Detection of Slow DDoS Attacks Based on Time Delay Forecasting

Vitalii Savchenko[1], Valeriia Savchenko[2], Oleksandr Laptiev[3], Oleksander Matsko[4], Ivan Havryliuk[5], Kseniia Yerhidzei[6] and Iryna Novikova[7]

[1,2] *State University of Telecommunications, Solomianska str.7, Kyiv, 03110, Ukraine*
[3]*Taras Shevchenko National University of Kyiv, 24 Bogdana Gavrilishina str., Kyiv, 04116,Ukraine,*
[4,5,6,7] *The National Defense University of Ukraine named after Ivan Cherniakhovskyi, Povitroflotsky av. 28, Kyiv, 03049, Ukraine*

Abstract

The article deals with the problem of detecting low and slow distributed DDoS attacks. Detecting such DDoS attacks is challenging because slow attacks do not significantly increase traffic. The authors suggest that detecting slow DDoS attacks will be effective based on analyzing and predicting host response latency in the network. The article proposes an original method for detecting such attacks, based on statistics of host interaction and predicting the individual trajectory of the traffic parameter behavior. The host response time delay is taken as a traffic parameter. An algorithm for calculating the individual trajectory of the time delay is proposed. The possibilities of using this method are shown based on the simulation of RUDY attacks on HTTP services. The parameters of the forecast accuracy are investigated depending on the accumulated information on the response delays.

Keywords

Slow and low DDoS attack**s**, slow attack detection, network response prediction, latency, individual trajectory**.**

1. Introduction

Recently, DDoS attacks are rapidly increasing in scale, frequency and technical complexity. For organizations that rely on Internet resources and applications for their activities (for example, for e-commerce enterprises), the consequences of DDoS attacks can be devastating. Inaccessible websites and servers can cast a shadow on a company's reputation and customers turn to competitors' resources [1].

One type of DDOS attack is slow denial of service attacks. Their feature is that denial of service is achieved in a hidden way using a small amount of traffic and does not require bandwidth filling. The attacker opens many endless connections and, when a certain threshold is exceeded, causes a denial of service in the victim's network. It uses transport (TCP) or application (HTTP) protocols. Detection and countermeasures must be built based on the characteristics of the attack.

Countering such attacks should include two main measures: 1) diagnose the attack at the earliest stages; 2) separate malicious traffic from normal traffic. By understanding which user requests are the result of a DDoS attack, you can configure appropriate settings for firewalls, routers, or implement other security measures.

III International Scientific And Practical Conference "Information Security And Information Technologies", September 13–19, 2021, Odesa, Ukraine
EMAIL: savitan@ukr.net (A. 1); savchenko.valeriya@gmail.com (A. 2); alaptev64@ukr.net (A. 3); macko2006@ukr.net (A. 4); ivan.havryliuk@gmail.com (A. 5); ergidzey@ukr.net (A. 6); irina_nov@ukr.net (A. 7)
ORCID: 0000-0002-3014-131X (A.1); 0000-0003-1921-2698 (A. 2); 0000-0002-4194-402X (A. 3); 0000-0003-3415-3358 (A. 4); 0000-0002-3514-0738 (A. 5); 0000-0003-4634-133X (A. 6); 0000-0003-4854-0682(A. 7)

1.1. Problem Statement

Methods for detecting slow DDoS attacks fall into two categories:

1. Signature methods, which are based on the construction of a model of "abnormal behavior" [2]. This model builds signatures of "abnormal" traffic behavior (a huge number of simultaneously arriving SYN + ACK packets, an inadequately long packet lifetime, too long a packet route "length", and so on). The model is most effective against attacks that fill the network bandwidth, or on local networks, where you can make a list of source addresses whose packets are guaranteed to be "normal". But such a model is ineffective against low-intensity DDoS, when it is difficult to reliably distinguish ordinary user requests from “malicious” ones.

2. Based on anomalies. This method is the opposite of signature. A general model of "normal" behavior is built, then the incoming traffic is compared with it, and if the differences exceed an acceptable threshold, an "alarm" is triggered. Research is conducted in the areas of statistical (parametric and nonparametric) methods, as well as data mining and neural networks. The last two approaches are being actively developed to detect low-intensity attacks. Disadvantages of the model: a large number of errors of the first kind due to the individuality of networks and traffic; long-term calculation of data on "normal" behavior; sensitive to the choice of statistical distributions.

