Method of Traffic Monitoring for DDoS Attacks Detection in e-Health systems and networks

Maksym Zaliskyi [1[0000-0002-1535-4384]], Roman Odarchenko [1[0000-0002-7130-1375]],

Sergiy Gnatyuk [1[0000-0003-4992-0564]], Yuliia Petrova [1[0000-0002-3768-7921]] and

Anastasiia Chaplits [1[0000-0002-5292-848X]]

[1] National aviation univercity, Kyiv, Ukraine, 03058

s.gnatyuk@nau.edu.ua, mzaliskyi@nau.edu.ua,
odarchenko.r.s@ukr.net, panijulia.p@gmail.com,
anastasia.chaplits@gmail.com

Abstract. eHealth is a complex system that will be gradually introduced in Ukraine over next several years . It is very efficient system that brings a lot of possibilities in the future. But there are a lot of potential problems in deployment of such protected systems. One of the most common problem is the cybersecurity provision. Cybersecurity is one of the key problems of modern society. Quickest detection of attacks on computer networks is the basis for successful operation of various spheres. This paper deals with the problem of distributed denial of service (DDoS) attacks detection procedure synthesis based on Neyman-Pearson criterion with a fixed sample size. The prerequisite for the synthesis of such procedure was the experimental study of the statistical characteristics of traffic consumption in the absence and presence of DDoS attack. The suitability of proposed procedure is confirmed both experimentally and by simulation.

Keywords: Cybersecurity, Intrusions Detection, Statistical Signal Processing, Changepoint, Distributed Denial Of Service Attack.

1 Introduction

1.1 Problem of DoS attacks

At the end of January 2018, the global media agency We Are Social and the developer of the platform for managing social networks HootSuite presented a report according to which more than four billion people around the world use the Internet. The number of Internet users by the end of 2018 amounted to 4.021 billion (53% of the world's population), which is 7% more compared to the same period in 2017 [1].

If in 2015 43% of the world population (3.2 billion people) had access to the network (in 1995 this figure was 1%), then by 2020 the Internet will be available for 60% [2].

The number of sensors and devices connected to the Internet of Things in the world in 2018 will be 21 billion, and by 2022 will exceed 50 billion, according to a study by Juniper Research [3].

At the same time, the global network is becoming increasingly dangerous, as it becomes more and more easier to organize all categories of cyberattacks on the most popular resources as well as on critical infrastructure. One of the most common attacks is threat realization directed to the denial of service (Denial of Service, DoS) [4].

The most common methods of DoS attacks are SYN-DDoS, TCP-DDoS, HTTP-DDoS. Also popular attacks are strong UDP attacks with amplification, which came into use a few years ago, but still remain relevant due to the ease of implementation, and the ability to provide tremendous power.

They are increasingly organized to block the operation of individual sites and entire information systems. With the increasing the number of devices connected to the Internet network (IoE concept – Internet of everything [5]), the threat from distributed DoS attacks (DDoS) is growing. They arise from the bot-nets – networks that consist of infected devices that are able to generate queries aimed at exhausting the resources of network devices or entire information networks.

The point of the DDoS attack is that there is a scarce resource in the victim's network infrastructure, the depletion of which causes a denial of service.

The most well-known recent attacks were aimed at exhausting the bandwidth of the site's connection to the Internet.

However, the development of broadband access technologies and cloud computing complicate this task. But, to all appearances, the intruders are not intimidated by the difficulties, and they are trying to organize more and more powerful attacks. In the spring of this year, the infrastructure of one cloud provider was attacked with a capacity of 400 Gbit / s, but more large-scale shares are possible as well [6]. In these conditions for providers, owners of information systems and simple users, it is important to determine the occurrence of the above attacks in a timely manner, and then counteract them.

1.2 DoS attacks in e-Health concept

"Electronic health" (eHealth) is a complex system that will be gradually introduced over several years. In the future, the eHealth system will enable everyone to quickly get their medical information, and to doctors - to correctly diagnose with a view of a coherent picture of the patient's health.

In Ukraine, the system will consist of a central component (CBC). It will be responsible for centralized storage and processing of information - and medical information systems (MIS), which hospitals and clinics can choose on the market and establish themselves.

