Application of Artificial Neural Network Technologies for Detection Denial of Service Attacks

Denis V. Soloviev[1], Yuri A. Gatchin[2], Vladimir I. Polyakov[2]

[1]*The Bonch-Bruevich University of Telecommunications, Bol'shevikov, 22/1, St. Petersburg, 193232, Russia*
[2] *ITMO University, Kronversky Pr. 49, bldg. A, St. Petersburg, 197101, Russia*

Abstract
The main purpose of distributed denial of service attacks (DDoS-attacks) is to lead the information system equipment to a state when it cannot serve legitimate users due to its limited resources. It is implemented by a virus infection of ordinary users' networks or smart IoT-devices by the subsequent inclusion of such computers and devices to a Botnet, which will after become a source of massive distributed DoS-attack. This article describes a method of early detection of such attacks using artificial neural network (ANN) algorithms. The structure of an automated neural network system for detecting attacks on an information system is reviewed.

Keywords 1
DDoS-attacks, artificial neural networks, DDoS-attacks detection, automated neural network system for detecting attacks.

1. Introduction

Practice shows that distributed denial of service attacks are a serious tool in the hackers hands. The successful result of that attack is in the money and reputation loss for victim organization. Also it is possible when DoS-attack is a background for another serious cybercrime like data thief [1]. It's not secret that there are loads of long time launched web-sites that allow to order a DoS-attack in the Internet. Almost every internet-user can create a personal account on such a web-site and control the of the DoS-attack strength, time distribution, and other parameters. At the attack beginning the hacker scans the network looking for potential future participants for the distributed DoS-attack and include them into the Botnet [2]. The participants are called the "zombie" computers. Chosen unprotected network hosts are included into the Botnet by exploiting vulnerabilities in software, for example, vulnerabilities in the operating system, application programs, data transfer protocols, Internet browsers, and others.

While playing online games an ordinary network users usually become Botnet members. When root access to a remote machine is achieved a hacker installs trojan-program that runs in the background, being completely invisible to ordinary computer users. This trojan software waits for a command to launch a DDoS-attack. In addition with the development of IoT-devices, smart-devices can also be sources of a distributed denial of service attack. The hackers do not even need to exert much effort to receive full remote access to IoT-devices. These IoT-devices either work with default unchanged administrator password or have extremely weak passwords which can received by brute-force method in a maximum several hours [3-5].

2. Denial of service attacks types

Russian Advances in Fuzzy Systems and Soft Computing: Selected Contributions to the 10th International Conference «Integrated Models and Soft Computing in Artificial Intelligence» (IMSC-2021), May 17–20, 2021, Kolomna, Russian Federation
EMAIL: 9218964588@mail.ru (A-1); gatchin1952@mail.ru (A-2); v_i_polyakov@mail.ru (A-3)

There are several types of denial of service attacks exist.

1. HTTP-flood. This type of DoS-attacks is based on overflowing the server internet-channel bandwidth using a lot of ping requests. It is the most primitive mechanism and is effective only if the server's communication channel is much tiny than the attacker's channel.

2. ICMP-flood. The most dangerous type of DoS-attacks and leads to negative consequences in almost 100% of cases. The essence lies in the use of an amplifying network through which a ping request is broadcast. The victim server address is indicated in the address of the sender of such a request. As a result of such attack all network hosts will send a response to the incoming request, overloading the resources of the victim server.

3. UDP-flood. This type of attack is similar to the ICMP-flood, but the UDP-protocol is used as the transport protocol. The result of the attack is almost complete overloading of the channel bandwidth and denial of service to legitimate users.

4. SYN-flood. This type of DoS-attacks is based on the peculiarities of establishing TCP-connections and is called "three handshakes" method. SYN packets are sent to the victim server with a fake non-existent address of the packet's sender. Such fake requests will never be reacted on, resulting a connection being queued and finally overflowing the server's network buffer. By performing thousands of requests hacker will make a network buffer overflow on the remote host, which lead to server system failure.

5. DoS-attacks by heavy requests. The purpose of such DoS-attacks is to overload the processor (processors) of the remote host with heavy computations. Calculations of complex mathematics in cycles of hundreds of thousands of iterations are used as such loads.