In any case, the problem of early detection of low or slow DDoS attacks remains relevant. The sooner the traffic parameters are found to be inconsistent with their normal values, the faster it will be possible to take measures to neutralize the attack. In this case, it is necessary to add parameter prediction modules to the existing detection systems.

1.2. Related Works Overview

There is a huge number of publications on the detection of slow DDoS attacks.

Reference [3] proposes an architecture that mitigates low and slow DDoS attacks by leveraging the capabilities of a software-defined infrastructure. At the same time, this approach requires a significant amount of computing resources, which will be involved in diagnostics.

The article [4] proposes a methodology for detecting LDDoS attacks based on the characteristics of malicious TCP streams by classifying them by decision trees. The studies are conducted using a combination of two datasets, one generated from a simulated network and the other from a publicly available CIC DoS dataset. Since this approach includes elements of artificial intelligence, a significant amount of statistics is required to train the system.

In [5], the authors tried to measure the impact of different variants of pulsating distributed denial-of-service attacks on the self-similar nature of network traffic and see if changing the H index can be used to distinguish them from a normal network. This approach is quite effective in the case of traffic self-similarity elements. Otherwise, detecting low and slow DoS attacks is very difficult.

Paper [6] proposes Canopy, a novel approach to detecting LSDDoS attacks by using machine learning techniques to extract meaning from observed TCP state transition patterns. At the same time, as in other models based on artificial intelligence, the detection system requires a large sample of training and significant resources for processing the results.

The work [7] compares machine learning methods for recognizing slow DDoS attacks: multilayer perceptron (MLP), backpropagation neural network, K-Nearest Neighbors (K-NN), Support Vector Machine (SVM) and polynomial naive Bayesian (MNB) algorithm. As in the previous cases, the application of the methods requires a large number of patterns for recognition.

In [8-9], a new classification method and model is proposed to protect against slow HTTP attacks in the cloud. The solution detects slow HTTP header attacks (Slowloris), slow HTTP body attacks (RUDY), or slow HTTP read attacks. At the same time, such approaches do not guarantee effective detection of attacks at the early stages of their development.

The papers [10-11] show a system that can detect and mitigate attacks in the network infrastructure. The main identification parameters in both models are the packet transmission rate and the uniform distance between packets, which does not allow to forestall the actions of intruders. Reference [12] discusses sampling data to create different class distributions to counteract the effects of highly imbalanced slow HTTP DoS datasets. At the same time, a significant number of samples (the authors use 1.89 million copies of attacks) in reality is quite difficult to achieve. The study [13] developed a metric-based system for detecting traditional slow attacks, which can be effective with limited resources, based on the study of similarities and the introduction of the Euclidean metric. This approach is only effective enough for a large number of such slow attack patterns, and for a large variety of such an approach is unlikely to be effective.

The most practical for implementation is the method proposed in [14,26], which determines the quality parameters of TCP connections, typical for slow HTTP attacks. This allows you to estimate the likelihood and time of the web server going into overload mode. However, such attack detection is based on observation statistics and uses predictions. The article [15] proposes an algorithm for detecting slow DDoS attacks based on traffic patterns depending on the server load state. This does not consider the decision-making process. In [16], various scenarios are considered and a hybrid neural network for detecting DDoS attacks is proposed. However, the method and general technique for detecting low intensity DDoS attacks are not considered. In [17], the authors consider interval forecasting based on a probabilistic neural network with a dynamic update of the smoothing parameter. But the problem of the dynamics of the model remains unresolved.

Thus, most of the works devoted to countering slow DDoS attacks are based on statistical models, do not address the issues of predicting host behavior, and therefore are not effective enough to detect attacks at early stages.

The aim of this work is to form a system for detecting slow DDoS attacks based on predicting traffic elements in the network. To successfully solve the identified problem, it is necessary to build a model and technology for predicting the behavior of traffic parameters taking into account the history of host interaction in the network, as well as to propose a technology for recognizing slow DDoS attacks.