Because eHealth systems are based on the use of public network solutions (mobile networks, computer networks, Internet), all the problems that may arise in them will affect and affect the work of the system as a whole. DoS attacks because of their simplicity of implementation can become widespread in these systems. At the same time, denial of access can be both a cause of both banal economic losses and even human casualties. Therefore, protection from this type of attack and their early detection is a very urgent task of the introduction of eHealth systems.

2 Modern Literature Analysis

Where automated means of attack are used, automated security measures can always be developed. In particular, some manufacturers produce special devices that can block unproductive requests. For example, such devices are in the arsenal of following companies: Cisco [7], Arbor Networks [8], CloudShield [9] and other vendors. Such solutions filter the spurious traffic at high speeds and designed primarily for providers – they should be installed not in the front of the corporate site, but as close to the source of unproductive requests.

According to the document of the National Institute of Standards and Technology (NIST, USA) SP800-94 [10], and the latest research of cybersecurity experts, intrusion detection and prevention system (IDPS) is the best way to detect DoS attacks, because IDPS is based on the method of detecting anomalies (Anomaly-Based Detection) and a method of network monitoring (Network Behavior Analysis, NBA) [11].

The task of DoS attacks detection (in this case, it is reduced to the task of classifying data) can be effectively solved using artificial neural networks. The advantage of this method is the ability to detect an attack without knowing specific signatures. However, there are also disadvantages – a large number of false signals in case of unpredictable network activity, along with time spent for the learning the system, during which characteristics of normal behavior are determined [12]. In [13] structural model for detecting slow DoS attacks proposed. In [14] are considered the issues of error reduction and early detection of DDoS-attacks by statistical methods taking into account seasonality; effective allocation of periods of seasonality.

For each of the above methods, the main parameters for analysis can be [14]: number of requests for a certain period; receipt of requests speed; number of requests from a particular source or from a particular network; number of requests to a specific destination (for a web server this is a specific script); time between requests and other various network activity parameters. In general, the presence of DDoS attack leads to a change in the structure of the consumed traffic. In other words, the stationarity of observed process is disturbed. Therefore, the problem of intrusions detection can be considered as problem of quickest changepoint detection. The theory of changepoint detection was described in [15-17]. In addition, in [17] the authors gave an example of the application of CUSUM and Shiryaev-Roberts procedures for detection of network anomalies. Paper [18] presents five methods for changepoint detection: density-estimation-based changepoint detection, density-ratio-estimation-based changepoint detection, clustering-based changepoint detection, hybrid changepoint detection. Authors showed that hybrid method performs best for different types of changepoints.

Another example of CUSUM algorithm to detect cloud DDoS flooding attacks was considered in [19]. Detection accuracy for different traffic flows for this method varies within 76-100 %. Comparison between two of the most promising anomaly detection methods (CUSUM-based and entropy-based) was presented in [20]. In [21] authors declared that additional to CUSUM entropy approach improves detection efficiency and detects attacks with high probability and low false alarms.

Papers [22, 23] deals with DDoS attack detection using artificial intelligence techniques. According to [23] accuracy for this method of intrusions detection is about 94%. Paper [24] concentrates on computer tool with complete environment of network and attacks on the network with detection of the attacks using simulation. This research can be used to improve the efficiency of attack detection. Also the analysis of the up-to-date literature shows that there are other methods for intrusions detection, such as those discussed in [25; 26].

3 Problem statement

The practice of computer networks using shows that quickest detection of intrusions is the basis for successful operation of various industries. Fulfilled literature analysis allows us to conclude that sufficient attention is paid to the questions of detecting attacks on computer networks. There are also a large number of detection algorithms. However, the efficiency of attacks detection procedures can still be increased.

In the general case, the efficiency measure can be considered as a function of the following form

$$\mathrm{Ef} = f(t_\mathrm{d}, D, P_\mathrm{fa}, U, C / \vec{A}),$$

where $\vec{A}$ is a set of algorithms for statistical data processing, t_d is a time interval from the moment of the beginning of the attack to the moment of its detection, D is a probability of correct detection, P_fa is a probability of false alarm, U is a computational requirements for the correct operation of the detection algorithm, C is function of penalties due to late detection of an attack or false detection.

The function $f(\cdot)$ must establish such dependence that its maximum should be equal one if probability of correct detection is one and $t_\mathrm{d} \to 0$. If $D \to 0$, P_fa increases, and t_d increases, the function $f(\cdot)$ must decrease to zero.

