DOS/DDOS-ATTACKS DETECTION BY THE AID OF ARTIFICIAL NEURAL NETWORKS METHOD

***Natalya Evglevskaya**, Ph.D, Military Telecommunication Academy named after the Soviet Union Marshal Budienny S.M., n.evglevskaya@gmail.com;*
***Andrey Privalov**, Dr.Sc., professor, of St. Petersburg State Transport University of Emperor Alexander I, aprivalov@inbox.ru.*

УДК 004.051

Annotation. In the article there are DoS/DDoS-attack interpretation and its main patterns. Method of DoS/DDoS-attacks detection by the aid of artificial neural networks (ANN) is proposed and explained. The authors present the chosen architecture of ANN, input parameters, output parameter, training method and algorithm, activation function. For DoS/DDoS-attacks detection the abnormal detection technology is considered.

Keywords: DoS/DDoS-attack; artificial neural network; training method; testing; parameter; limit; priority.

Introduction

Computer DoS/DDoS attacks are the most dangerous destructive information impacts. The effectiveness of single DoS-attacks is not too great, distributed attacks (DDoS) produce much larger effect.

Reasons for the expansion of computer attacks of this type are the simplicity of their implementation, exhaustive information about the implementation algorithm, low requirements for knowledge and computing resources of the hacker [1].

The multilevel information protection system includes a number of independent barriers; it allows to provide the trusted safety of the telecommunication object, if hacker uses any vulnerabilities.

In the context of development and expansion of the Internet of Things (IoT), a number of botnets grows. The botnets are stronger, the hackers use IoT-devices more often to realise the most powerful DoS/DDoS-attacks.

DoS-attack is an attack, leading to the blocking of information processes in the system.

If the attack is carried out simultaneously by the aid of great number of computers, they talk about a distributed attack (Distributed Denial of Service, DDoS) [2].

According to statistics, compiled by Arbor Networks and Verisign Inc companies, resources that were subjected to this type of attacks, were unavailable for 5 hours in 46% of cases, and in 23% of cases the period of unavailability of the resource/service stretched for 12 hours and more [3].

Now the classifications of DoS/DDoS-attacks, proposed in literary sources [4 - 8], summarize attacks for public networks as Internet, have no classification patterns of data systematization, are not informative enough, are private in generalization and are not a strict scientific classification of DoS/DDoS-attacks.

There are a lot of DoS/DDoS attacks; their combinations are used, in such a way, to implement 99% of all DoS/DDoS attacks in the world.

The main areas of these attacks are:

- channel capacity;
- network protocol stack vulnerabilities;
- applications vulnerabilities [9].

For the moment the following types of DoS/DDoS-attacks are known:

1. ICMP flood.

2. Ping flood.
3. UDP flood.
4. DNS flood.
5. VoIP flood.
6. Media data flood.
7. NTP flood.
8. SIP register flood.
9. SIP client call flood.
10. TCP SYN flood.
11. SYN-ACK flood.
12. HTTP flood.
13. ICMP fragmentation flood.
14. UDP fragmentation flood.
15. Fragmented ACK flood.
16. ACK and PUSH ACK flood.
17. RST/FIN flood.
18. Recursive HTTP GET flood.
19. Random recursive HTTP GET flood.
20. Single request HTTP flood.
21. Single session HTTP flood.
22. SSL garbage flood.
23. Misused application attack.
24. Faulty application attack.
25. SSDP DDoS-attack.
26. Teardrop attack.
27. Ping of death.
28. Fragmented HTTP flood.
29. Smurf attack.
30. Fraggle attack.
31. Dummy DHCP- clients.
32. Land attack.
33. DNS amplification Attack.
34. NTP amplification attack.
35. IP Null attack.
36. TCP Null attack.
37. Fake session attack.
38. Multiple SYN-ACK fake session attack.
39. Multiple ACK fake session attack.
40. Type of service flood attack.
41. SIP malformed attack.