2. Development of a method for detecting slow DDOS attacks based on predicting of traffic parameters

2.1. Determining the traffic parameter for detecting a slow DDoS attack

The most expedient for detecting slow DDoS attacks is the architecture proposed in [18]. Such an IDS should consist of four modules: 1) traffic collection module; 2) module for calculating traffic parameters; 3) forecasting module; 4) module for classifying attacks (Fig. 1).

The system works as follows:

1. For some time, the Traffic Collection Module records the main traffic parameters required for further calculations: IP addresses of the sender and recipient; TCP window size; package arrival time.

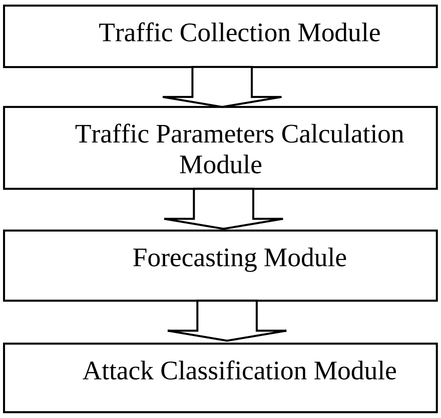

Traffic Collection Module
Traffic Parameters Calculation Module
Forecasting Module
Attack Classification Module

Figure 1: IDS structure

2. In the module for calculating traffic parameters for each IP address, the average delay between transmitted packets is calculated

$$\overline{T} = \frac{1}{k-1}\sum_{i=1}^{k}\left(t_{i+1}-t_i\right) \qquad (1)$$

where:

t_i – the *i*-th package arrival time;

t_{i+1} – the *i*+1-th package arrival time;

k – the number of packets received during the analyzed period.

The beginning and end of the session are recorded by a built-in timer, after which the duration of open connections is calculated.

3. The decision on the presence of a possible slow HTTP attack is made in the attack classification module based on the comparison of the obtained indicators with the average statistical values.

As it was shown in [18] the decision about the presence of a slow DDoS attack should be made based on the traffic parameters forecast, which can be generated based on the study of statistics in other systems. Thus, it is advisable to add a situation forecast block to the considered action algorithm.

2.2. Predicting the delay time between transmitted packets

The interaction of computer systems in the network forms an individual trajectory of changes in traffic parameters for each pair of interaction. Such trajectories have their own characteristics both in the normal mode of operation and during a slow DDoS attack. In order to start actions on time to neutralize a slow DDoS attack, it is necessary to predict the time trajectory of traffic parameters, which depends on the actions of the interacting system.

Prediction of an individual traffic trajectory has already been studied in [19], in which traffic parameters were determined at long intervals (week, month). The same approach was used to predict slow DDoS attacks in [18]. At the same time, in both cases, only direct indicators were investigated: in [19] - the amount of information per unit of time, in [18] - the average delay between transmitted packets.

Slow DDoS attacks are characterized by the fact that they are not characterized by significant deviations in traffic indicators and therefore different parameters must be used to detect them.

Along with direct indicators (the amount of information and the average delay time), when using the method of canonical decomposition of a random process, the values of the correlation function are also calculated for each of the measurements, which makes the method more effective for predicting weak disturbances.

To monitor the traffic parameters, as before in [18], it is advisable to use the average time interval of the delay between packets in the session, which can be represented as a vector of parameters $X = (X_1, X_2, ..., X_H)$ [20]. Condition fulfillment $X \in S_0$, where S_0 this is the tolerance area of the vector *X*. Random process $X(t)$ reflects the change in delays between traffic packets over time [21]. Process $X(t)$ statistically defined in the range $t \ge t_1$, where t_1 is the beginning of observations and $t_k \ge t_1$ [22].

The forecasting problem is posed as follows: for the parameter $x_\omega(t) \in S_0$, which is observed in the interval $t_1 \le t \le t_k$, determine the release time of a specific implementation $x_\omega(t)$ beyond the limits S_0 based on the definition of a posteriori process $X(t)$ [23].