The purpose of this paper is the synthesis of such algorithm for detection of attacks on computer networks, in which the maximum efficiency measure is provided for the given requirements on the parameters D, P_fa, t_d and U. In other words, it is necessary to provide

$$\mathrm{Ef} = \sup\left(0 \le \mathrm{Ef} \le 1 \ \forall \vec{A} : t_\mathrm{d} \le t_\mathrm{d}^*, D \ge D^*, P_\mathrm{fa} \le P_\mathrm{fa}^*\right),$$

where t_d^*, D^*, P_fa^* are requirements on the parameters.

It should also be noted that the basis for the synthesis of the algorithm for detecting attacks will be the experimental study described below. The analysis of the detection algorithm will also be performed by statistical modeling.

4 Experimental Study

In this research study the following network was designed (Fig. 1). This network consists of four laptops, server-laptop, router and switch.

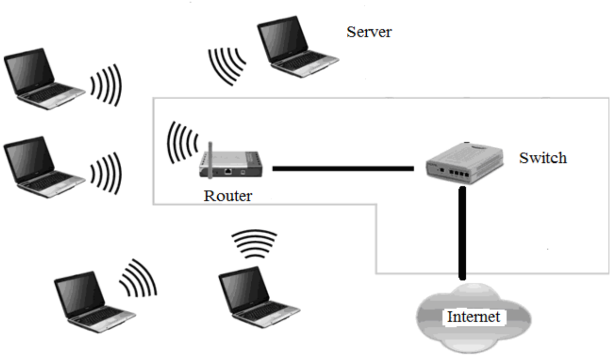

Fig. 1. Network architecture.

To analyze the traffic, the Wireshark program was used.

After starting to capture traffic, Wireshark captures network packets in real time and displays them in the user interface window. The example of packet transfer time series in the local network during 5 minutes in case of information presence without DDoS attacks is shown in the Fig. 2.

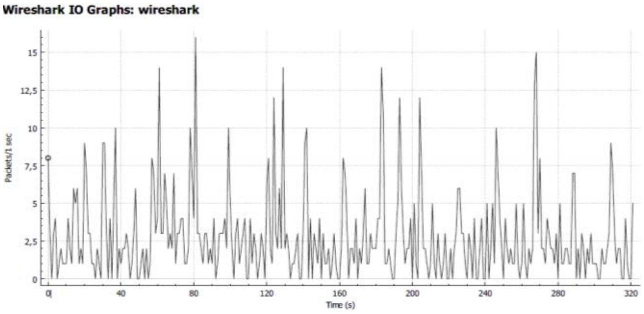

Fig. 2. Analysis of network traffic during 5 minutes without DDoS attacks.

Let’s consider the simulation procedure for a possible DDoS attack on the server. To do this, we will ping our server from four laptops at the same time, thereby simulating a ping flood attack. The DDoS attack is carried out in such way: we pass the packet of 32 bytes to the server and receive an average response of 20 ms TTL (time to live). In the general case we sent 118 packages from each attacking laptop.

The example of packet transfer time series in the local network during 6 minutes in case of DDoS attacks presence is shown in the Fig. 3. On the graph we can see increasing in the number of packets per second, which means the beginning of the attack, and the decrease in the number of packets, that signs the end of the attack.

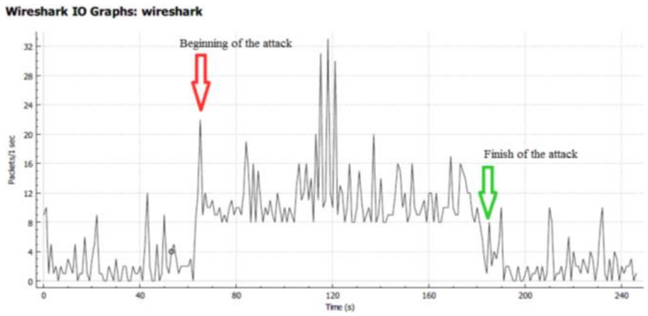

Fig. 3. Analysis of network traffic during 6 minutes in case of DDoS attacks presence.

5 Detection procedure synthesis

Synthesis of the procedure for attacks detection we can perform on the basis of Neyman-Pearson criterion. In this case, we assume that the sample has a fixed size n.