As a result of the generalization of presented DoS/DDoS-attacks, they can be described in the following way:

- attacks, realized by sending a large number of packets/requests to the target device by hacker;
- attacks, realized by sending packets with maximum permissible size to the target device by hacker;
- attacks, realized by sending requests with temporary source address by hacker;
- attacks, realized by sending requests by hacker, in response to which data with high volume are received;
- attacks, realized by sending requests by hacker with the wrong structure.

Possible consequences of DoS/DDoS-attacks implementation may be:

- partial resource starvation;
- complete resource starvation.

The analysis result of the realization algorithms of different types of DoS/DDoS-attacks by hacker allows to confirm that the generalized patterns of this attacks type are:

- network traffic extent;
- capacity decrease of attacked device;
- processor load;
- disk space load;
- random access memory load;
- capacity decrease of link channels;
- multiple connection requests [10].

It should be noted that such the DoS/DDoS-attacks pattern as «Disk space load» correlates with «Random access memory load» and «Processor load». Such the DoS/DDoS-attacks pattern as «Capacity of attacked device» correlates with «Network traffic extent».

Analysis of works in the field of artificial neural networks (ANN) [11] has shown that the main lines of researches and practical applications are:

- detection of audio images;
- detection of visual images;
- translations of text etc.

It should be emphasized that the ANN usage is the method of the task solution. Therefore, as usual, all lines of researches in the field of ANN are the way of applying the ANN method to solve a particular task.

It is known that a neuron is a computational unit, that receives information, produces simple calculations over it and transmits it further. Figure 1 shows a simple model of the neuron. On the left side you can see a biological neuron, and on the right side - a classic presentation of an artificial neuron. In this case, the input signals are identified X_1, X_2, X_3, ... , X_n, each signal is multiplied by corresponding weight and arrives at the measured adder, then by the means of the activation function we get an output neural signal.

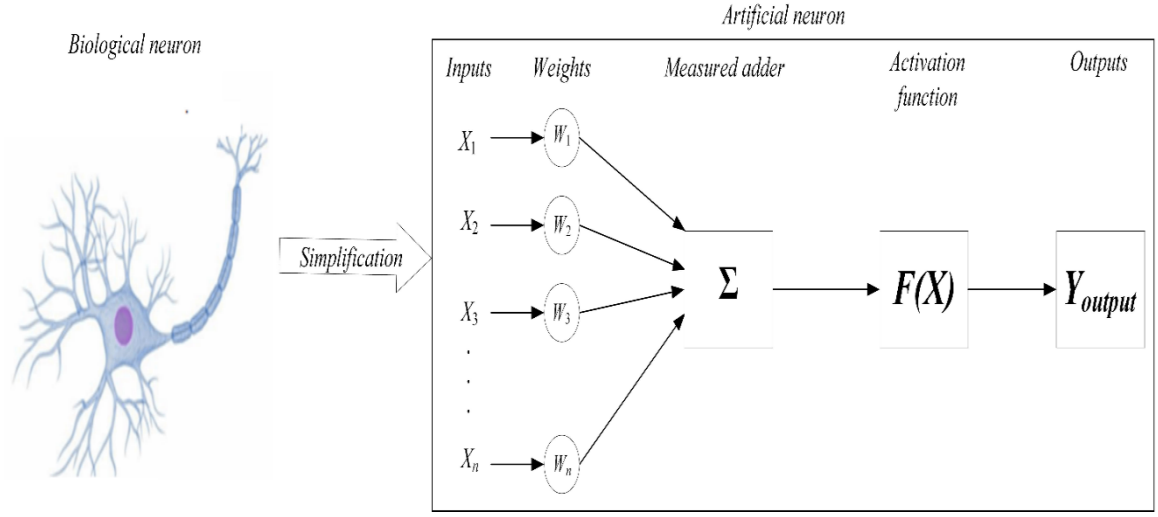

Figure 1

Figure 2 presents a simple diagram of ANN, one of the components of which is a neuron presented in the figure 1.