The probability that a particular trajectory of a parameter ω guaranteed to fall within the acceptable range $s > t_k$, if by then t_k including his condition was described as $x_\omega(t), t_1 \le t \le t_k$ [24], will be

$$P^{ps}(s) = P\{X(s) \in S_0 / x_\omega(t)\}, \quad t_1 \le t \le t_k, s \ge t_k \tag{2}$$

To solve the forecasting problem, the process under study must be represented by the formula

$$X(t) = m(t) + \sum_{\nu} V_\nu \phi_\nu(t), \tag{3}$$

where $m(t)$ – mean function of the process;

$\phi_\nu(t)$ – non-random (coordinate) time functions;

V_ν – random, uncorrelated coefficients $M[V_\nu] = 0$, $M[V_\nu, V_\mu] = 0$, $\nu \ne \mu$.

This representation, proposed in [18, 19], allows it to be applied to any traffic parameter that can be represented as a time series. Process $X(t)$ can be written as a random sequence $X(t_i) = X(i), i = \overline{1,I}$ in a discrete series of observations t_i [25]:

$$X(i) = m(i) + \sum_{\nu=1}^{i} V_\nu \phi_\nu(i), i = \overline{1,I} , \tag{4}$$

where V_ν – random coefficient with parameters $M[V_\nu] = 0$, $M[V_\nu, V_\mu] = 0$, $\nu \ne \mu$; $M[V_\nu^2] = D_\nu$; $\phi_\nu(i)$ – non-random coordinate function, $\phi_\nu(\nu) = 1$, $\phi_\nu(i) = 0$ while $\nu > i$.

The formulas for variance and correlation function can be written as

$$D(i) = \sum_{\nu=1}^{i} D_\nu \phi_\nu^2(i), i = \overline{1,I} , \tag{5}$$

$$D(i,j) = \sum_{\nu=1}^{inf(i,j)} D_\nu \phi_\nu(i) \phi_\nu(j), \ i,j = \overline{1,I} . \tag{6}$$

Thus, the representation of random processes of traffic parameters (2) allows solving the problem of detecting a slow DDoS attack based on predicting the delay between transmitted packets.

2.3. Slow DDoS Attack detection algorithm based on delay time prediction

To detect slow DDoS attacks within the framework of approach (1) - (6), the following algorithm for predicting delays between transmitted packets is proposed.

```
0. Start
1. $X(t) \leftarrow X(t), t=\overline{1,T}$ – formation of an array of process observations $X(t)$.
2. $x(\mu) \leftarrow x(\mu), \mu=\overline{1,k}$ – formation of an array of control results.
3. $L \leftarrow Length[X(t)]$ – determining the number of trajectories observed.
4. $m(t)=Mean[X(t)]$ – calculating the mean of a random function $X(t)$.
5. $c=Covariance[X(t)]$ – calculating the covariance matrix for $X(t)$.
6. $d=Variance[X(t)]$ – calculating an array of variances of a process $X(t)$.
7. $\phi=Table[0,\{T\},\{T\}]$ – determining the initial value of the coordinate functions.
8. $\hat{X}(t)=X(t)-m(t), t=\overline{1,T}$ – centering the source data.
9. $V(t)=X_l(t)-m(t), t=\overline{1,T};\ l=\overline{1,L}$ – determination of initial values of random coefficients.
10. $\phi_1=\frac{c_{1,j}}{d_1}, j=\overline{1,T}$ – definition of the first coordinate function.
11. For $i=1$ to $i=T$
12. $d_i=c_{i,i}-\sum_{j=1}^{i-1}\phi_{i,j}^2 d_j$ – variance override.
13.     For $j=1$ to $j=T$
14.     $\phi_i=\frac{1}{d_1}\left(c_{i,j}-\sum_{l=1}^{i-1}d_l\phi_{i,l}\phi_{j,l}\right)$ – redefining coordinate functions.
15.     for j
16. for i
17. For $i=2$ to $i \le T$
18.     For $k=1$ to $k<i$
19.     $\phi_{i,k}=0$ – redefining the coordinate functions of a random process.
20.     for k
21. for i
22. For $i=2$ to $i \le T$
23.     For $l=1$ to $l=L$
24.     $V_{l,i}=\hat{X}_{l,i}-\sum_{k=1}^{i-1}V_{l,k}\phi_{k,i}$ – determination of random coefficients.
25.     for l
26. for i
27. $p_s \leftarrow Length[x(\mu)]$ – size of the array of control results.
28. $M_1=Table\left[m_i+(x_1-m_1)\phi_{1,i},\{i=\overline{1,T}\}\right]$ – determination of the initial predicted trajectory.
29. For $h=2$ to $h=p_s$
30. $M_h=Table\left[M_{h-1,i}+(x_h-M_{h-1,h})\phi_{h,i},\ \{i=\overline{1,T}\}\right]$ – calculation of forecast control points.
31. for h
32. $X_{forecast}=Table\left[M_{k,i}+\sum_{j=k+1}^{i}V_{k,j}\phi_{k,j},\ \{k=\overline{1,p_s}, i=\overline{1,T}\}\right]$ – calculation of predicted trajectory.
33. End
```

