Application of Artificial Intelligence Technology in Computer Network Security

Jialiang Zhang
(Corresponding author: Jialiang Zhang)
Criminal Investigation Police University of China, Shenyang, Liaoning, 110854, China
No. 83-21-212, Tawan Street, Huanggu district, Shenyang, Liaoning, 110854, China
(Email: zhangjl_vip@sina.com)
(Received; revised and accepted)

Abstract

Since the 21st century, the degree of informatization has been greatly accelerated, which has brought great convenience to people's life. Moreover the problem of computer network security has become a crucial point in the development of information technology. How to protect network security and safeguard their own rights and interests are the problems faced by network security. Artificial intelligence technology is also developing with the progress of information technology. This study proposed the application of artificial intelligence in computer safety protection by combining artificial intelligence with computer network security. Artificial intelligence based Trojan horse detection model was established and tested. The experimental results demonstrated that the proposed artificial intelligence model could accurately and rapidly detect out Trojan horse program, with a low false alarm rate and missing alarm rate, suggesting favorable performance. This work provides a reference for the application of artificial intelligence technology in computer network security.

Keywords: Artificial intelligence; Computer network security; Trojan horse detection

1 Introduction

Artificial intelligence, a branch of computer science, is a new technical science which focuses on developing theories, methods, technologies and application systems for simulating, extending and expanding human intelligence [3, 27]. The technology can operate computer by simulating the intelligence of multiple people to make it solve and analyze problems like human. Artificial intelligence technology has been widely used in various fields, and scholars in various countries have conducted considerable research on it. Liao *et al.* [13] applied artificial intelligence technology in the medical field to help nurses solve problems and guide nursing. It was found through investigation that the heterogeneity of artificial intelligence technology in nursing diagnosis was 87%, suggesting a high applicability in the medical field. Wang [28] explored the application of artificial intelligence technology in intelligent video surveillance system, established artificial intelligence technology based image surveillance system, and explained the feasibility and advancement of the system through verification. Network is extremely developed currently; however there are many threats such as virus on the Internet. How to prevent those threats has been the primary problem.

Morel [16] considered that network security needed to be based on artificial intelligent technology. He also advocated focusing on Web application security in practice and controlling the possibilities of false positive and false negative using knowledge based system, probabilistic reasoning and Bayesian updating. Demertzis and Iliadis [7] proposed a network based online system for network security protection. The system analyzed the basic characteristics of network traffic with the minimum computing power to find the existence and types of potential network abnormalities and identified Packed Executable with the minimum computing power and resource to find the existence of malicious software. Ling *et al.* [14] proposed a model built on AdjointVM. The model is a virtual computer with the ability of double circular chain intrusion detection which can block the invasion of attacker. In this study, artificial intelligence was analyzed and applied in network safety protection; the way how to combine artificial intelligence and computer network security was proposed. This work provides a reference for the application of artificial intelligence in network security.

2 Artificial Intelligence Technology

Artificial intelligence technology mainly aims at studying and developing simulation of human brain, i.e. developing artificial intelligence systems which can operate artifi-

cial intelligence behaviors through computer according to human body intelligent activity rules [5]. Artificial intelligence technology involving many subjects and theories including linguistics, computer science and neurology is a subject with high comprehensive level [12]. Application of artificial intelligence technology in practice should coordinate with other subjects to achieve the combination of theory and technology and generate intelligence technologies that imitate human brain.

Artificial intelligence technology has four major characteristics. The first characteristic is favorable fuzzy information processing capacity. Compared to other computer technologies, it was better in processing fuzzy information [4]. The second characteristic is strong collaboration ability. Artificial intelligence divides network security management into three levels, and managers at the higher level should monitor managers at the lower level. Such a complete monitoring system greatly enhances the collaboration ability of network security defense. Next is good learning and nonlinear processing ability. It can learn during information mining. The current network is complex and changes constantly. Many unexpected matters may happen during network security management, which makes computer network a nonlinear control object [20]. The last characteristic is low computational cost. Calculation tasks can be fulfilled by one time based on optimal solution obtained through control algorithm, which reduces resource consumption and achieves energy conservation [23].

