AMERICAN Journal of Public Diplomacy and International Studies
Volume 01, Issue 05, 2023 ISSN (E): 2993-2157

Neural Networks in Cybersecurity

Davronov Farhodjon Shuxrat o'g'li
(University of public security of the Republic of Uzbekistan)
farhoddavronov98@gmail.com

Abstract

Deep learning is a part of machine learning based on neural networks. Nowadays, everyone has heard about neural networks, and maybe not everyone knows what it is and what it does, but the name itself is familiar to everyone.

INTRODUCTION

Many devices that exist now have a neural network inside them that solves a particular task of the system. In fact, if you look deeper, this is a rather complex structure, resembling a collection of neurons in the human brain. Their very idea made many people take up this industry in order to get outstanding results. Therefore, by 2021, neural networks are being used in various areas of our lives. Cybersecurity is no exception.

Cybersecurity is a complete set of all methods responsible for protecting networks and software. With the implementation of IoT, cybersecurity is becoming more important than ever. Computer networks are vulnerable to many threats. Moreover, the system needs to be protected not only from external threats, but also needs to be protected from internal ones, such as unauthorized use of authorized access.

The main task that we face is the detection of suspicious users before they can fully commit an attack on the system.

Tasks solved by the neural network

The range of tasks solved by neural networks is quite large, but here are the main tasks that are most relevant at the moment.

An important feature of the neural network is that it is able to identify various dependencies, can find elements that were not previously in the network, and study the patterns of deliberate attacks.

The main classification, based on the above:

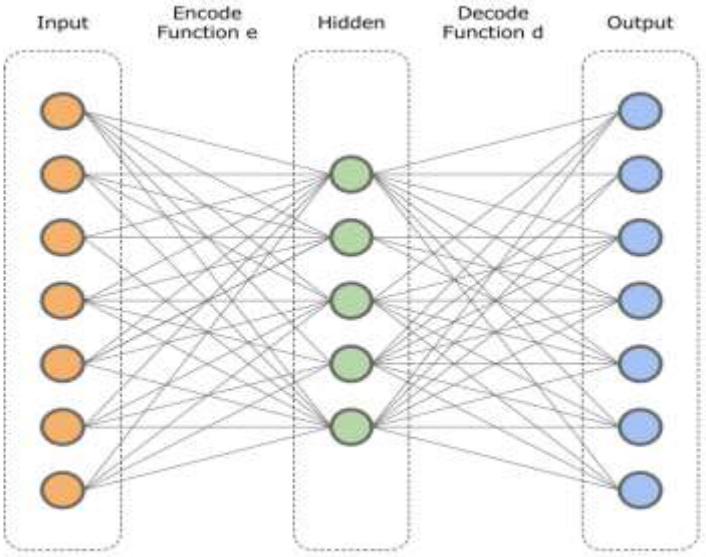
• Intrusion detection;
• Identifying certain information in the learning process, and using it to create an improved network;
• Fraud and malware detection;
• Risk assessment and analysis of system behavior.

In addition, I would like to list the areas of application in applied tasks: application in firewalls and threat detection.

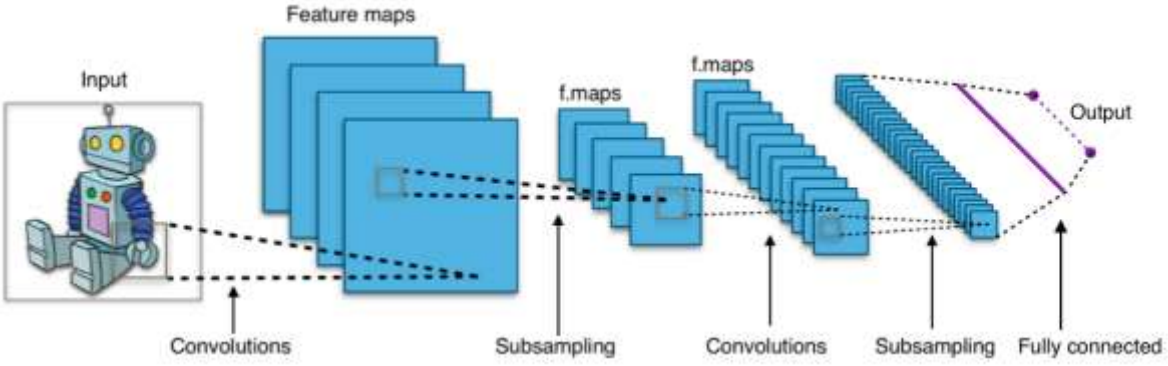
The first subtask is that the neural network analyzes traffic and tries to predict a possible intrusion. Here, the advantage of a neural network is that it can learn independently without relying on the data embedded in it.