The application of the algorithm makes it possible to construct a forecast of the system response delay time and determine the moment when this parameter goes beyond the critical values. In the event that latency is classified as a slow DDoS attack, security measures must be taken. A slow DDoS attack decision must be made for each sender IP address based on a comparison of predicted latency parameters with critical values to determine when the parameter enters the critical zone. This approach takes into account the statistics of the behavior of the interacting hosts, as well as the behavior of other hosts in similar situations in the event of a slow DDoS attack.

3. Application of the algorithm for detecting slow DDOS attacks based on predicting the response delay time

Slow DDOS attack detection simulations are performed for the RUDY attack. RUDY is a network server attack designed to crash a web server by sending long requests. The attack is carried out using a tool that scans the target website and detects embedded web forms. Once the forms have been detected, RUDY sends valid HTTP POST requests with an abnormally long content-length header field, and then begins entering information, one byte per packet. This type of attack is difficult to detect due to small fluctuations in incoming traffic.

For clarity, only one case of an attack against the background of normal traffic was taken, as shown in Figure 2. The average delay between transmitted packets is considered as the parameter under study.

The prediction algorithm was applied to the process shown in Figure 2, taking as the initial observation values individual points in the time series that correspond to a partial trajectory (blue line in Figure 2). Considering this line as a control line, the first values of the time series were taken as the initial observation data, corresponding to t = 1, 30, 60 s of observations.

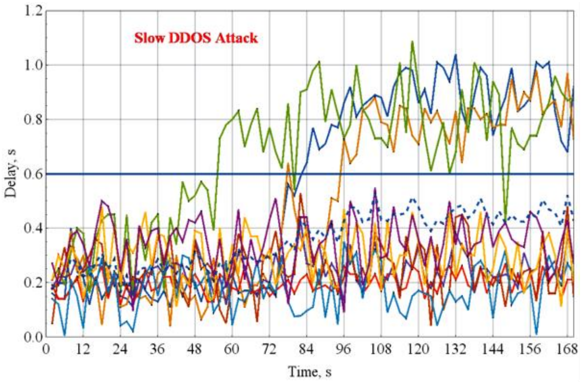
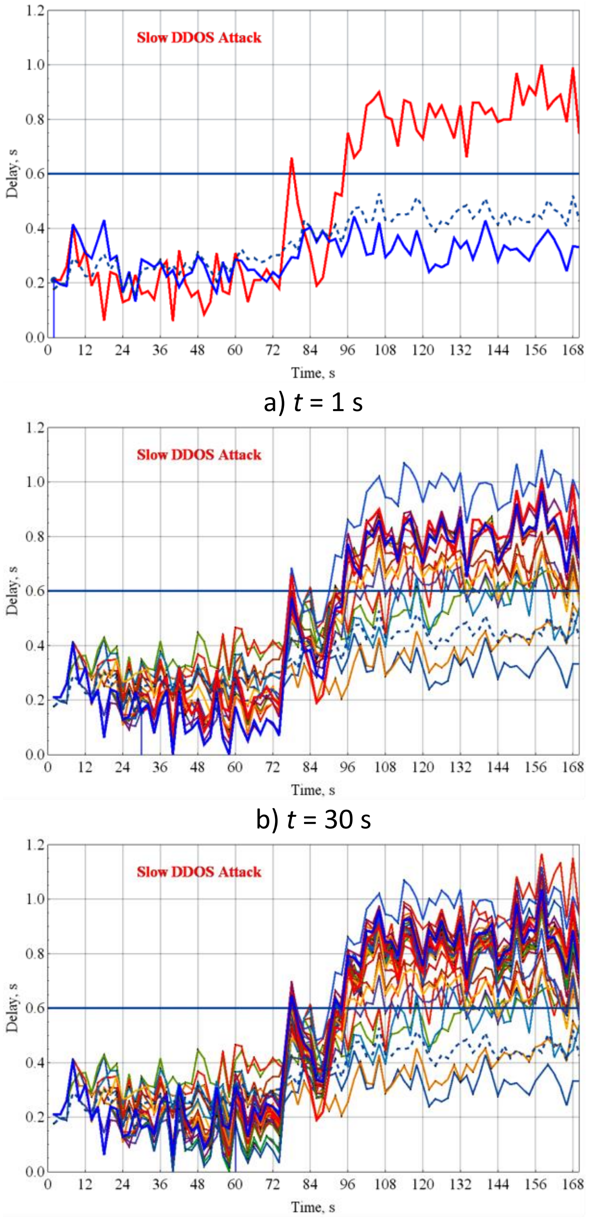