3 Application of Artificial Intelligence Technology in Computer Network Security

3.1 Firewall

Firewall technology is the most extensively applied technology in network security management. It can protect computer network through identifying all activities which may damage the completeness and confidentiality of information [6, 8, 10]. Firewall can guarantee information security. Setting firewall can isolate hostile attacks from Hacker to computer in the internal and external network.

3.2 Anti-virus Technology

Online anti-virus technology based on artificial intelligence can timely discover the invasion of network virus and alarm users to respond timely according to warning messages [17, 21, 22].

3.3 Establishment of Rule Generation Type Expert System

Expert technology is one of the extensively applied artificial intelligence technologies in network security management [2, 15]. Expert system is an invasion detection system designed based on all professional knowledge of experts. Application of expert system can reduce the workload of invasion detection.

3.4 Application of Artificial Neural Network System

Artificial neural network is good at identifying invasion mode which carries noise or is hidden [24]. The system is designed based on the long-term simulation of human brain; hence it has favorable learning ability and strong adaptive capacity and can efficiently identify invasion behaviors.

3.5 Application of Artificial Immunological Technique

Artificial immunological technique, one of artificial intelligence technologies, can simulate a series of defense manifestations produced after human immunity [29]. In computer network management, it can improve the learning ability of natural defense mechanisms, prevent information from invasion by network virus, and effectively protect the integrity and confidentiality of information.

4 The Framework of Trojan Horse Detection Model

Trojan horse virus refers to a kind of virus which controls a computer through specific programs. Generally, Trojan horse virus is divided into two programs, i.e. control site and controlled site. Trojan horse virus is prevalent currently. Unlike other viruses, it will neither multiply nor infect other files on purpose. But it induces users to download through disguise and then provide the channel of the invaded computer for the invader; as a result, the invader can damage or steal users' documents and even control host remotely. General viruses have strong infection ability because of self replication. It multiplies through self replication and spread by taking advantage of the weakness of computer.

Artificial intelligence based Trojan horse detection model classified programs using Bayesian classifier according to program behaviors and Trojan horse behavior features library. The model was mainly composed of program behavior extraction, behavior features library, program behavior analyzer, Trojan horse processor and user negotiation and judgment.

The main function of program behavior extraction was to monitor and record suspicious behaviors in system and send the recorded data to program behavior analyzer. There were suspicious behaviors such as automatic operation of documents, hiding documents and closing

security system when Trojan horse operated. Trojan horse behavior features library included information such as Trojan horse behaviors and its action objects of the

