NOVEL METHOD FOR LOW-RATE DDoS ATTACK DETECTION

A A Chistokhodova and I D Sidorov

Information Security Department, South Federal University, 2, Chekhov Ave., Taganrog, 347922, Russia

E-mail: achis515@gmail.com, idsidorov@gmail.com

Abstract. The relevance of the work is associated with an increasing number of advanced types of DDoS attacks, in particular, low-rate HTTP-flood. Last year, the power and complexity of such attacks increased significantly. The article is devoted to the analysis of DDoS attacks detecting methods and their modifications with the purpose of increasing the accuracy of DDoS attack detection. The article details low-rate attacks features in comparison with conventional DDoS attacks. During the analysis, significant shortcomings of the available method for detecting low-rate DDoS attacks were found. Thus, the result of the study is an informal description of a new method for detecting low-rate denial-of-service attacks. The architecture of the stand for approbation of the method is developed. At the current stage of the study, it is possible to improve the efficiency of an already existing method by using a classifier with memory, as well as additional information.

1. Introduction

Growing technological capabilities, a high software customization level, an increasing complexity level of attacks on information systems lead to the fact that the structure of potential attacks becomes more and more complicated. A distributed denial of service attack (DDoS) is a serious threat to the security of cyberspace. Categories of DoS attacks and general approaches to detecting such attacks are considered in work [1]. In accordance with the research conducted by Kaspersky Lab, the DDoS attacks number is increasing [2, 3]. Fig 1 shows DDoS attacks distribution by types over the past year.

![Figure 1. DDoS attacks statistics for 2016-2017](image-url)
Fig. 1 shows that the share of simple DDoS attacks decreases, and the share of non-trivial, high-level attacks increases.

Thus, the need for reliable methods for detecting low-rate denial-of-service attacks [4] increases dramatically. The low-rate distributed "denial of service" attack has a unique ability to mask its traffic, because it is very similar to normal traffic. It may help avoid detection by existing schemes of abnormality detection. The information metric can only quantify differences in network traffic with different probability distributions.

2. The basic method for detecting low-rate attacks

Here are the properties that may indicate the low-rate DDoS attack presence in captured traffic:

- HTTP protocol payload;
- sequence of packets arriving at the network node;
- Time stamp delta between neighboring packets.

In the article [5], they proposed a method for detecting low-rate attacks. This method takes into account the first and second traffic properties and surpasses previously proposed ones in efficiency. This method cuts traffic into sliding windows. As a Kohonen network input, it uses a feature vector extracted from the network packet. Then, the Kohonen network reduces input vector dimension [6]. In fact, a single value - the winner neuron number - replaces the feature vector with 50-60 components. As an input vector for a multilayer perceptron, a sliding window or a histogram constructed by this window is used. The input vector size is determined by the sliding window size or the histogram components number. The decision block is the final block in this method. It translates the non-linear network output into one of three decisions: norm, attack, uncertainty. Fig. 2 shows the scheme of this method.

![Figure 2. A diagram of the basic method for detecting low-rate attacks](image)

Also in work [7], it is said that "... two types of pre-stored vector sets - obtained from "pure" traffic, and obtained from attacking packets are used for research", which is demonstrated by Fig. 3a.

![Figure 3a. Test data visual representation for the base method](image)

In Fig. 3a, monochrome color indicates pure traffic, and the lattice pattern indicates illegitimate traffic. These designations will be preserved further. The scale under the traffic flow is the output data from the decision block corresponding to the slashed windows. In this case, testing will be performed in more difficult conditions, where normal traffic prevails (Fig. 3b).

![Figure 3b. Visual representation of the type of test data in the proposed method](image)
Traffic, which was shown in Fig. 3b, is very close to traffic with low-rate DDoS attack. The scale breaks traffic by timestamps and demonstrates that even with a small share of illegitimate traffic - the output of the decision block will be a positive result.

3. The modified method for detecting low-rate DDoS attacks.
The proposed method for detecting a low-rate attack is based on the method described in [7], but several blocks are replaced with more efficient ones. The method described in [5,8] has the following significant drawbacks:

- limited size of the sliding window;
- if a researcher wants to change the size of the sliding window, it leads either to the re-learning of the neural IDS component if histogram is used; or to complete rearrangement of the ANN architecture if the sliding window is fed directly as the input;
- there is a growing need to increase the training set size to compensate the increased number of variants of packets permutations in the window with the growth of the sliding window length;
- during traffic generations, no samples were created in which pure traffic predominates with a minor admixture of illegitimate traffic.

Let us consider the modified method for low-rate DDoS attack recognition. Let us single out the main steps, as shown in Fig. 4.

![Figure 4](image-url)

**Figure 4.** A scheme of the proposed method for detecting low-rate attacks

1) Obtaining input data. Here it is network traffic. Captured data occur at the network level of the OSI exchange communication model. A data type is a package.