Figure 2: Traffic patterns

Figure 3a shows the forecast results for t = 1 s. Since there are few initial observational data, the process is reproduced as a whole in terms of the average value. In this case, the values of the predicted traffic in the event of an attack will be very different from the real ones (red curve).

Increasing the number of observations to t = 30 s (Figure 3b) increases the reliability of further prediction and at t = 60 s we can talk about a fairly accurate prediction $P^{ps}(s) \geq 0{,}99$. In Figure 3b and 3c curves of other colors show how forecasting will be carried out when receiving data from other control points $t_{\mu}, \mu = \overline{1,k}, k < I$, preceding the moment t_k. That is, the probability of error in choosing the correct trajectory depends on the amount of raw data observed. It is logical to assume that in this case the forecast accuracy will be too dependent on the trajectory behavior characteristics that lead to abnormal traffic, as well as on the observed frequency of anomalies. Thus, the method "selects" the required trajectory depending on the entry point and the average trajectory.

For this example, the important question is how the forecasting accuracy depends on the number of a priori observations. This issue has already been considered in [18], where it was shown that in 60...90 s the deviation of the predicted trajectory from the control one decreases to 5...0%. This confirms the adequacy of the predictive model for identifying slow DDoS attacks based on predicting network latency.



a) t = 1 s

b) t = 30 s

c) t = 60 s

Figure 3. Delay Time forecasting with observation time t = 1, 30, 60 s: — forecast value; — compared value; --- mean value

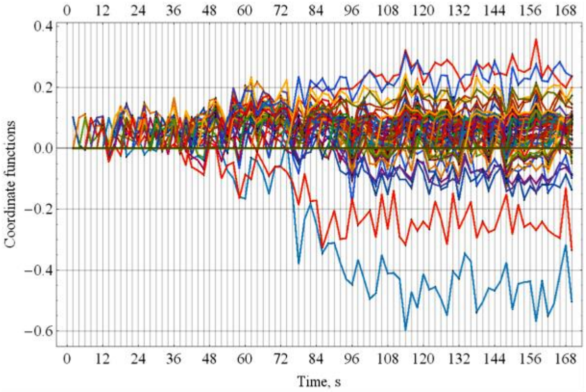


Figure 4: Coordinate functions

Even more interesting is the question of the behavior of the coordinate functions (Fig. 4). These functions are recalculated at each stage of calculating the predicted value and at the final stage are constant for a certain statistical series. They describe the relationship of the current parameter at the time of observation with its statistical data obtained during previous observations. As can be seen from Figure 3 a)–c), the coordinate functions respond to changes in the trajectory over time somewhat more than the average or forecast lines, which can be an additional factor in forecasting.

4. Conclusions

1. Low and slow DDoS attacks are difficult enough to detect due to minor changes in traffic parameters. Existing methods for detecting slow DDoS attacks require significant statistical material for training artificial intelligence systems. More promising, according to the authors, are methods based on predicting traffic parameters, in particular, the packet delay time in the network.