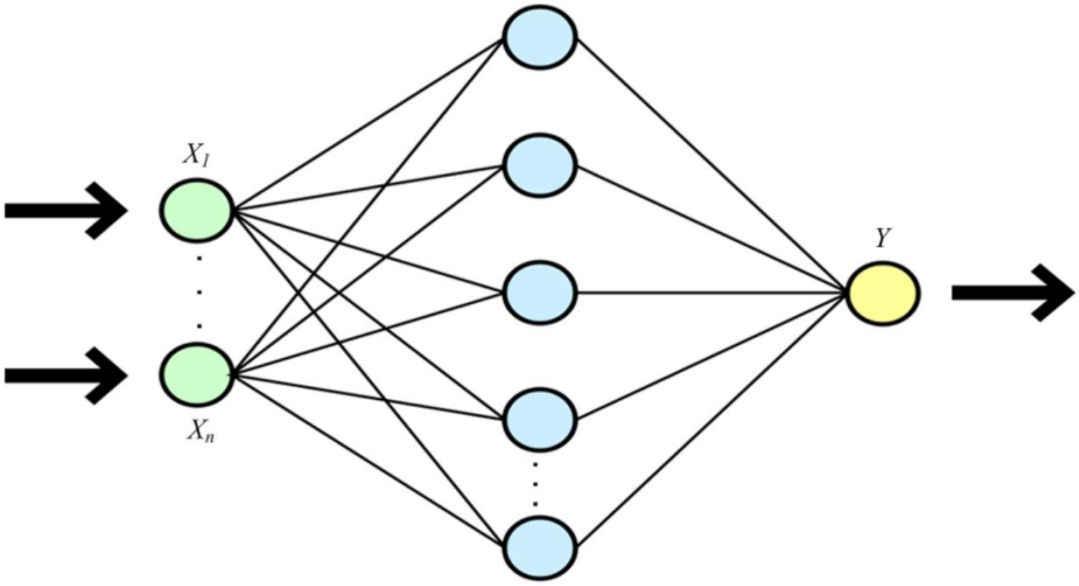

Figure 2

Neurons are divided into three main types: input (green), hidden (blue) and output (yellow). When a neural network consists of a large number of neurons, they use the term hidden layer. So, there are input layer that receives information, hidden layers (or one hidden layer) that process information and output layer that displays the result.

Using ANN method for DoS/DDoS-attacks detection that hacker realizes against a network device is the most effective method, because it is impossible to present the dependence of output parameters on input parameters in the form of equations or algorithms.

Figure 3 shows ANN architecture for tasks solution of DoS/DDoS-attacks detection.

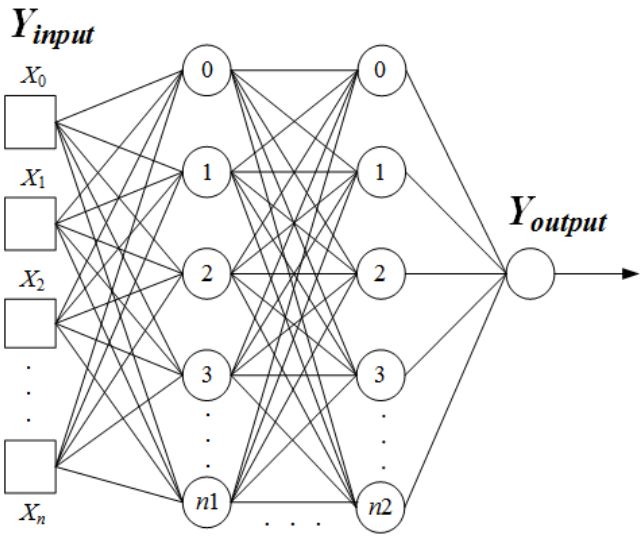

Figure 3

It is denoted in the figure: X_i – input parameters (i = from 1 to n), X_0 – bias neuron, Y_{output} – output parameter.

The ANN training method is a gradient method of back propagation of error [11].

Sigmoid function is chosen as an activation function, presented by equation (1).

$$y = \frac{1}{1+e^{-x}}. \quad (1)$$

The advantage of using this function is that it lets to calculate a derivative easy enough by the aid of equation (2).

$$y' = y \cdot (1 - y). \quad (2)$$

As the result in the output layer of ANN is known previously, the training algorithm for neural network is the training algorithm with the teacher.

