UDC 004.49

THE ROLE OF NEURAL NETWORKS IN CYBERSECURITY SYSTEM

Kulbako A.S.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Perevyshko A. I. - senior lecturer of the department of foreign languages

Annotation: As you can see from the title this text is about the role of neural network in cybersecurity system. At the beginning, the author gives a valuable information on antivirus. After that it is spoken about working principles of neural networks used as a theoretical antivirus. Next, the author describes the models of neural networks PCA-DNN and Open AI. At the end, it is pointed out opportunity for the development of neural networks in the field of cybersecurity. I think this text is informative for the students of engineering specialties.

Keywords: Antivirus, neural networks, PCA-DNN, Open AI, social engineering, network security.

Introduction: Today, neural networks are one of the most popular and progressive information technologies used in various spheres of life. They demonstrate their versatility, they can solve complex mathematical problems, create amazing images and generate unique content. However, the potential of neural networks is not limited only to satisfying personal needs — they can also significantly improve security in cyberspace.

Given that our reality is easily vulnerable to cyber threats, including hacker attacks, break-ins and other forms of cybercrime, the use of advanced technologies to protect digital data becomes an important factor. And neural networks are one of those options.

The main part: To understand the role of neural networks in cybersecurity, we should consider various methods of detecting and neutralizing viruses, one of which is antiviruses. Antiviruses are tools that analyze other programs for the presence of harmful code in them. There are a huge number of antiviruses in the world, each of which has its own patterns of recognizing the characteristics of viruses. Therefore, to simplify, Antiviruses are divided into two types: static and dynamic.

Static antiviruses are software tools focused on preliminary analysis of source code, files and system resources in order to detect pre-known malicious threats. They are based on the signature method, where virus identification occurs by comparing the characteristic "signatures" of known threats. A static antivirus scans files and system resources, and then compares the data obtained with a database of virus signatures. If a match is found, the program is triggered and takes measures to remove or block the malicious object. The main advantage of using a static antivirus is its low resource consumption. However, we must understand that because of this, this type of antivirus is not able to adapt to new viruses [1].

Dynamic antiviruses represent a more modern approach to combating malicious software. They are based on real-time analysis of program behavior. In fact, antiviruses actively monitor the actions of programs in the system, track changes and identify suspicious activity. They use methods such as heuristic analysis, which is a sequence of actions. Initially, the antivirus monitors running programs. Then it detects virus programs, which it then sends to the "sandbox" (a virtual machine that emulates the behavior of a real computer), where it already conducts a full analysis and assessment of the threat. If the virus is still dangerous in the sandbox, the antivirus takes measures to block and delete this program [1].

The main positive quality of this type of antivirus is the ability to quickly detect new threats. Moreover, neural networks are gradually being introduced into dynamic antiviruses, which are used to correctly analyze the virus threat in the sandbox. However, all this leads to the fact that dynamic antiviruses can cause additional load on computer systems, which can reduce the performance of the device. Of course, developers are constantly working on optimizing these systems, but in many cases such optimization reduces the effectiveness of dynamic antiviruses.

However, despite possible disadvantages, the introduction of neural networks into the malware detection process provides more accurate threat recognition [1].

Therefore, realizing the potential of neural networks, we can consider that they are an alternative way to fight viruses. They are programs that consist of many elements called neurons that are connected to each other using weights. These programs can take different types of data, such as images, texts, or sounds, and process them using mathematical functions. We should note the fact that neural networks can be trained on data, finding patterns in them and adjusting their weights. This is the reason why they can be used to detect viruses by analyzing their structure or behavior and comparing them with known samples. Thus, these programs can be effective because they can adapt to new types of viruses and do not require a lot of resources to work.

For example, a possible neural network model for virus detection may consist of several layers, each of which is capable of processing different aspects of the input data. The input layer accepts the binary data of the program, the middle layers process this data, and the output layer predicts whether the program is harmless. In order for this model to work correctly, it needs to be trained by sending a large number of malware examples to the input. The model learns to understand patterns in the data indicating the presence of a virus. After training, the model is checked on new data to assess its ability to detect viruses.