2. Predicting the delay time of packets in the network allows you to solve the problem of detecting slow DDoS attacks based on an algorithm for finding unknown future values for a time series of traffic parameters. The proposed method is a combination of artificial intelligence and statistical analysis and uses a self-learning algorithm provided there are sufficient attack statistics. The developed algorithm of the method makes it possible to accurately determine the random process at control points and to provide a minimum of the mean square of the approximation error in the intervals between these points.

3. Further research in the field of countering slow DDoS attacks can be devoted to the issues of forecasting at intervals that are not covered by statistics or the operation of the method in the absence of some observations or strong data noise.

5. References

[1] Enrico Cambiaso, & Gianluca Papaleo, & Giovanni Chiola, & Maurizio Aiello. (2013). Slow DOS Attacks: Definition and Categorisation. International Journal of Trust Management in Computing and Communications. 1. 300-319. 10.1504/IJTMCC.2013.056440.

[2] David Holmes. Mitigating DDoS Attacks with F5 Technology. [Electronic Resource] URL: https://www.f5.com/pdf/white-papers/mitigating-ddos-attacks-tech-brief.pdf

[3] Vasileios Theodorou, & Mark Shtern, & Roni Sandel, & Marin Litoiu, & Chris Bachalo. (2014). Towards Mitigation of Low and Slow Application DDoS Attacks. Proceedings - 2014 IEEE International Conference on Cloud Engineering, IC2E 2014. 10.1109/IC2E.2014.38

[4] Michael Siracusano, & Stavros Shiaeles, & B.V. Ghita. (2018). Detection of LDDoS Attacks Based on TCP Connection Parameters. Conference: 2018 Global Information Infrastructure and Networking Symposium (GIIS). 1-6. 10.1109/GIIS.2018.8635701

[5] Gagandeep Kaur, Vikas Saxena, J.P. Gupta, Detection of TCP targeted high bandwidth attacks using self-similarity, Journal of King Saud University - Computer and Information Sciences,Volume 32, Issue 1, 2020, Pages 35-49, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2017.05.004.

[6] Lucas Cadalzo, Christopher H. Todd, Banjo Obayomi, W. Brad Moore and Anthony C. Wong. Canopy: A Learning-based Approach for Automatic Low-and-Slow DDoS Mitigation. ICISSP 2021 - 7th International Conference on Information Systems Security and Privacy

[7] Vinícius de Miranda Rios, Pedro R.M. Inácio, Damien Magoni, Mário Freire. Detection of reductionof-quality DDoS attacks using Fuzzy Logic and machine learning algorithms. Computer Networks, Elsevier, 2021, 186,

pp.107792. ff10.1016/j.comnet.2020.107792ff. ffhal-03182934f

[8] A. Dhanapal and P. Nithyanandam. The Slow Http Distributed Denial of Service Attack Detection in Cloud. Scalable Computing: Practice and Experience. Volume 20, Number 2, pp. 285–298, 2019.

[9] A. Dhanapal_and P. Nithyanandam. The Slow HTTP DDOS Attacks: Detection, Mitigation and Prevention in the Cloud Environment. Scalable Computing: Practice and Experience. Volume 20, Number 4, pp. 669–685, 2019.

[10] T. Lukaseder, S. Ghosh, F. Kargl. Mitigation of Flooding and Slow DDoS Attacks in a Software-Defined Network. 16 August 2018. https://arxiv.org/pdf/1808.05357.pdf

[11] H. Abusaimeh, H. Atta, H. Shihadeh. Survey on Cache-Based Side-Channel Attacks in Cloud Computing. International Journal of Emerging Trends in Engineering Research. Volume 8, No.4, p.1019-1026, April 2020.

[12] L. Calvert, T. M. Khoshgoftaar Impact of class distribution on the detection of slow HTTP DoS attacks using Big Data. Journal of Big Data. 6, 67, 2019.

[13] B. Cusack, and Z. Tian. Detecting and tracing slow attacks on mobile phone user service. In Valli, C. (Ed.). The Proceedings of 14th Australian Digital Forensics Conference, 5-6 December 2016, Edith Cowan University, Perth, Australia. pp. 4-10, 2016.