The initial data for the analysis are the results of measurements of the traffic packets per second x_i obtained using Wireshark program. We suppose that x_i is a random variable with independent values described by an identical probability density function (PDF) in case of attacks absence. In order to determine the nature of the probability density function for x_i, we use the results of an experimental study. An example of an experimentally obtained PDF for the case of five minutes of traffic monitoring without attacks is shown in the Fig. 4.

Mean quantity of traffic packets per second is equal to 2.71. Let's check the hypothesis about the exponential distribution of random variable x_i. To do this we use chi-square test.

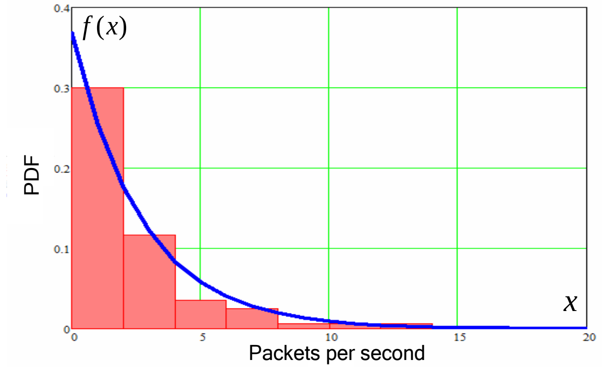

Fig. 4. Experimentally obtained PDF of traffic packets per second in case of attacks absence.

During calculation the last four intervals were combined into one. So, following value was calculated

$$\chi^2_{\text{calc}} = 10.236,$$

and this value is less than threshold value $\chi^2_{\text{th}} = 11.341$, so the hypothesis about exponential PDF is accepted with a significance level equal to 0.01.

Accordingly, the probability density function of traffic packets per second for considered example is the following

$$f_0(x) = 0.369 e^{-0.369x} h(x),$$

where $h(x)$ is Heaviside step function.

An example of experimentally obtained PDF for the case of two minutes of DDoS attacks is shown in the Fig. 5.

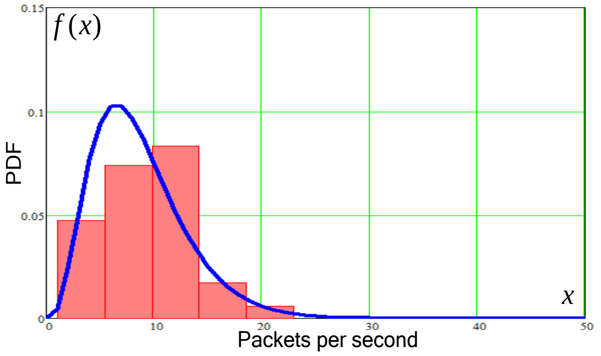

Fig. 5. Experimentally obtained PDF of traffic packets per second in case of attacks presence.

To determine the nature of PDF in the Fig. 5, the following assumption was made. In the case of attack from a single computer, the traffic flow PDF is exponential. In our experiment, an attack was carried out from four computers. Therefore, the experimentally obtained PDF can be represented as a sum of four exponentially distributed random variables. Such PDF is described by chi-square distribution. For this particular case one attack was characterized by exponential distribution with parameter $\lambda = 0.462$. So, PDF in the Fig. 5 can be described by following equation

$$f_1(x) = 7.563 \cdot 10^{-3} x^3 e^{-0.461x} h(x).$$

Let's check how experimental data coincide with PDF $f_1(x)$. According to chi-square test we can obtain

$$\chi^2_{\text{calc}} = 10.403,$$

and this value is less than threshold value $\chi^2_{\text{th}} = 11.341$, so the hypothesis about PDF $f_1(x)$ type is accepted with a significance level equal to 0.01.

According to Neyman-Pearson criterion we can write the likelihood ratio

$$\Lambda(x_i, n, k, \lambda) = \frac{\Phi(x_i / \mathrm{H}_1)}{\Phi(x_i / \mathrm{H}_0)},$$

where $\Phi(x_i / \mathrm{H}_1)$ is a likelihood function for alternative H_1 (there is DDoS attack in the traffic flow); $\Phi(x_i / \mathrm{H}_0)$ is a likelihood function for hypothesis H_0 (the traffic flow doesn't contain DDoS attack).