Detection of DoS/DDoS-attacks demands realization of either first condition or second condition:

1) Understanding expected behavior of the attacked device.

2) Knowledge of all possible DoS/DDoS-attacks types, their varieties and collections.

In the first case the abnormal detection technology is used, and in the second case the misuse detection technology is used [12].

Let's suppose, that for DoS/DDoS-attacks detection the method based on the identification of abnormal functioning of attacked device is used. Moreover, abnormal functioning of attacked device is departure from the normal mode.

An example of abnormal functioning can be a great number of connections coming to the device during a short period of time, high processor load, a large extent of occupied random access memory, a large total extent of device network traffic [12]. All DoS/DDoS-attacks have these patterns regardless of their varieties.

However, abnormal behavior is not always an attack. So, there are two extreme cases:

1) Missing attack which is not abnormal behavior (error of first kind).

2) Abnormal behavior detection, which is not an attack (error of second kind).

As the anomalies detection metric, the acceptable limit for each of ANN input parameters was chosen. The achievement or exceedance of this acceptable limit indicates that there is DoS/DDoS-attack [12].

Besides that, it is necessary to mention, that choice of such DoS/DDoS-attacks detection metric as limited values of input parameters does not let to detect low-rate DoS/DDoS-attacks.

For detecting attacks it is necessary to rang the input parameters.

For this task solution paired comparison matrixes of hierarchy analysis method (HAM) were used as mathematical tool. Formalization of experts estimations in HAM is made by means of relative importance scale.

By the aid of received results of input parameters ranging, the priority is given each of the input parameters. The priority points at the importance degree of the parameter compared to the other parameters.

Further, in conformity with chosen input parameters, their limited values and priorities, ANN training rules have been developed.

As follows from the realized computer experiments in ANN testing it was found that as the size of the overall input sample rises, the time of ANN training increases (figure 4).

After ending of ANN training, the trained network needs testing. During testing data are supplied to ANN input, which network did not «watch» during training, and data of output parameter. In this case weight coefficients do not change during testing.

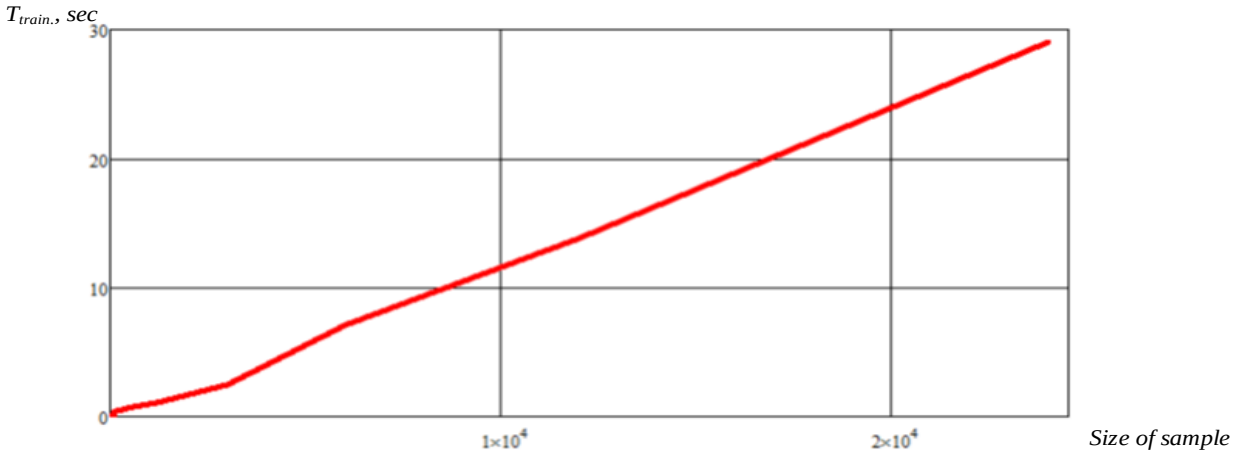

Figure 4

At the ANN output the calculated values are compared to the established values.

If the testing error does not exceed the established value, it is considered that the ANN colligates input data well and realizes the task setting before it.