[14] Ie. V. Duravkin, A. Carlsson, A. S. Loktionova. Method of Slow-Attack Detection. Information processing systems, issue 8 (124), pp. 102-106, 2014.

[15] I.V. Ruban, D.W. Pribylnov, E.C. Loshakov. A method of detecting a low-speed denial-of-service attack. Science and technology of the Air Force of the Armed Forces of Ukraine, № 4(13). 85-88, 2013.

[16] Ya. V. Tarasov. Investigation of the application of neural networks for the detection of low-intensity DDoS-attacks of the application level. Cybersecurity issues №5(24), 23-29, 2017.

[17] Y. M. Krakovsky, A. N. Luzgin. The cyberattack intensity forecasting to information systems of critical infrastructures. Problems of smart cities and sustainable development of territories. SAFETY2018, Ekaterinburg, October 4-5, 34-42, pp. 180-187, 2018.

[18] Vitalii Savchenko, Oleh Ilin, Nikolay Hnidenko, Olga Tkachenko, Oleksandr Laptiev, Svitlana Lehominova, Detection of Slow DDoS Attacks based on User's Behavior Forecasting. International Journal of Emerging Trends in Engineering Research (IJETER) Volume 8. No. 5, May 2020. Scopus Indexed - ISSN 2347 – 3983. pp.2019 – 2025.

[19] Vitalii Savchenko, O. Matsko, O. Vorobiov, Y. Kizyak, L. Kriuchkova, Y. Tikhonov, A. Kotenko. Network traffic forecasting based on the canonical expansion of a random process. Eastern European Journal of Enterprise Technologies. VOL 3, NO 2 (93). p. 33-41, 2018.

[20] Vitalii Savchenko, Viktor Zaika, Maksym Trembovetskyi, German Shuklin, Liubov Berkman, Kamila Storchak, Ihor Rolin. Composite Radioisotope Coating Parameters and Reflecting Characteristics Calculation Selection Method. International Journal of Advanced Trends in Computer Science and Engineering. Volume 8, No.5, September - October 2019. – P. 2246-2251. https://doi.org/10.30534/ijatcse/2019/60852019

[21] Vitalii Savchenko, Oleh Vorobiov, Oksana Tkalenko, Olha Polonevych, German Shuklin, Maksym Trembovetskyi, Viktor Zaika, Marianna Konopliannykova. Influense of Composit Materials Nonlinear Properties with Radioisotope Inclutions on Reflected Radiations. International Journal of Advanced Trends in Computer Science and Engineering. 2019. No.6. P. 2716-2720.

[22] Vitalii Savchenko, V. Akhramovych, A. Tushych, I. Sribna, I. Vlasov. Analysis of Social Network Parameters and the Likelihood of its Constraction. International Journal of Emerging Trends in Engineering Research. Volume 8, No. 2, p. 271-276, February 2020.

[23] Serhii Yevseiev, Roman Korolyov, Andrii Tkachov, Oleksandr Laptiev, Ivan Opirskyy, Olha Soloviova. Modification of the algorithm (OFM) S-box, which provides increasing crypto resistance in the post-quantum period. International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE) Volume 9. No. 5, September-Oktober 2020, pp. 8725-8729.

[24] Oleg Barabash, Oleksandr Laptiev, Oksana Kovtun, Olga Leshchenko, Kseniia Dukhnovska, Anatoliy Biehun. The Method dynavic TF-IDF. International Journal of Emerging Trends in Engineering Research

(IJETER), Volume 8. No. 9, September 2020. pp. 5713-5718.

[25] Oleg Barabash, Oleksandr Laptiev, Volodymyr Tkachev, Oleksii Maystrov, Oleksandr Krasikov, Igor Polovinkin. The Indirect method of obtaining Estimates of the Parameters of Radio Signals of covert means of obtaining Information. International Journal of Emerging Trends in Engineering Research (IJETER), Volume 8. No. 8, August 2020. Indexed- ISSN: 2278 – 3075. pp.4133 – 4139.

[26] Oleksandr Laptiev, Savchenko Vitalii, Serhii Yevseiev, Halyna Haidur, Sergii Gakhov, Spartak Hohoniants. The new method for detecting signals of means of covert obtaining information. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. pp.176 –181.