DOI: 10.54254/2755-2721/19/20231040

Application of artificial intelligence in network security defense

Yuqiang Cao

Beijing YuYing School, Beijing, China, 100036

18301397069@163.com

Abstract. With the development of today's social network, people use the Internet more frequently and become more reliant on it. However, as a result of the development of the network, network attacks are becoming more frequent, and people have an imperative need for a secure and dependable computer network. Meanwhile, the technology of artificial intelligence is progressively maturing, so the application of artificial intelligence in network security defense will be a more effective means of addressing network security's hidden dangers. This paper focuses primarily on the benefits of the application of artificial intelligence to network security defense, as well as summarizing and analyzing the application of artificial intelligence to network security defense. This paper concludes, by analyzing the most recent literature and evaluations, that AI plays a crucial role in resolving network security issues and can effectively withstand certain network attack threats.

Keywords: artificial intelligence, machine learning, deep learning.

1. Introduction

People's primary source of information is now the Internet. In 2017, approximately 48 percent of the global population utilized the Internet as a source of information [1]. This increased to 81 percent in developed nations [2]. The increased use of the Internet has made it a prime target for cybercriminals. A secure and dependable computer system must guarantee the confidentiality, accessibility, and integrity of the data it contains. Moreover, with the advancement of artificial intelligence, machine learning technology now plays a crucial function in network security. There is a great deal of information on the Internet that describes the application of Machine Learning (ML) to the prediction of cyber threats on the dark web or deep web. Mohammad et al. With the advancement of science and technology, artificial intelligence is increasingly used to solve computer security problems. However, this paper focuses on introducing a variety of artificial intelligence algorithms to solve network security problems using the deep learning algorithm [3]. This paper will first introduce the status quo of network security and artificial intelligence, and then analyze and introduce the specific application of machine learning algorithms in network security by reflecting the benefits of their application through an analysis of various machine learning algorithms. This paper will aid those unfamiliar with artificial intelligence and network security in comprehending the application of artificial intelligence to network security. In addition, it can serve as a resource for future researchers investigating related topics.

2. Cyber security and artificial intelligence

2.1. Network security status

Kaspersky defines cyber security as follows: Cyber security is the discipline of defending against malicious attacks on computers, servers, mobile devices, electronic systems, networks, and data. Information technology security is also known as electronic information security. The term is applicable in a variety of contexts, ranging from business to mobile computing, and can be categorized into a few categories [4].

With the advancement of science and technology and the growth of society, today's network security faces a variety of threats, such as unauthorized access to the computer and attempts to harm or alter its data. In 2018, Cisco's annual report (Cisco is a renowned network solution provider) revealed that more than 0.5 percent of attacks caused damages of $500 million or more [5]. Phishing and malware are the most prevalent forms of Internet security. Phishing is a website disguised as a legitimate one in order to take the user's information, similar to a scammer. Malware consists primarily of viruses, worms, and trojans. Viruses are uncommon in the network environment of today. The primary characteristic of viruses is their ability to infect other files, making them difficult to remove. Self-replication distinguishes worms from other malicious software. Similar to a phishing website, a Trojan horse disguises itself as an ordinary piece of software and activates its functions only after the user executes the pertinent program. In addition, unauthorized spam is a common threat; spam will occupy our mailboxes, causing us to spend more time cleaning them, and for mobile terminals, spam mail such as spam text messages and phone calls, etc. These are also the most significant threats to network security in modern society.

Moreover, network assaults can be broadly classified into four categories [6]. The first type is Denial of service (DOS), in which the perpetrators overload the memory resources of the computer to prevent normal users from accessing it. In Remote to Local (R2L), attackers send data packets to computers through networks and exploit vulnerabilities to obtain unauthorized access to computers. User to root (U2R) occurs when network access is restricted and an adversary gains access to the system root directory by exploiting a vulnerability using an ordinary user account. Using networks to acquire information or vulnerabilities in preparation for future attacks is known as probing.

2.2. Current state of artificial intelligence

Artificial intelligence, a subfield of computer science, is a trending topic in contemporary culture. An artificial neural network (ANN) is an early effort to simplify the model of biological neuronal systems. Machine learning (ML) is a subfield of artificial intelligence in which algorithms can construct models from trained data and make new predictions. Widespread use of machine learning algorithms to solve security issues, detect new attacks, and identify fraudulent websites [7-8].

There are numerous types of machine learning techniques. Common methods for machine learning include supervised learning, unsupervised learning, reinforcement learning, semi-supervised learning, etc. Supervised and unsupervised learning are the two most fundamental learning methods. Training models with existing data and then classifying or predicting unknown data constitutes supervised learning. Unsupervised learning, on the other hand, does not have any known data and discovers the internal structure and rules of data in various methods. In addition, reinforcement learning was utilized by the most famous AlphaGo program some time ago [9].

Moreover, deep learning is a subfield of machine learning. With the advancement of technology in recent years, deep learning has become increasingly prevalent in applications such as autonomous driving. Traditional machine learning performed better with less data in the past, whereas deep learning performed better with more data.