Conclusion

Considering all advantages and disadvantages, DoS/DDoS-attacks detection method by the aid of ANN is the most suitable solution for information security.

Compared to another methods of computer attacks detection, the advantage of ANN usage is their capability to analyze data, even if these are incomplete or corrupted. Neural networks can learn from previous events, that allows to achieve high efficiency and adaptivity of attacks detection systems [1].

References

1. Dubonos A.S., Evglevskaya N.V., Karasenko A.O., Lauta O.S., 2020.
Obzor metodov zashchity setey svyazi spetsialnogo naznacheniya ot DDOS atak [Methods review OF dedicated networks security from DDOS attacks]. Trudy dvenadtsatoy obshcherossiyskoy nauchno-prakticheskoy konferentsii «Innovatsionnyye tekhnologii i tekhnicheskiye sredstva spetsialnogo naznacheniya» [Works of the twelfth all-Russian scientific and practical conference «Innovative technologies and dedicated technical means»]. St. Petersburg. 260-264.
2. Evglevskaya N.V., Lauta O.S., Mikhail I.I., 2019.
Obnaruzheniye DoS/DDoS-atak na osnove metoda iskusstvennyh neyronnyh setey [DOS/DDOS-attack detection on the basis of artificial neural network method]. Trudy Mezhdunarodnoy nauchno-practicheskoy conferentsii «Transport Rossii: problemy i perspectivy [Research and practical conference (International) «Russia transport: problems and prospects» Proceedings]. St. Petersburg. 421-424.
3. Chto takoye DDoS ataka. Nastroyka effektivnoy zashchity ot DDoS atak na server [What is DDoS attack. Setting up of the protection efficiency against DDoS attacks]. Available at: https://rigweb.ru/support/khosting-i-domeny/tipy-ddos-atak-i-sposoby-zashchity-ot-nikh/ (accessed November 14, 2018).
4. Bazovaya model ugroz bezopasnosti personalnyh dannyh pri ih obrabotke v informatsionnyh sistemah personalnyh dannyh [Standard threat model of personal data security when they are processed in the information systems of personal data]. Approved by Russia FSTEC Assistant Director 15.02.08. – 70 p.
5. Makarenko S.I. 2017. Informatsionnoye protivoborstvo i radioelektronnaya borba v setetsentricheskih voynah XXI veka [Information confrontation and electronic warfare

during network-centric warfares in the XXI century]. St. Petersburg: Hi-Tech Publs. – 549 p.
6. DDoS-ataki: tipy atak i urovni modeli OSI [DDoS-attacks: types of attacks and model OSI levels]. Available at: https://firstvds.ru/technology/types-of-ddos (accessed April 24, 2020).
7. Model OSI – baza znaniy DDOS-GUARD [Model OSI – knowledge base of DDOS-GUARD]. Available at: https://ddos-guard.net/ru/info/schema-osi (accessed May 13, 2019).
8. Kotsynyak M.A., Kuleshov I.A., Lauta O.S. 2013. Ustoychivost informatsionno-telekommunikatsionnyh setey [Resistibility of information and telecommunication networks]. St. Petersburg: Saint Petersburg State Polytechnical University Publs. – 91 p.
9. DDoS-ataki: tipy atak i urovni modeli OSI [DDoS-attacks: attacks types and OSI model levels]. Available at: https://firstvds.ru/technology/types-of-ddos (accessed August 12, 2020).
10. DOS i DDoS-ataki: ponyatie, raznovidnosti, metody vyyavleniya i zashity [DOS and DDoS-attacks: concept, types, detection methods and protection]. Available at: https://compconfig.ru/net/dos-i-ddos-ataki.html (accessed December 10, 2018).
11. Arhangelskaya E. 2018. Glubokoye obucheniye. Pogruzheniye v mir neyronnyh setey [Deep learning. Immersion in the neural networks world]. St. Petersburg: St. Pete Publs. – 480 p.
12. Lukatskiy A. 2000. Obnaruzheniye atak [Detection of attacks]. St. Petersburg: Cbhv Publs. – 563 c.