Likelihood functions can be represented as

$$\Phi(x_i / \mathrm{H}_1) = \prod_{i=1}^{n} f_1(x_i / \mathrm{H}_1)\,,$$

$$\Phi(x_i / \mathrm{H}_0) = \prod_{i=1}^{n} f_0(x_i / \mathrm{H}_0)\,.$$

According to obtained experimental results we can write

$$f_0(x_i / \mathrm{H}_0) = \lambda e^{-\lambda x_i} \ \text{ for } \ \forall\, i \in [1, n]\,,$$

$$f_1(x_i / \mathrm{H}_1) = \begin{cases} \lambda e^{-\lambda x_i}\,, \text{for } \ \forall\, i \in [1, k-1], \\ \dfrac{\lambda^4 x_i{}^3}{6} e^{-\lambda x_i}\,, \text{for } \ \forall\, i \in [k, n], \end{cases}$$

where λ is a parameter of exponential PDF of traffic flow without attacks, k is a time moment when the attacks begin.

Then

$$\Lambda(x_i, n,\ k, \lambda) = \frac{\prod\limits_{i=1}^{n} f_1(x_i / \mathrm{H}_1)}{\prod\limits_{i=1}^{n} f_0(x_i / \mathrm{H}_0)} =$$

$$= \frac{\prod\limits_{i=1}^{k} \left(\lambda e^{-\lambda x_i}\right) \prod\limits_{i=k}^{n} \left(\dfrac{\lambda^4 x_i{}^3}{6} e^{-\lambda x_i} \right)}{\prod\limits_{i=1}^{n} \left(\lambda e^{-\lambda x_i}\right) \prod\limits_{i=k}^{n} \left(\lambda e^{-\lambda x_i}\right)} = \frac{\prod\limits_{i=k}^{n} \left(\dfrac{\lambda^4 x_i{}^3}{6} e^{-\lambda x_i} \right)}{\prod\limits_{i=k}^{n} \left(\lambda e^{-\lambda x_i}\right)} =$$

$$= \prod_{i=k}^{n} \left(\frac{\lambda^3 x_i{}^3}{6} \right) = \frac{\lambda^{3(n-k+1)}}{6^{n-k+1}} \prod_{i=k}^{n} x_i{}^3.$$

Logarithm of likelihood ratio

$$\ln \Lambda(x_i, n,\ k, \lambda) = \ln\left(\frac{\lambda^{3(n-k+1)}}{6^{n-k+1}} \prod_{i=k}^{n} x_i{}^3 \right) = = (n-k+1) \ln \frac{\lambda^3}{6} + 3 \sum_{i=k}^{n} \ln x_i.$$

Let $\theta_j = \ln \Lambda(x_i, n,\ j, \lambda)$ for є $\forall\, j \in [1, n]$ is a decisive statistic. So

$$\theta_j = (n - j + 1) \ln \frac{\lambda^3}{6} + 3 \sum_{i=j}^{n} \ln x_i\ .$$

It should be noted that the statistics θ_j correspond to the so-called CUSUM algorithm. In addition, to avoid the uncertainty of the logarithmic function in the decisive statistics, all zero packets measurements were replaced by ones.

Decision-making scheme was accepted as follows. Each sample of the decisive statistics θ_j is compared with the threshold V. The threshold was calculated by statistical modeling in such a way that to provide a given probability of correct detection D at a certain level of DDoS attacks intensity. The decision about DDoS attack presence is taken at decisive statistics first exceeding the threshold. If $\theta_j \geq V$, then we make decision about DDoS attack detection and otherwise about its absence.

6 Detection procedure analysis

To assess the accuracy of DDoS attacks detection, let's perform an analysis of considered procedure. Fig. 6 presents the realization of decisive statistic for data shown in Fig. 3.