3. The characteristics and benefits of artificial intelligence's deep learning algorithm

3.1. Strong defensive capability

3.1.1. Strong fuzzy information processing ability. Users are exposed to a variety of data every day in the current big data environment, and it is difficult to determine whether some of the fuzzy data contain security hazards. These complicated data and information will endanger users. Therefore, ambiguous processing by artificial intelligence can solve many of our security issues. In addition, people will utilize the imprecise information processing capability of artificial intelligence to identify application or system vulnerabilities. This technology can be used for good, such as discovering bugs in one's own software, but it can also be exploited by bad actors, who can rapidly discover massive zero-day vulnerabilities that pose serious security threats.

3.1.2. Learning and reasoning ability. The ability of Ai to learn and reason is crucial for addressing network security issues. Diverse potential threats have multiplied alongside the Internet's rapid growth, and there is a dearth of qualified personnel and adequate technology to combat the various issues. Nevertheless, with the assistance of artificial intelligence, data can be analyzed and model prediction can be used to effectively resolve this issue. Using AI to analyze the most recent data and make accurate predictions in order to address the same type of threat or prevent a large number of prospective threats.

3.2. Low-use cost

There is no doubt that the conventional network security system will consume a great deal of time and resources, resulting in overall inefficiency and inadequate defense effectiveness. Under such conditions, the cost is enormous and it is difficult to guarantee the network's security. In contrast, data processing is more efficient and effective with the use of artificial intelligence-based algorithms. Faced with vast amounts of data, they are able to complete the calculation and analysis of data in an efficient manner, enabling them to reflect more effective defense effects in the face of threats. Under the premise of minimal cost, network security protection can be accomplished more efficiently using artificial intelligence.

4. The application of artificial intelligence in network security defense

4.1. Detect intrusions on computer networks

There are three categories for network analysis of intrusion detection systems. First, detection based on misuse. Misuse-based detection is used to identify known system attacks. Misuse-based detection is used to detect abnormal situations, differentiating between normal and abnormal situations, and Anomaly-based detection is a method that combines the first two detection methods to enhance detection accuracy [10]. These three detection methods are all traditional intrusion detection methods. However, with the advancement of science and technology, assailants may have discovered vulnerabilities in these traditional detection methods, which could lead to their failure and the loss of critical data. Consequently, these techniques no longer effectively defend users from intrusions. We can therefore use artificial intelligence to analyze the attack pattern of an intrusion in order to detect or prevent its occurrence.

Table 1 shows the evaluation of intrusion detection effects of various machine learning technologies from 2018-2020.

Table 1. Comparison and summary of intrusion detection ML models from 2018 to 2020 [11].

Published Year	Dataset	Sub-Domain	Learning Model	Attack Types	Results		
					Accuracy	Precision	Recall
2018	KDD	Misuse-Based	DT	-	99.96%		-
2018	KDD CUP99	Hybrid-Based	DT	-	92.87%	99.90%	-

Table 1: (continued).

2018	DARPA	Misuse-Based	ANN	-	99.82%		-
2018	UNSW-15	Anomaly-Based	ANN	Dos, U2R, Probing, R2L	92.40%	-	-
2018	KDD 99	-	NB, AdaBoost, RF	Dos, U2R, Probing, R2L	NB 91.03% Adaboost 99.89% RF 99.93%		
2019	NSL-KDD	Anomaly-Based	SVM	-	89.70%		
2019	KDD 99	-	SVM, NB, ANN	Dos, U2R, Probing, R2L	95.03%		95.23%
2019	NSL-KDD	Anomaly-Based	RF	-	95.10%	92.50%	
2019	NSL-KDD	Anomaly-Based	DBN	-	99.45%	99.20%	99.70%
2019	NSL-KDD	Anomaly-Based	ANN	-	94.50%		
2019	NSL-KDD	Hybrid-Based	RF	-	75.30%	81.40%	75.30%
2019	CICIDS	-	RF, Gradient Boosting Tree	Dos, DDos	-	-	-
2019	ISCX 2012	-	SVM, MLP, PCA	Dos, U2R, Probing, R2L	SVM 87.02% IBK 94.29% MLP 82.42%	SVM 90.10% IBK 91.40% MLP 87.20%	SVM 87.00% IBK 99.60% MLP 82.40%
2019	KDD 99, NSL-KDD UNSW-NB15	-	NB, SVM DR, RF	Dos, U2R, Probing, R2L, DDos	NB 92.90% SVM 80.10% RF 78.40%	NB 99.90% SVM 69.20% RF 94.40%	NB 91.40% SVM 96.90% RF 72.50%
2019	NSL-KDD	-	DT, MLP, SVM, KNN	Dos, U2R, Probing, R2L	DT 97.14% MLP 97.02% SVM 97.42% KNN 96.51%	-	DT 95.57% MLP 95.80% SVM 96.81% KNN 94.79%

Table 1: (continued).

