Monte Carlo method for solving the problem of predicting the computer network resistance against DoS attacks

V A Voevodin, D S Burenok and V S Cherniaev
Department of Information security, National Research University of Electronic Technology, Shokin sq., 1, Zelenograd, 124498, Russia
E-mail: vva541@mail.ru, corr.dmitry@yahoo.com, sergeich1997@yandex.ru

Abstract. The application of the Monte Carlo method to solving the problem of identifying and assessing the protection against DDoS attacks of weak nodes is considered. The field of research is of practical and theoretical interest, since the methods developed by the classical theory of reliability are focused on simple, stationary flows. Under the conditions of DDoS attacks, the flow of attacking requests is not stationary, so the known analytical models give an unacceptable error. For the reliability of the results, the freedom to choose the distribution function, the moments of arrival of the attacking requests, their duration and the response of the attacked node is required. The method is applicable for modelling a computer network when organizing an information security audit.

1. Introduction
The development of digital technologies of information transmission with the increasing complexity of the IT infrastructure of enterprises is one of the reasons for the growth of cybercrime [1]. One of the most common computer attacks is a denial of service attack, which purpose is to disrupt the availability of an information system for authorized users. If such an attack is carried out by several distributed sources, it is positioned as a DDoS attack [2, 3]. In 2020, the number of distributed denial-of-service attacks increased significantly, and the beginning of 2021 was marked by an increase in their intensity [4, 5]. The mechanism of this attack is to create a stream of false requests, the intensity of which exceeds the maximum resource of the server for processing requests, which leads to a failure in its operation. The source of malicious requests are distributed botnets consisting of ordinary users’ computers infected with viruses, which are able to synchronously execute commands transmitted from the control source of the attack [6]. A distinctive feature of this kind of attack is that its implementation leaves almost no legally significant evidence. There are special programs and services that can be used to organize a DDoS attack, which are actively used in unfair competition. At the same time, the costs of organizing an attack are disproportionately small compared to the possible financial and reputational losses of the attacked company. Therefore, taking measures to protect against these attacks is an urgent task of information security management bodies (IS). Along with traditional protection measures, the most reasonable and effective way to manage the risk of information security is information risk insurance [7]. However, the procedure for insuring IS risks requires an involvement of independent auditor for risk assessment [8, 9], who has appropriate methods.
2. DDoS attacks
The general classification of DDoS attacks is shown in figure 1.

![Diagram](image)

**Figure 1.** General classification of DDoS attacks.

DDoS attacks differ in their impact and in the level of implementation [10]. According to the impact, attacks can be aimed at the computing resources of a computer network, as well as at bandwidth. In the simulation, this will mean that attacks targeting bandwidth are based on a large number of requests, while their processing time is short. Attacks targeting resources form a relatively small number of complex requests to the network, but their processing time is significantly longer.

The division by implementation is determined by the level in the TCP/IP model at which the attack is carried out. The application layer corresponds to an attack on the business logic of network. There is no access to the database on the Transport and Network layer, so interaction with it cannot be simulated. Primarily web sites and file servers operating over the HTTP/HTTPS and FTP/NFS protocols. It is also possible to carry out attacks on other network applications that are accessed at this level, for example, through the API. The most common are POST and GET flood. Attacks at the transport and network level do not depend on business logic, therefore, they are easier to execute, do not require personalization for a specific network being attacked. In this case, the most common is SYN flood.

The analysis of the stress testing software tools [11, 12], as well as the tools used in practice by attackers, showed that the absolute majority of resource-oriented attacks are carried out on the Application layer. Attacks on the channel bandwidth are carried out on the Transport layer and Network layer. Figures 2 and 3 show the time graphs of some of the world's largest DDoS attacks for 2019 and 2020, passing through the Imperva CDN network. Figures 2 and 3 show the fundamental difference between Resources (Application layer) and Bandwidth (Transport and Network layer) attacks. In the first case (figure 2), the attack is based on the complexity of processing requests, in the second (figure 3) – on the speed and the number of incoming requests.
Figure 2. POST flood RPS (requests per second) graph. Peak flow about 292,000 RPS.

Figure 3. SYN flood RPS graph. Peak flow about 140,000,000 RPS.