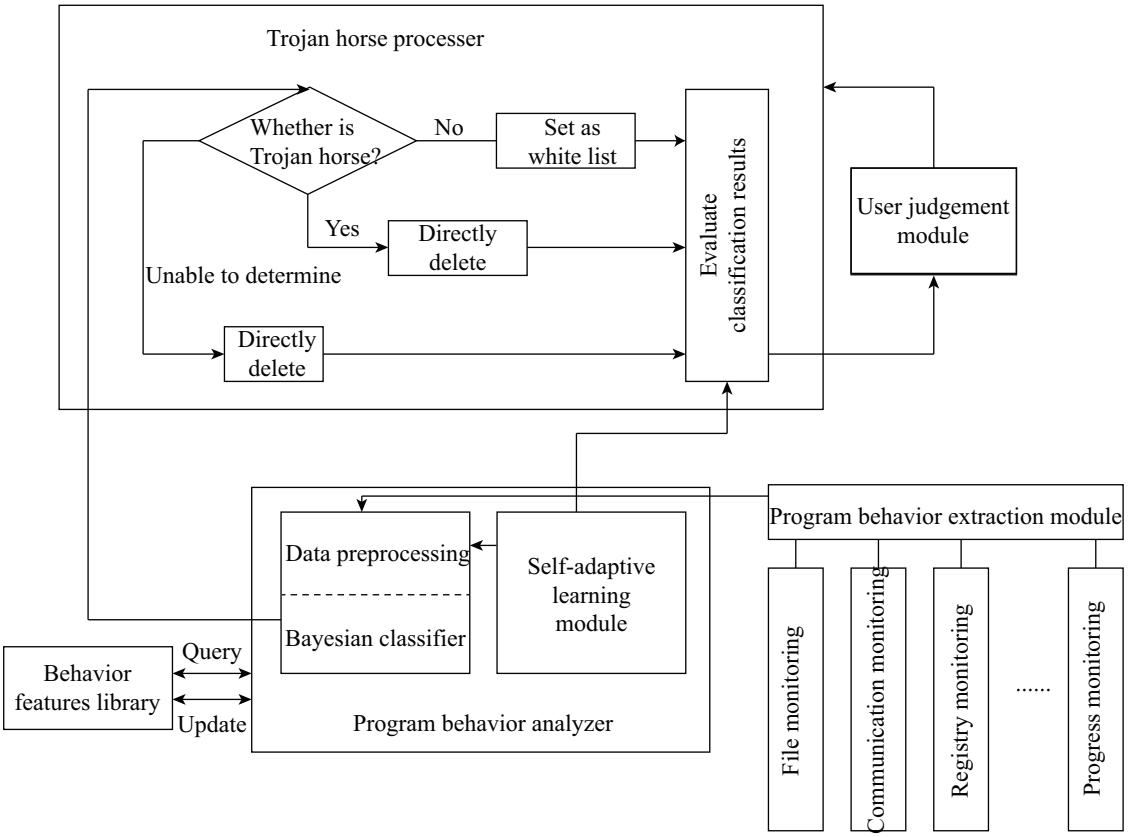

Figure 1: Artificial intelligence based Trojan horse detection model

Table 1: Brief description of behavior analysis module

		Input	**Output**	**Process**
Data preprocessing	Redundancy elimination	Processing feature vector independence	Non-redundant feature set	(1) Calculate feature CRR (2) Eliminate features with low correlation degree
	Feature vector independence processing	Non-redundant feature set	Mutually independent non-redundant feature set	Merge behavior attributes and reduce using SNCB model
	Weight calculation	Mutually independent non-redundant feature set	Feature weight	(1) Assign influence factors (2) Obtain influence degree (3) Calculate weight
Classification calculation		(1) Sample features set (2) Classification algorithm (3) Unknown examples (4) System parameter table	Classification results	(1) Statistical calculation of sample features (2) Extraction of features of examples (3) Classification
Classifier learning		Classification performance table performance table	(1) Feature set table (2) System parameter table	(1) Incremental learning (2) Relearning (2) Relearning

behaviors and a large amount of basic probability information. Program behavior analyzer, an important component of the system, could determine the category of programs using Bayesian classifier and constantly study according to the data provided by the behavior library to enhance its classification ability. In user judgment module, user set a value, and the size of the value determined the category width of the classifier. When the classifier was unable to make correct judgment, then it was processed by users; users processed results using processor after judgment. The main framework is shown in Figure 1.

4.1 Program Behavior Extraction Module

The monitoring and capture of program behaviors should be done inside operating system to achieve the monitoring of file system, registry and system process. In this study, APIHOOK technology was used to intercept the call of system program.

4.2 Behavior Features Database

Behavior characteristics database which included behavior characteristics of Trojan horse and normal program could provide basic evidences for computer classification. It could be divided into characteristic set database and feedback adaptive database. The characteristic set database mainly included characteristic set table, testing features table, parameter table and feature datum table. Feedback adaptive database mainly included classification performance table and system parameter table.

4.3 Behavior Analysis Module

Behavior analysis module had function of data preprocessing, classification calculation and classifier learning (Table 1).