2020	Customized	-	AdaBoost, J48, SVM, NB	DDos	Adaboost 93.40% J48 90.30% SVM 85.30% NB 73.10%	-	Adaboost 93.40% J48 90.20% SVM 85.20% NB 70.50%
2020	NSL-KDD	-	Deep Neural Network	Dos, U2R, Probing, R2L	95.40%	96.20%	93.50%
2020	KDD-99	-	NB, DT, RF	Dos, U2R, Probing, R2L	99.80%	99.80%	

4.2. Automatic spam detection

Today, E-mail is increasingly utilized, and inappropriate spam will negatively impact users' usage. Some advertising and marketing substantially consume the bandwidth of Internet users, thereby reducing the network's efficiency. In addition to email, other attack vectors include social media, blogs, and other platforms, such as Facebook, Twitter, YouTube, and others. It has had a significant impact on people's livelihoods. Traditional spam filtering categorizes spam and rejects it. This approach, however, is ineffective, and as attackers discover ways to circumvent it, traditional methods are no longer appropriate for addressing such security issues. Consequently, with the development of artificial intelligence, machine learning techniques can be utilized to increase efficiency and defend against such assaults with great effectiveness. Multiple platforms have utilized machine learning techniques to detect and filter spam, using a variety of methods to increase efficiency and security. ML techniques for spam classification, spam filtering, and spam identification have been proposed in the literature [12-14].

4.3. Detecting malware

Malware is a type of software that is intentionally installed on a computer and interferes with the user's normal use. It has the potential to severely harm the computer's data. Malwares include viruses, Trojan horses, and adware of uncertain origin. Criminals use this malicious software to exploit computer vulnerabilities, and the victims include not only ordinary people but also the military and businesses. In the past, detection was based on digital signature technology, but some idiotic malware and zero-day malware are ineffective. Nonetheless, machine learning technology can effectively identify zero-day attacks and idiosyncratic malware, as well as novel or hybrid malware attacks [15]. When combined with other artificial intelligence technologies, machine learning can significantly improve the accuracy of detection.

5. Conclusion

This paper focuses primarily on the current state of artificial intelligence and network security, analyzes the benefits of AI to network security, and introduces AI's application in network security. Artificial intelligence can assist in resolving network security problems and threats more effectively and efficiently than traditional methods. This paper does not introduce a specific artificial intelligence technology to aid in network security defense, so it could be enhanced in this regard. With the ongoing development and enhancement of artificial intelligence technology, it is anticipated that increasingly efficient technologies, such as deep learning technology, will emerge. The combination of these novel technologies and network security is anticipated to be the primary focus of future research.

References

[1] ICT Fact and Figures 2017, Jun. 2020, https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf.

[2] Telecommunication Development Bureau, Oct. 2017, https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx.

[3] M. Almukaynizi, A. Grimm, E. Nunes, J. Shakarian and P. Shakarian, "Predicting cyber threats through hacker social networks in darkweb and deepweb forums", Proc. Int. Conf. Comput. Social Sci. Soc. Americas (CSS), pp. 1-7, 2017.

[4] What is Cyber-Security?, Jan. 2020, https://www.kaspersky.com.au/resource-center/definitions/what-is-cyber-security.

[5] Cisco 2018 Annual Cybersecurity Report, Dec. 2018, https://www.cisco.com/c/m/en_au/products/security/offers/annual-cybersecurity-report-2018.html.

[6] J. Raiyn, "A survey of cyber attack detection strategies", Int. J. Secur. Appl., vol. 8, no. 1, pp. 247-256, Jan. 2014.

[7] J. B. Fraley and J. Cannady, "The promise of machine learning in cybersecurity", Proc. SoutheastCon, pp. 1-6, Mar. 2017.

[8] A. Kulkarni and L. L. Brown, "Phishing websites detection using machine learning", Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 7, pp. 8-13, 2019.

[9] J. X. Chen, "The evolution of computing: AlphaGo", Comput. Sci. Eng., vol. 18, no. 4, pp. 4-7, Jul. 2016.

[10] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection", IEEE Commun. Surveys Tuts., vol. 18, no. 2, pp. 1153-1176, 2nd Quart. 2016.

[11] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed and M. Xu, "A Survey on Machine Learning Techniques for Cyber Security in the Last Decade," in IEEE Access, vol. 8, pp. 222310-222354, 2020, doi: 10.1109/ACCESS.2020.3041951.

[12] S. M. Lee, D. S. Kim, J. H. Kim and J. S. Park, "Spam detection using feature selection and parameters optimization", Proc. Int. Conf. Complex Intell. Softw. Intensive Syst., pp. 883-888, Feb. 2010.

[13] L. H. Gomes, C. Cazita, J. M. Almeida, V. Almeida and W. Meira, "Characterizing a spam traffic", Proc. 4th ACM SIGCOMM Conf. Internet Meas. (IMC), pp. 356-369, 2004.

[14] C. Castillo and B. D. Davison, "Adversarial Web search", Found. Trends Inf. Retr., vol. 4, no. 5, pp. 377-486, 2011.

[15] E. Gandotra, D. Bansal and S. Sofat, "Malware analysis and classification: A survey", J. Inf. Secur., vol. 5, no. 2, pp. 56, 2014.