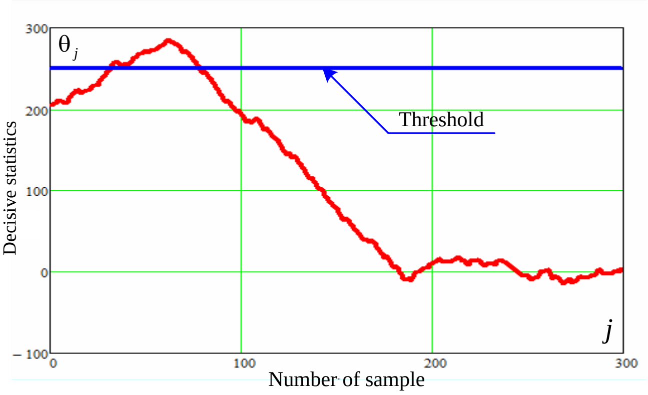

Fig. 6. Realization of decisive statistic in case of DDoS attacks presence.

As can be seen in the Fig. 6, the decisive statistics θ_j exceed the threshold V. Therefore, we make the correct decision about the presence of DDoS attack in the traffic flow. In addition $\max(\theta_j)$ corresponds to time moment of attack beginning.

It should be noted that the analysis of such procedures with further estimation of unknown parameters was considered by the authors in [27; 28].

To construct the operating characteristic, the simulation was used. The obtained dependence of probability of correct detection of intrusions on the quantity of attacking computers is shown in the Fig. 7.

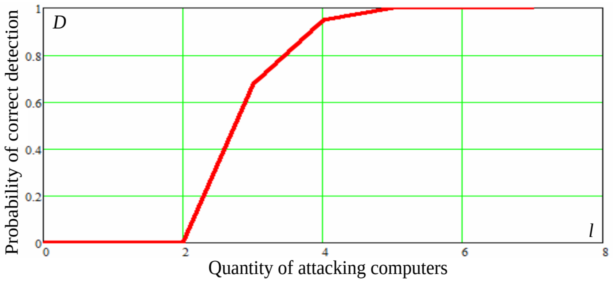

Fig. 7. The dependence of probability of correct detection of intrusions on the quantity of attacking computers.

Conclusion

eHealth is a complex system that will be gradually introduced over several years. It is very efficient project that will bring a lot of possibilities in the future. But there are a lot of potential problems in development and deployment of such high-level protected systems. One of the most common problem is the huge amount of DoS attacks in the Internet. DoS attacks can damage servers, storages etc. That's why it is very important to develop novel methods of Traffic Monitoring for DDoS Attacks Detection in e-Health systems and networks.

The problem of synthesis and analysis of the procedure for DDoS attacks detection was considered in this paper. The synthesis of the detection procedure was carried out on the basis of Neyman-Pearson criterion. The analysis was performed by simulation. The proposed procedure for attacks detection can be considered as a type of CUSUM algorithm. Maximum of decisive statistic corresponds to time moment of attack beginning.

The simulation results showed that the detection procedure has high accuracy at low computational capability. In the considered example, the probability of correct detection is 0.95 in case of attacks from four computers and approximately 1 in case of attacks from five computers and probability of false alarm $P_{\text{fa}} \to 0$. The requirements for t_{d} can be provided by using online calculations in the moving window by selecting the appropriate sample size.

The results of the research study can be used for various computer network systems security against DDoS attacks.

References

1. McDonald, N.: Digital In 2018: World's internet users pass the 4 billion mark, – We Are Social USA (2018) https://wearesocial.com/us/blog/2018/01/global-digital-report-2018 last accessed 20/10/2018
2. ICT Facts and figures 2017 (2017) https://www.itu.int/ en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf last accessed 20/10/2018
3. IoT Connections to grow 140% to hit 50 billion by 2022, as edge computing accelerates ROI (2018) https://www.juniperresearch.com/press/press-releases/iot-connections-to-grow-140-to-hit-50-billion last accessed 20/10/2018