Table 2: Duration of 10 times of detection

No.	Artificial intelligence technology(S)	Traditional technology (S)
1	1.4172	10.2547
2	0.9388	11.1024
3	1.2511	9.0325
4	0.8219	9.6935
5	1.2101	10.5241
6	1.5114	9.9857
7	0.9918	10.2155
8	1.1192	11.0123
9	0.9712	10.3954
10	1.0116	9.9069

4.4 System Response Module

After classification of programs which needs detection, system processing was needed. For example, Trojan horse program needs to be eliminated once abnormal behaviors of Trojan horse were detected out; monitoring stopped if normal program was detected out. When the model was unable to identify a program, then the program was isolated, determined by users, and processed after determination [1, 9, 26].

5 Experimental Results and Analysis

Artificial intelligence technology and the traditional computer network security management technology were tested to compare the network protective efficacy of the two technologies.

Firstly the detection speed of the two technologies was compared; 990 legal programs and 10 Trojan horse viruses. The Trojan horse programs used in this study was from China Hacker Union, and the legal programs were from common software and system files. The detection results are shown in Table 2.

As shown in Table 2, artificial intelligence technology cost no more than 1.5 s for scanning 1000 files, while the traditional technology cost more than 9 s. It indicated that artificial intelligence technology could more effectively and rapidly scan network source files and identify Trojan horse virus, suggesting a great role in the protection of computer network security.

To further test the detectability of artificial intelligent technology, parameter $\delta(\delta > 1)$ was introduced to measure the classification width of the classifier. The larger the value of δ, the smaller the determination scope, the more accurate the result, but the more undecidable situations; the smaller the value of δ, the larger the determination scope, the less undecidable situations, but the less accurate the result. The two technologies were tested by for three times according to different detection width δ. t stands for the number of Trojan horse programs, and n stands for the number of legal programs. The experimental results are shown in Table 3.

It could be seen from Table 3 that the detection effect of the artificial intelligent technology was superior to that of the traditional technology, and moreover the artificial intelligent technology had a low missing alarm rate and false alarm rate, suggesting a favorable performance in detecting Trojan horse viruses. But it should be noticed that the number of unclassified programs increased though the detection rate improved with the increase of δ. Hence the value of δ should not be too large.

With the development of information technology, the crime pattern has also changed, and internet gradually becomes a novel criminal means [25]. The development of network technologies results in the increase of network crimes and the severity of network invasion and attack;

Table 3: Comparison of the two technologies under different detection width

Evaluation index	δ=2, t=100,n=200		δ=8, t=100, n=200		δ=20, t=160, n=180	
	Artificial intelligent technology	The traditional technology	Artificial intelligent technology	The traditional technology	Artificial intelligent technology	The traditional technology
Number of Trojan horse viruses identified	96	82	98	83	158	129
Number of Trojan horse viruses identified as legal programs	4	8	1	9	3	9
Number of legal programs identified as Trojan horse virus	2	6	2	5	1	5
Number of unclassified	2	-	6	-	8	-
Detection rate	96%	82%	98%	83%	98.75%	80.6%
Missing alarm rate	4%	8%	1%	9%	3%	9%
False alarm rate	2%	4.67%	1%	4.67%	1.18%	4.11%
Unclassification rate	0.67%	-	2%	-	2.35%	-

hence stronger network defense systems are needed [19]. Artificial intelligence technology, one kind of computer science, is a technology simulating the thinking process and behaviors of human through computer. It mainly includes the principles of intelligence implementation and the manufacturing of computers which can simulate computer. Nakayamada *et al.* [18] applied artificial intelligence into electron beam lithography modeling and improved the production efficiency and location preciseness through adjusting point spread function. Kang *et al.* [11] introduced the tendency of artificial intelligence technology and applied it in health care, aiming to provide optimal treatment scheme for patients in clinical tests. This study applied artificial intelligence technology into network security management and found that the technology could precisely and rapidly detect virus files in other files.