The second subproblem is that the network has already created an image of normal behavior in the network, and now any deviation from this image will be considered an anomaly. Some attacks are easy to predict, as they were known to us in advance. Nevertheless, scammers create attacks that

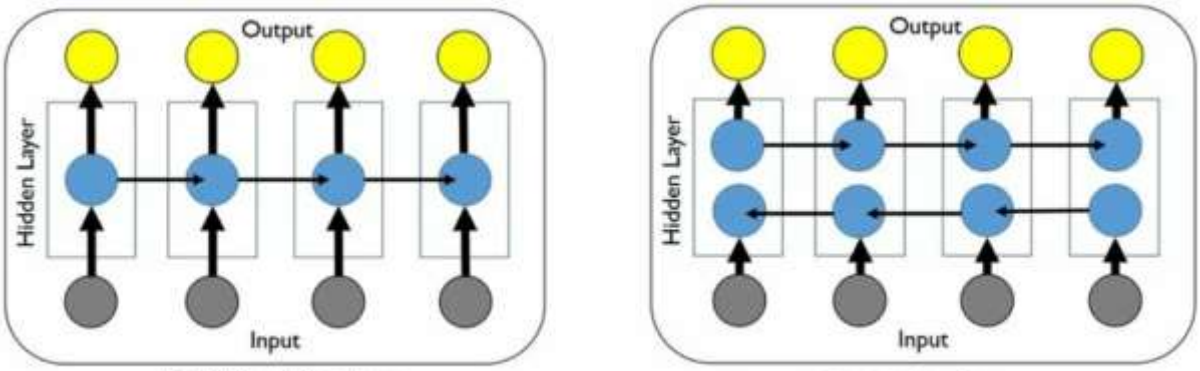
occur purposefully on new weaknesses in our system. Such an attack has no predecessors, and can harm our system before we have time to neutralize it.
The use of artificial neural networks for intrusion detection is quite an interesting and innovative topic at the moment. This is due to the fact that neural networks have flexibility, which gives them the ability to learn in real time, which increases the likelihood of correct triggering when detecting attacks.
Types of attacks
Consider the basic classification of attacks.
1. DoS attack, which is carried out in order to bring the system to failure. A huge amount of traffic is generated, due to which the server is rebooted, and then it is blocked.
2. R2L – obtaining access of an unknown user to a computer from a remote system.
3. Probe – port scanning, which leads to obtaining confidential information.
4. U2R – obtaining superuser benefits by a registered user.
5. Man-in-the-Middle – eavesdropping on a conversation or actively participating, changing the content of your messages, presenting yourself as a person or system with whom you think you are talking.
6. Session Hijacking (Cookie Hijacking) – using a valid computer session to gain unauthorized access to information or services in a computer system.
For the first four types of attacks, an extensive study of threat detection using neural networks was conducted in the article "Artificial Neural Network for Cybersecurity: A Comprehensive Review". The review article considered the results of models for classifying attacks on datasets with network connection data, such as KDD Cup 99, NSL-KDD, Alexa, OSINT, etc. The best results were shown by the LSTM, CNN-based architecture, BiLSTM and Autoencoder models. Therefore, this article proves the concept of successful use of neural networks for threat detection with sufficiently high accur.