3. The experiment process

It was experimentally found that it is completely useless to analyze all incoming traffic to DoS-attack detection and it is enough to analyze attack signatures. For example, for denial-of-service attacks, for which the transport protocol is TCP, it is sufficient to analyze some fields from the headers of IP-packets. It was experimentally found that the most optimal for analysis are the fields in the IP-packet: "Identification" (ID), "Flags (FL)", "Source IP" (SIP), "Source port number" (SPN) and "Destination port number" (DPN). All IP-packets of DoS-attack generated by hacker are highly fragmented, have some identical source IP-addresses with the same destination and source ports, which led us to choice these fields for analysis and training samples formation. However, in some articles [6-7], it was proposed to analyze 55-bytes of IP-packet, in which 5-bytes is from the header (IP-address with port number) and 50-bytes of payload, which in our opinion is a difficult computational task which requiring large computing resources and a long time to obtain a high-quality solution. Analysis the first 50-bytes of the payload (the first 50-bytes of the IP-packet body) in our opinion will not indicate DoS-attack but will only require additional computational power.

Next we proceeded to select the structure of the artificial neural network (ANN) and the learning algorithm that are most suitable for our task. In the process of the article analysis [7-8] we was decided to use the multilayer perceptron structure with a one hidden layer. The sigmoid function for neurons activation for the hidden layer we use. We use back-propagation algorithm for ANN learning. The ANN structure is shown in Figure 1.

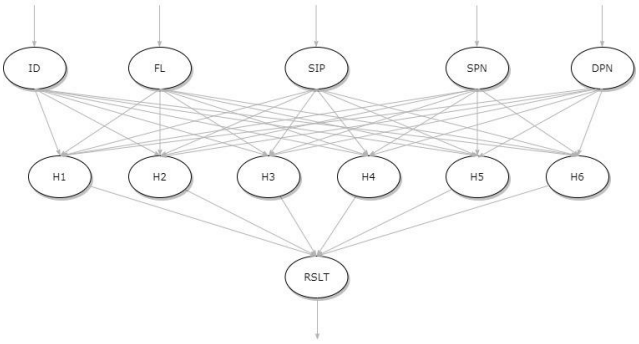

Figure 1: The ANN structure

The ANN structure consists of five neurons in the input layer (neurons: ID, FL, SIP, SPN, DPN), 6 neurons in the hidden layer (H1-H6) and one neuron in the output layer (RSLT). Due to the use of the sigmoid function as an activation function for the neurons of the hidden layer the input data ID, FL, SIP, SPN, DPN were normalized to the (0,1) interval. The signal from the output neuron determined to us the presence (1) or absence of DoS-attack (0). In the hidden the number of neurons layer was selected experimentally and it was found that 6 neurons are optimal for obtaining a high-quality solution in a reasonable time.

The experiment virtual stand was assembled and shown in Figure 2. All experimental data were collected on one computer using VM Workstation tools. A virtual machine running Ubuntu Server OS with an Nginx web-server was used as a victim server. A Kali Linux virtual machine with a tool for stress testing web-servers like SlowHTTPTest was used as an hacker's machine. We also created a virtual machine running the Ubuntu Desktop OS to monitor the effectiveness of the attack and to record network traffic.

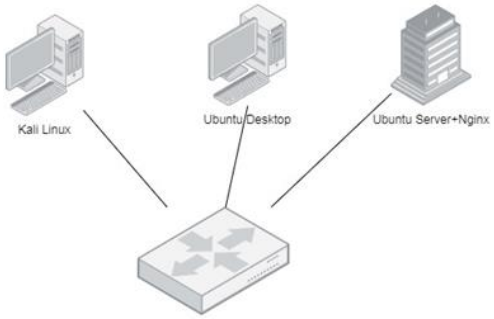

Figure 2: The experimental stand structure

In the beginning the "Slowloris" attack was launched from the Kali Linux virtual machine to generate DoS-traffic and then we generate legitimate traffic. The traffic was recorded and analyzed using the Wireshark. Then a training sample was formed. The training sample was a data array of 1000 rows by 6 columns. The sample was formed from the recorded traffic by taking data from required fields of the IP-packet and converting from hexadecimal to the decimal number system with normalization to the (0,1) interval. Each odd line of the training sample contained data extracted from the infected DoS-traffic and each even line contained data from legitimate internet-traffic. It was decided to use 85% of the sample for training ANN and 15% for testing. After training the ANN on a sample of 850 rows it detects infected traffic with a 97% probability.