4. DDOS attack scripts (2018) https://www.incapsula.com/ddos/ddos-attack-scripts.html last accessed 20/10/2018
5. Internet of Everything (2018) https://newsroom.cisco.com/ioe last accessed 20/10/2018
6. Roberts, A.: Public cloud service definition, Version 2.9 (2018) https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/vcat/vmware-public-cloud-service-definition.pdf last accessed 20/10/2018
7. Configuring denial of service protection (2018) https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/dos.pdf last accessed 20/10/2018
8. Arbor Networks DDoS attack protection solutions (2017) https://www.netscout.com/sites/default/files/2017-09/SB_DDoSAttackProtection_EN.pdf last accessed 20/10/2018
9. Protect against DDoS attack (2018) https://www.cloudflare.com/ddos/ last accessed 20/10/2018
10. Scarfone K., Mell P.: Guide to Intrusion Detection and Prevention Systems (IDPS) Recommendations of the National Institute of Standards and Technology (2007) https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf
11. NIST Special Publication 800-94. Guide to Intrusion Detection and Prevention Systems (2007)
12. Cannady, J., Mahaffey, J.: The Application of Artificial Neural Networks to Misuse Detection: Initial Results. In: 1998 National Information Systems Security Conference (NISSC'98), pp. 443-456. Arlington (1998)
13. Ruban, I.V., Pribylnov, D.V., Loshakov, E.S.: Method of Identifying a Low-speed Attack of Type «Failure to Maintenance». Science and Technology of the Air Forces of the Armed Forces of Ukraine, 4 (13), 85-88 (in Russian) (2013)
14. Ternovoi, O.S., Shatokhin, A.S.: Early Detection of DDoS Attacks by Statistical Methods Taking into Account Seasonality. Mathematical substantiation and theoretical aspects of information security, 1 (25) Volume 1, 104-107 (in Russian) (2012)
15. Zhyhlyavskyi, A.A., Kraskovskyi A.E.: Changepoint Detection of Random Processes in Problems of Radio Engineering, St. Petersburg: LU Publishing, 224 p. (in Russian) (1998)
16. Shiryaev, A.N.: Stochastic Problems about Changepoint, Moscow: MCNMO, 392 p. (in Russian) (2016)
17. Tartakovsky, A., Nikiforov, I., Basseville M.: Sequential Analysis. Hypothesis Testing and Changepoint Detection, New York: Taylor & Francis Group, 580 p. (2015)
18. Jin, S., Zhang, Z., Chakrabarty, K., Gu, X.: Changepoint-based Anomaly Detection for Prognostic Diagnosis in a Core Router System. IEEE Transactions on computer-aided design of integrated circuits and systems, pp. 1-14 (2018)
19. Osanaiye, O., Choo, K.-K.R., Dlodlo, M.: Change-point Cloud DDoS Detection using Packet Inter-arrival Time. In: 8th Computer Science and Electronic Engineering (CEEC), pp. 204-209. Colchester (2016)
20. Callegari, A., Pagano, M., Giordano, S., Berizzi, F.: CUSUM-based and Entropy-based Network Anomaly Detection: an Experimental Comparison. In: 8th International Conference on the Network of the Future (NOF), pp. 132-134. London (2017)
21. Özçelik, İ., Brooks, R.R.: Cusum - Entropy: An efficient Method for DDoS Attack Detection. In: 4th International Istanbul Smart Grid Congress and Fair, pp. 1-5. Istanbul (2016)
22. Zhang, A., Zhang, T., Yu, Z.; DDoS Detection and Prevention based on Artificial Intelligence Techniques. In: 2017 3rd IEEE International Conference on Computer and Communications (ICCC), pp. 1276-1280. Chengdu (2017)
23. Hsieh, C.-J., Chan, T.-Y.: Detection DDoS Attacks based on Neural-network using Apache Spark. In: International Conference on Applied System Innovation (ICASI), pp. 1-4. Okinawa (2016)
24. Mishra, V.P., Shukla, B.: Development of Simulator for Intrusion Detection System to Detect and Alarm the DDoS Attacks. In: International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS), pp. 803-806. Dubai (2017)

25. Alsirhani, A., Sampalli, S., Bodorik, P.: DDoS Attack Detection System: Utilizing Classification Algorithms with Apache Spark. In: 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), pp. 1-7. Paris (2018)

26. Conti, M., Gangwal, A., Gaur, M.S.: A Comprehensive and Effective Mechanism for DDoS Detection in SDN. In: IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 1-8. Rome (2017)

27. Solomentsev, O., Zaliskyi, M., Nemyrovets, Yu., Asanov, M.: Signal Processing in case of Radio Equipment Technical State Deterioration. In: Signal Processing Symposium 2015 (SPS 2015), pp. 1-5. Debe (2015)

28. Solomentsev, O., Zaliskyi, M., Kozhokhina, O., Herasymenko, T.: Reliability Parameters Estimation for Radioelectronic Equipment in Case of Change-point. In: Signal Processing Symposium 2017 (SPSympo 2017), pp. 1-4. Jachranka Village (2017)