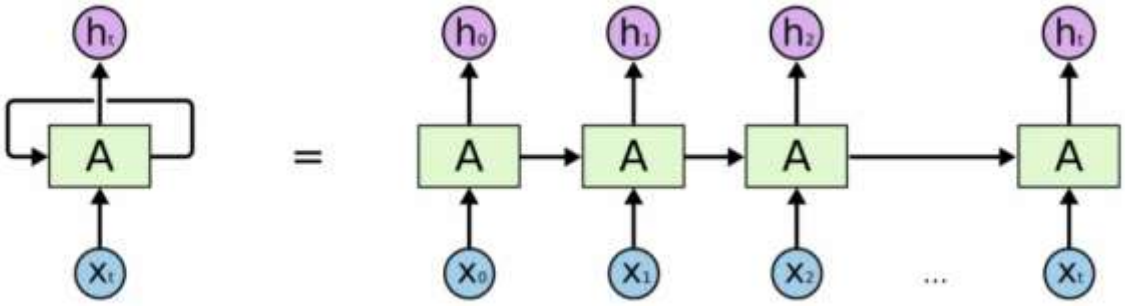
Autoencoder



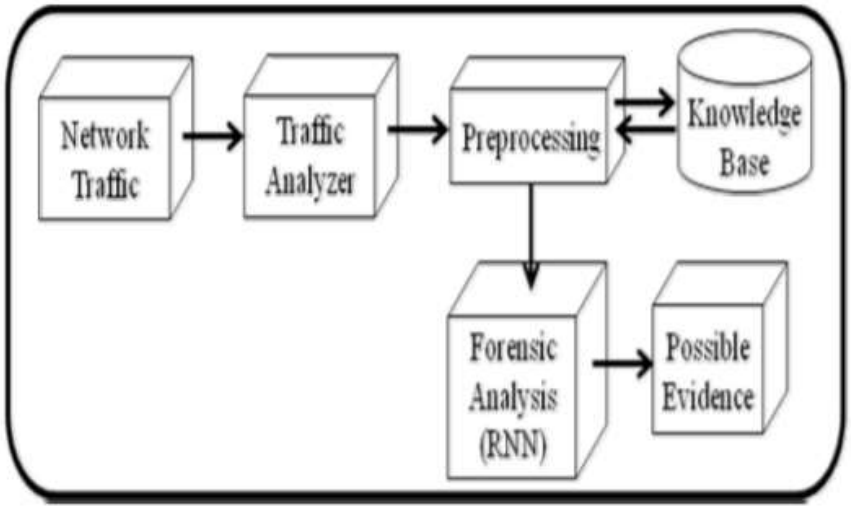
CNN



In addition to the DoS-type attack, such attacks as Man-in-the-Middle and Session Hijackin were considered in the article "Attacks Recognition Using Recurrent Neural Network". As the name suggests, recurrent neural networks cope with detecting these attacks by processing the database of users connected to the network as a time series of events. The structure of the work is shown in the picture below.



Recurrent neural network



Structure of network traffic analysis using RNN

Let's move on to a more detailed consideration of DoS, or rather a subcategory of this attack, namely DDoS.

DDoS attacks, neural networks are coming to the rescue!

DDoS attacks are becoming very popular today.

Experts identify several reasons for this. Firstly, because of the hatred of organizations. For example, the famous attack on the FBI when they decided to go against hackers. Secondly, for the sake of entertainment. Many novice attackers create them to see how much they will harm the system. Thirdly, blackmail and extortion, or other motivation for using this type of attack.

Identifying this type of attack is quite a difficult task from the point of view of the algorithm, because there are no common signs for all that will indicate that network requests really belong to real users, and not attackers.

The main difference from DoS is that this attack is carried out simultaneously from a large number of IP addresses. Such a set of computers is called a "botnet".

In turn , they themselves also have several subgroups:

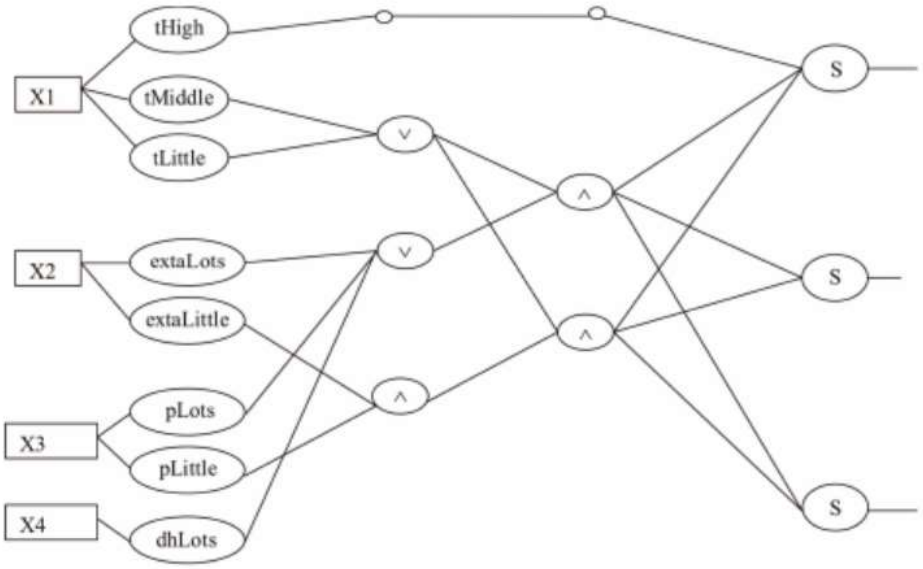
Attacks

• at the protocol level (exploits the vulnerability of the network protocol stack - SYNflood),

• at the application level (leads to application inactivity),

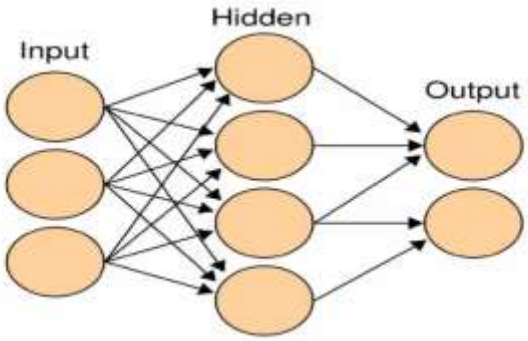
• with bandwidth saturation (there is a bombardment of requests to take up the entire bandwidth, one of the most dangerous attacks, since 100% denial of service can occur).