2) Network package conversion into a characteristic vector. Time marks are added at this stage.

3) Vector dimensionality decrease. This can be a principal component analysis or a self-organizing map.

4) Calculation of additional time marks for packets clustered in the same way.

5) To recognize the attack, a classifier with memory is used, which takes into account:
   - results of the Kohonen network classification;
   - additional timestamps;
   - its own hidden states.

6) Splitting the output of the network into classes: norm, attack, unclassified.

7) Formation of response. This can be a warning to the administrator, cutting off sources of attack or other measures.

In [5, 8], a shallow multilayer perceptron was used, which is not the best network architecture. At the stage of preliminary research, it was revealed that LSTM [9] - networks of long short-term memory – significantly exceed the standard neural networks for tasks similar to the authors’. This network is a recurrent one, and it is capable of learning long-term dependencies. LSTM is based on a chain of previous events - this is its normal state. Traditional neural networks do not have this
property, and it is their main drawback for such tasks. This network can also forget information from the cell state based on filters. Let us imagine, for example, that one wants to classify events over a fairly long period of time, in which any impact is important, even if it is insignificant (low-rate, as in the given case). Thanks to this kind of network, it becomes possible to increase the accuracy of attack detection. There are varieties of LSTMs, such as, for example, deep controlled recurrent neural networks (Depth Gated RNNs), presented in Yao, et al (2015) [10].

Figure 5 shows the stand architecture for modified method approbation.

![Figure 5. Stand architecture](image)

The stand for carrying out experiments to test a modified method consists of at least two separate machines. An attack simulator is physically located on one of the machines. It can perform several attack types on the target machine: slowloris, rudy and http-flood. The researcher can select the type of attack in a manual mode. Also, one of the features of attack simulator is the ability to generate the necessary traffic, simply by setting the normal traffic percentage as a parameter. In a series of first experiments, a low-rate Slowloris attack is used. On the same machine, there are the tools for monitoring the efficiency and the console associated with the artificial neural network. The target itself is located physically on another machine. Low-rate DDoS attacks mostly target the web-services, which is why the victim is a web-server. There is also a sniffer agent to gather traffic. The data from the sniffer are transferred to the console to be processed by the neural network.

4. Conclusion
The problem of detecting DDoS becomes more serious due to the low-rate DDoS attacks evolution. Low-rate DDoS attacks strongly differ from traditional DDoS-attacks, as their traffic is similar to legitimate traffic.

The article proposes a method for detecting low-rate denial-of-service attacks, which differs from the existing method [7] by using additional timestamps, as well as the usage of classifiers with memory. The classifier with memory allows researcher to store the state of the system, not limited by the sliding window. Additional timestamps will allow the classifier to detect regularities in the arrival time of similar packages.

For training and testing of the method, it is suggested to use normal traffic with a small admixture of anomalous one, which is similar to the behavior of real information systems. This will improve the quality of the training sample and reduce the number of false alarms to a minimum.

References
[1] Douligeris C and Mitrokotsa A 2004 DDoS attacks and defense mechanisms: classification and state-of-the-art Elsevier Computer Networks 44-5 643–665
[2] Khalimonenko A, Strohschneider J and Kupreev O DDoS attacks in Q4 2016 Kaspersky
security bulletin 2016

[3] Khalimonenko A, Kupreev O and Ilganaev K DDoS attacks in Q3 2017 Kaspersky security bulletin 2017

[4] Moustis D, Kotzanikolaou P 2013 Evaluating security controls against HTTP based DDoS attacks Fourth International Conference on Information, Intelligence, Systems and Applications (IISA)

[5] Abramov E S, Sidorov I D 2009 Metod obnaruzheniya raspredelyonnyih informatsionnyih vozdeystviy na osnove gibridnoy neyronnoy seti Izvestiya YuFU. Tehnicheskie nauki 11 (100) 251 154 – 164

[6] Kohonen T 2001 Self-Organizing Maps. Third, extended edition. (Springer)

[7] Abramov E S, Tarasov Ya V and Tumoyan E P 2016 Neyrosetevoy metod obnaruzheniya nizkointensivnyih atak tiya «otkaz v obsluzhivanii» Izvestiya YuFU. Tehnicheskie nauki 63 58-71

[8] Abramov E S, Tarasov Ya V 2017 Primenenie kombinirovannogo neyrosetevogo metoda dlya obnaruzheniya nizkointensivnyih DDoS-atak na web-servisyi Inzhenernyiy vestnik Dona №3 (2017)

[9] Haykin, 1999 Neural Networks: A Comprehensive Foundation. Prentice Hall, Upper Saddle River (New Jersey)

[10] Yao K, Cohn T, Vylomova K and Duh K 2015 Depth-Gated Recurrent Neural Networks 5