning and reasoning ability, which can significantly improve the efficiency of information data processing [6]. Secondly, AI tech has strong fuzzy information processing ability, so it can control and manage network resources with uncertain information. In addition, AI tech has strong network defense assistance ability, so it can strengthen the coordination of various measures and fully mobilize the common advantages of all defense links. And the cost of
network defense based on AI tech is low. Based on accurate data expansion, it improves the utilization efficiency of various resources and realizes the optimal configuration of network data.

3.3. Utilization of AI tech in network security defense
First of all, in the utilization level of intelligent firewall in network security defense, it can analyze and process all kinds of data by itself, reduce the calculation amount of data by computer, accurately intercept harmful data flow, and greatly enhance the defense performance of firewall. Secondly, in the utilization level of spam automatic detection tech in network security defense, based on AI tech, it can automatically detect spam and carry out intelligent identification to ensure e-mail network security. In addition, in the utilization level of intrusion detection, it can accurately and efficiently analyze the network information and data types to resist the interference of external bad information, monitor the invasion of various viruses, and strengthen the protection of network system and equipment.

4. Conclusion
In summary, as an important support to ensure the stability and orderly operation of network environment, network security has become the hot spot of many modern technologies represented by AI. The utilization of AI in network security defense can greatly improve the protection ability of network security, release the flexibility and security of network more powerful, and ensure the normal expansion of many fields of utilization. This paper analyzes the utilization process of AI in network security research. Through the research on the utilization of network security defense based on AI, this paper analyzes the current situation of network security defense, the utilization advantages of AI tech and the specific utilization of AI tech in network security defense.

References
[1] Li Zeyu. Analysis on the utilization of AI tech in network security defense [J]. Information and communication, 2018 (1): 196-197.
[2] Liao Fuzhao, Lu yourong, Ma Yun. Current situation and expansion of military information system requirements engineering [J]. Command information system and tech, 2013, (5): 6-11.
[3] Liu Fei. Analysis on the utilization of AI tech in network security defense [J]. Electronic production, 2016 (17): 32-33.
[4] Qi Yongli. Research on military computer network information security [J]. Information security and tech, 2012, (09): 12-14.
[5] Wu Jingjing. Analysis on the utilization of AI tech in network security defense [J]. Computer and network, 2017, 43 (14): 60-61.
[6] Wu Yuandi, Si Guangya, Luo PI. Utilization of AI tech in Cyberspace Security Defense [J]. Computer utilization research, 2015, 32 (8): 2241-2244.