In 2009, an article was published telling about the creation of a "fuzzy" neural network that fought attacks like SYN flood. The essence of such a classifier was that, according to the input data, it could determine the degree of confidence in the attack. This neural network was a multi-layered structure with direct propagation, which allows it to adapt to a specific situation. The network itself was a collection of neurons calculating the values of the fuzzy conjunction function, disjunctions, neurons calculating the membership of fuzzy sets and calculating the output of the classifier itself.



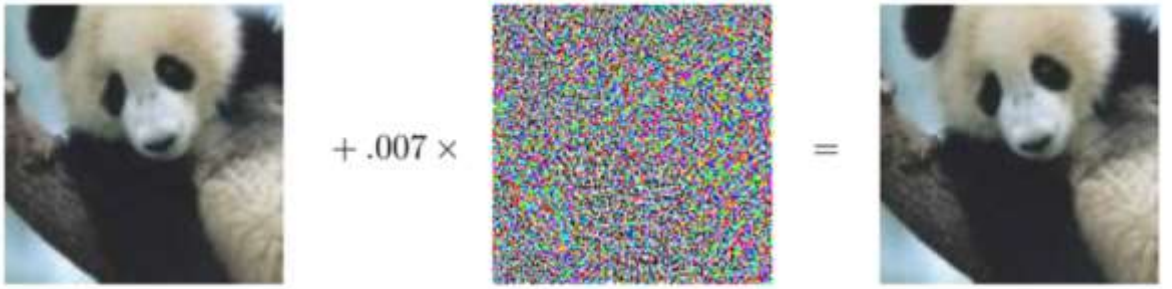
"Fuzzy" neural network classifier

In 2014, another interesting work was published, which talked about the use of a multilayer perceptron with two hidden layers. The peculiarity of this work was that they used one rather non-trivial optimization method (the particle swarm method). This method displays the behavior of, for example, bees. The application of this method does not require knowledge of the gradient of the optimized function. This method helped to achieve better results and reduce the number of system reactions to false threats.



Multilayer Perceptron architecture

The other side of the coin of using neural networks is the problem of hacking neural networks themselves. When trying to hack the neural network itself, it is enough to correctly select its parameters that most strongly affect the output of the network, thus it becomes possible to change the operation of any neural network (for example, a video camera in a zoo will see a gibbon instead of a beautiful panda). Additional modifications are finetune with special loss functions based on the normalization of real data or dynamic changes in the weights of the neural network during operation.



These are several examples of the use of neural networks in the fight against attacks, the number of which will only grow in the future.

Conclusion: In this article, the main provisions of cybersecurity were considered, such as problem statements, types of actual attacks, and methods of fighting with the help of neural networks. Undoubtedly, neural networks are an innovative solution to cybersecurity problems. They can be used to analyze threats, prevent and predict attacks, and accelerate the internal processes of the system. And I, in turn, hope that this article was useful to many users who wanted to dive into the topic of innovative cybersecurity methods.

List of literature:

[1] *Taleb, Nassim Nicholas (2007),* The Black Swan: The Impact of the Highly Improbable, Random House, ISBN 978-1400063512.
[2] *Флориан Трамер, Фан Чжан, Ари Juels, Майкл К. Рейтер, Томас Ristenpart,* Кража моделей машинного обучения с помощью API прогнозирования
[3] *Ян ГудФеллоу, Николас Papernot, Сэнди Хуан, Ян Дуан, Питер Аббел и Джек Кларк:* Атакуя машинное обучение с состязательные примеры
[4] *Сатья Наделла:* Партнерство будущего
[5] *Claburn, Thomas:* Google troll-destroying AI не может справиться с опечаткой
[6] *Марко Баррено, Блейн Нельсон, Энтони Д. Джозеф, J.D. Тайгар:* Безопасность машинного обучения
[7] *Wolchover, Натали:* Этот пионер искусственного интеллекта имеет несколько проблем
[8] *Конн, Ариэль:* Как мы выравниваем искусственный интеллект с человеческими ценностями?
[9] *Смит, Брэд:* Необходимость срочных коллективных действий, чтобы держать людей в безопасности в Интернете: Уроки кибератаки на прошлой неделе
[10] *Николас Карлини, Пратьуш Мишра, Тавиш Вайдья, Юаней Чжан, Мика Шерр, Клей Шилдс, Дэвид Вагнер, Венчао Чжоу:* Скрытые голосовые команды
[11] *Фернанда Виегас, Мартин Уоттенберг, Даниэль Смилков, Джеймс Векслер, Джимбо Уилсон, Никхил Торат, Чарльз Николсон, Google Research:* Big Picture