6 Conclusions

In conclusion, artificial intelligence has strong fuzzy information processing ability, collaboration ability, learning ability, nonlinear processing ability and cost few resources in calculation. Based on artificial intelligence, this study proposed a Trojan horse detection model. The model could rapidly and accurately detect Trojan horse virus. The experiment suggested that the model could precisely find out Trojan horse viruses in a short time while defending computer network security, with a low missing alarm rate and false alarm rate. This work provides a reference for the application of artificial intelligence technology in computer network security management.

References

[1] A. A. Al-khatib, W. A. Hammood, "Mobile malware and defending systems: Comparison study," *International Journal of Electronics and Information Engineering*, vol. 6, no. 2, pp. 116–123, 2017.

[2] M. H. R. Al-Shaikhly, H. M. El-Bakry, and A. A. Saleh, "Cloud security using Markov chain and genetic algorithm," *International Journal of Electronics and Information Engineering*, vol. 8, no. 2, pp. 96-106, 2018.

[3] M. Anderson, R. Bartk, J. S. Brownstein, *et al.*, "Reports of the workshops of the thirty-first AAAI conference on artificial intelligence," *AI Magazine*, vol. 38, no. 3, pp. 72-82, 2017.

[4] C. Bhargava, V. K. Banga, and Y. Singh, "Reliability Comp arison of a fabricated humidity sensor using various artificial intelligence techniques," *International Journal of Performability Engineering*, vol. 13, no. 5, pp. 577-586, 2017.

[5] A. Bundy, *Preparing for the Future of Artificial Intelligence*, Penny Hill Press, 2016.

[6] D. Dai, "Human intelligence needs artificial intelligence," *Sensors*, vol. 5855, no. 3, pp. 95-99, 2018.

[7] K. Demertzis and L. Iliadis, *Hybrid Artificial Intelligence System for Cyber Security*, Apr. 2014. (`file:///C:/Users/user/Downloads/bioHAIFCS.pdf`)

[8] C. Huang and C. Wang, "Network security situation awareness based on the optimized dynamic wavelet neural network," *International Journal of Network Security*, vol. 20, no. 3, pp. 593-600, 2018.

[9] S. Islam, H. Ali, A. Habib, N. Nobi, M. Alam, and D. Hossain, "Threat minimization by design and deployment of secured networking model," *International Journal of Electronics and Information Engineering*, vol. 8, no. 2, pp. 135–144, 2018.