Nowadays, the problem of Internet insecurity from hacker attacks remains very relevant. The possibility of hacking pages, websites, databases, as well as overloading servers or downtime from spam continue to pose serious threats. The field of cybersecurity often turns out to be insufficiently protected, and the lack of effective control measures creates a space for malicious actions.

However, modern technologies offer new approaches to solving this problem. Among them, PDA-DNN stands out - an innovative neural network designed to detect potential cyber attacks. This model uses a combination of Principal Component Analysis (PCA) and deep neural network (DNN), which allows it to more effectively identify anomalies in network behavior.

PDA-DNN has high accuracy in detecting various types of attacks, including port scanning, distributed denial of service (DDoS) attacks, botnets and others [2].

The principle of operation of PCA-DNN is as follows. First, the network data is transformed using the principal component method to extract the most crucial components. Then these components are fed into a neural network comprising multiple hidden layers, tasked with classifying the data into normal or abnormal categories. If the resulting output deviates from the input value beyond a specified range, the network deems this data as abnormal [2].

Social engineering, a method of acquiring information through manipulation and deception, involves attackers communicating with victims while impersonating someone else. Neural networks emerge as a potent tool in combating this technique due to their capability to analyze intricate patterns of behavior and manipulation. OpenAI, for instance, has developed a neural network algorithm designed to ascertain the authorship of a given text [3].

This program analyzes the structures of words, sentences, language tools, and so on. By training a neural network based on data, it can learn to understand common tactics used by social engineers, for example, phishing emails. The neural network's analytical capabilities enable it to recognize subtle nuances in communication styles and detect potential threat, thereby serving as a valuable asset in the battle against social engineering. Moreover, neural networks can help in creating personalized and dynamic security. Neural networks, due to constant analysis of user behavior patterns such as login time, a typical means of communication, can establish the level of normal user behavior. Any deviation from this level, for example, an unexpected request to transfer a money or join a group, may trigger a security alert indicating a possible attack.

Figure 1 - Example of social engineering

Conclusion: The current scenario illustrates that conventional virus protection methods may prove ineffective against emerging technologies. However, neural networks that can quickly analyze and adapt to new information may be the best solution for cybersecurity. Moreover, it is worth accepting the important fact that the development of neural networks is dramatically increasing. For example, in Figure 2, we can see two photos taken by a neural network. The difference between these two photos is 9 years.

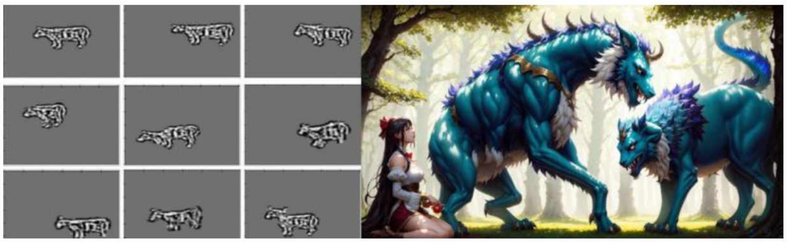

Figure 2 - Development of neural networks in the field of design

The theoretical models discussed in this article and the available resources for the development of neural networks develop the prospects for their use in real conditions. In the near future, these models may turn from concepts into reality, which opens up new prospects for cybersecurity.

Given the rapid progress in the field of artificial intelligence, neural networks can become not just a tool, but a real strong ally in the fight against cyber threats. Their ability to adapt, identify anomalies, and learn from changing cyber-attack scenarios makes them an important component in a cybersecurity strategy.

Thus, the use of neural networks in the field of cybersecurity not only promises to strengthen protection against cyber threats, but also highlights the need for further research and innovation in this area. At the same time, given the rapid pace of technology development, neural networks can become a key element of an effective security strategy in the digital world.

References

1.Введение в понятие антивирусов.: [Electronic resource] - https://telegra.ph/Vvedenie-v-ponyatie-antivirusov-04-21.

2.Cyber threat intelligence using PCA-DNN model to detect abnormal network behavior.: [Electron7ic resource]- https://www.researchgate.net/publication/357406133_Cyber_threat_intelligence_using_PCA-DNN_model_to_detect_abnormal_network_behavior.

3.New AI classifier for indicating AI-written text.: [Electronic resource] - https://openai.com/blog/new-ai-classifier-for-indicating-ai-written-text.