4. Automated neural network attack detection system

We have developed the structure of an automated neural network system for detecting denial of service attacks (ANSOA). The structure is shown in Figure 3. The attack detection module is the main neural network computing unit in this structure. It identifies the type of denial of service attack and forms a solution to remove attack in real time. Also it forms recommendations for the server's system administrator and enter DoS-attack traffic data into the system's knowledge base. The tracking module works with the network interface directly and takes data from the server's event log. The main aim of the response module is to develop control action to attacked server. That action leads to leveling the consequences of the DoS-attack. The data management module needs to store the data of system functioning in ANSOA database. The control module implements the control and coordination with all of ANSOA modules.

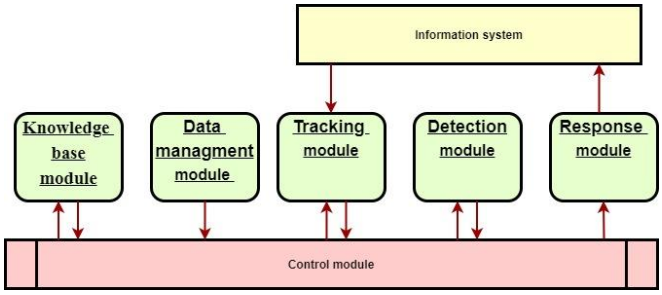

Figure 3: The ANSOA structure

5. Conclusion

Distributed denial of service attacks are an extremely dangerous type of DoS-attack. Successful proceeding of DDoS-attacks is dangerous for people and organizations and leads to financial and reputational losses. Artificial intelligence (AI) technologies in general and artificial neural networks in particular allow to solve problems that cannot be mathematical formalized.ANN ia an effective tool for detecting such anomalies as "infected" network traffic by DoS-attack. The results of our work describe the possibility of developing and successful using ANSOA for DoS-attacks detecting and loss reduction after it proceeding.

6. Acknowledgements

We express our deep gratitude to professor Igor A. Zikratov, the dean of the ISiT-faculty of the Bonch-Bruevich University of Telecommunications, for supporting our work.

7. References

[1] Report of "Kaspersky Lab": "DDoS attacks in the IV quarter of 2020" [Electronic resource]. - Access mode: https://securelist.ru/ddos-attacks-in-q4-2020/100469/ (date of access: 11.04.2021).

[2] Article of the "Free Wikipedia Encyclopedia": "Botnet" [Electronic resource]. - Access mode: https://en.wikipedia.org/wiki/Botnet (date of access: 11.04.2021).

[3] Article "Habr": "Hacking cameras: attack vectors, vulnerability search tools and protection against surveillance" [Electronic resource]. - Access mode: https://habr.com/ru/company/ivideon/blog/443462/ (date of access: 04/11/2021).

[4] Article "Cnet": "Why it was so easy to hack the cameras that took down the web" [Electronic resource]. - Access mode: https://www.cnet.com/how-to/ddos-iot-connected-devices-easily-hacked-internet-outage-webcam-dvr/ (date accessed: 04/11/2021).

[5] Izvestia article: “Hackers got access to 15 thousand CCTV cameras in Moscow” [Electronic resource]. - Access mode: https://iz.ru/1079917/2020-10-29/khakery-poluchili-dostup-k-15-tysiacham-kamer-nabliudeniia-v-moskve (date of access: 04/11/2021).

[6] Tarasov Ya.V., Abramov E.S., Tumoyan E.P. A neural network method for detecting low-intensity denial-of-service attacks // Izvestia SFedU. Technical science. - 2016.S. 58-71.

[7] Tarasov Ya. V. Investigation of the use of neural networks for detecting low-intensity DDoS attacks of the applied level // Cybersecurity Issues. 2017. No. 5 (24). S. 23-28.

[8] Saied A., Overill R.E., Raszik T, Detection of known and unknown DDoS attacks using Artifical Neural Networks // Neurocomputing. 2016.172. P. 385-393.