[10] M. S. Hwang, C. T. Li, J. J. Shen, Y. P. Chu, "Challenges in e-government and security of information", *Information & Security: An International Journal*, vol. 15, no. 1, pp. 9–20, 2004.
[11] K. Y. Lee and J. Kim, "Artificial intelligence technology trends and IBM watson references in the medical field," *Korean Medical Education Review*, vol. 18, no. 2, pp. 51-57, 2016.
[12] S. Li, "Handwritten character recognition technology combined with artificial intelligence," *Journal of Discrete Mathematical Sciences & Cryptography*, vol. 20, no. 1, pp. 67-178, 2017.
[13] P. H. Liao, P. T. Hsu, W. Chu, and W. C. Chu, "Applying artificial intelligence technology to support decision-making in nursing: A case study in Taiwan," *Health Informatics Journal*, vol. 21, no. 2, pp. 137-148, 2015.
[14] C. H. Ling, W. F. Hsien, and M. S. Hwang, "A double circular chain intrusion detection for cloud computing based on adjointVM approach," *International Journal of Network Security*, vol. 18, no. 2, pp. 397-400, 2016.
[15] Y. Miao, "Fuzzy cognitive map for domain experts with no artificial intelligence expertise," in *International Conference on Control Automation Robotics & Vision*, Singapore, Dec. 2014.
[16] B. Morel, "Artificial intelligence and the future of cybersecurity," in *Proceedings of the 4th ACM workshop on Security and Artificial Intelligence*, pp. 93-98, 2011.
[17] K. Murugan and P. Suresh, "Efficient anomaly intrusion detection using hybrid probabilistic techniques in wireless ad hoc network," *International Journal of Network Security*, vol. 20, no. 4, pp. 730-737, 2018.
[18] N. Nakayamada, R. Nishimura, S. Miura, H. Nomura, and T. Kamikubo, "Electron beam lithographic modeling assisted by artificial intelligence technology," in *Proceedings of Symposium on Photomask and Next-Generation Lithography Mask Technology*, SPIE 10454, 2017.
[19] E. U. Opara, O. A. Soluade, "Straddling the next cyber frontier: The empirical analysis on network security, exploits, and vulnerabilities," *International Journal of Electronics and Information Engineering*, vol. 3, no. 1, pp. 10–18, 2015.
[20] J. Orozco, Y. Bello, D. Patino, J. Colorado, F. Ruiz, and L. Solaque, "Non linear control of a robotic arm for pipeline reparation," *IEEE Latin American Transaction*, vol. 14, no. 12, pp. 4681-4687, 2017.
[21] A. A. Orunsolu, A. S. Sodiya, A. T. Akinwale, B. I. Olajuwon, M. A. Alaran, O. O. Bamgboye, and O. A. Afolabi, "An empirical evaluation of security tips in phishing prevention: A case study of nigerian banks," *International Journal of Electronics and Information Engineering*, vol. 6, no. 1, pp. 25-39, 2017.
[22] A. A. Orunsolu, A. S. Sodiya, A. T. Akinwale, B. I. Olajuwon, "An anti-phishing kit scheme for secure web transactions," *International Journal of Electronics and Information Engineering*, vol. 6, no. 2, pp. 72–86, 2017.
[23] C. Ramirez-Atencia, V. Rodrguez-Fernndez, A. Gonzalez-Pardo, and D. Camacho, "New artificial intelligence approaches for future UAV ground control stations," in *IEEE Congress on Evolutionary Computation*, San Sebastian, Spain, June 2017,
[24] R. Silipo and C. Marchesi, "Artificial neural networks for automatic ECG analysis," *Neural Network*, vol. 96, no. 5, pp. 80-90, 2017.
[25] J. R. Sun, M. L. Shih, and M. S. Hwang, "Cases study and analysis of the court judgement of cybercrimes in Taiwan," *International Journal of Law Crime & Justice*, vol. 43, no. 4, pp. 412-423, 2015.
[26] A. Tayal, N. Mishra and S. Sharma, "Active monitoring & postmortem forensic analysis of network threats: A survey," *International Journal of Electronics and Information Engineering*, vol. 6, no. 1, pp. 49–59, 2017.
[27] B. M. Wagman, "Artificial Intelligence and Human Cognition," *Quarterly Review of Biology*, vol. 68, no. 1, pp. 126-131, 2008.
[28] J. J. Wang, "Research on image monitoring system based on artificial intelligence technology," *Agro Food Industry Hi Tech*, vol. 28, no. 1, pp. 1816-1819, 2017.
[29] M. Wang, S. Feng, C. He, Z. Li, and Y. Xue, "An artificial immune system algorithm with social learning and its application in industrial PID controller design," *Mathematical Problems in Engineering*, vol. 2017, no. 3, pp. 1-13, 2017.

Biography

Jialiang Zhang, born in Harbin in the 3rd, January, 1981, has gained the master degree in the field of computer software engineering from Northwestern Polytechnical University, Shaanxi, China. Now he works as a lecturer in National Police University of China, Liaoning, China. His interests of research include computer software, database and network. He has published several papers in different journals of public security colleges. Moreover he won the second prize in the Innovation Competition for College Students in the Ministry of Public Security held in 2017 as an instructor, the second prize in the Education Software Competition held by the Ministry of Education of Liaoning Province held in 2015 and the second prize in the Courseware Competition of Liaoning Province held in 2015.