Real customers of DDoS attacks, before paying for a long-term attack, usually order a test lasting 5-10 minutes. If the test attack is successful, the full payment is made for a certain period of time. In this regard, it is rational to simulate only the first minutes of a DDoS attack, since this is enough to assess the security of a computer network.

3. Network organization
Modern computer networks are designed linearly, with clearly allocated levels. This ensures the absence of switching loops, as well as the possibility of horizontal scaling. By increasing the number of nodes at each level, the overall network performance increases. Figure 4 shows a typical computer network diagram.

Figure 4. General computer network diagram.
The load balancer can be an external server that does not belong to the organization, including an entire network of servers, as well as an internal server of the organization. Its task is to distribute incoming requests to the network between the internal servers of the organization. For this, the Least Connections balancing method is used [13]. In the simulation, this will mean that requests will be redirected to nodes that have fewer active connections at a given time.

For modeling, a network node is represented as a server in a queuing system, and the computer network itself is represented as a queuing network [14]. Requests coming to the server can be considered as a flow of requests. The frequency of requests occurrence is characterized by arrival rate $\lambda$ and departure rate $\mu$. The ratio $\lambda$ to $\mu$ is called the load factor of the queuing system and is denoted by the letter $\rho$. In the problem under consideration, the model can be described as a multi-channel system with a limited queue and a limited waiting time in the queue [15]. Requests will be serviced according to the FIFO principle – the earlier the request is in the queue, the earlier it will be serviced and there is no request priority. Figure 5 shows a marked graph of system states, in which the state $S_0$ corresponds to the situation when all channels are free and there is no queue, the state $S_{n+i}$ shows that all $n$ channels are busy servicing requests and there are $i$ channels in the queue. The state $S_{n+m}$ corresponds to the case when all $n$ channels and $m$ places in the queue are occupied. The value of $\nu$ characterizes the intensity of the departure of requests from the queue, which corresponds to the departure of requests from the server due to exceeding the maximum time spent in it and the occurrence of the «504 Gateway Time-out» error.

The verbal service model is presented as follows. Let the server receive applications with some intensity $\lambda$. When functioning in the normal mode, the law of distribution of the input flow of these requests can be considered as Poisson for a sufficiently large period of time. The service of received requests is carried out with the intensity of $m$. Handler processes act as service channels. If all channels and places in the queue are occupied, a failure occurs, which corresponds to an overflow of the request queue on the real server and the occurrence of the «502 Bad Gateway» error.

The above description of the server in terms of queuing theory is suitable, for example, for servers with Nginx. The number of channels, the length of the queue, the maximum time spent in the queue are set in the Nginx configuration files by the parameters «worker connections», «backlog», «timeout». The Nginx request processing scheme is shown in figure 6. Many other network applications, for example, Apache, are arranged similarly.
If a DDoS attack is conducted on the Application layer, then it is important to take into account the server's access to the database. It can be located both inside a computer network, and with the involvement of cloud services and data centers. There is no access to the database on the Transport and Network layer, so interaction with it shouldn't be simulated.

There are analytical expressions that can be used to calculate the probability of finding a queuing system in each of the states, as well as the probability of failure. However, in the conditions of DDoS attacks, their use is incorrect, since in the process of modeling a DDoS attack on a server, several requests may come to the server at the same time, which violates the requirements of orderliness for the flow of incoming requests and, therefore, it can no longer be considered Poisson without rough assumptions that can lead to unacceptable erroneous results [16]. Thus, the classical tools of the theory of queuing systems are unsuitable for solving the task. The solution is to use Monte Carlo simulation modeling. Simulation modeling allows to track changes in system states over time and is well applicable for modeling random processes, such as DDoS attacks [17, 18].

4. Modeling
In general, the development of a simulation model of discrete systems with stochastic functioning, which include queuing systems, is carried out in the following order [19]:
1) setting the distribution law of a random variable;
2) generation of values of random variables with a given distribution law;
3) formation of application flows and service simulation;
4) modeling of queues of service requests;
5) processing of simulation results

An important stage in the development of a simulation model is the formation of flows, which is carried out in various ways:
- by direct enumeration of the moments of events;
- by indicating the various moments of events and the number of events that occur at each of these moments;
- by indicating the sequence of durations of time intervals between events;
- by indicating the duration of the intervals between different moments when events occur, and the number of events at each of these moments;
- by a function X(t) equal to the number of events in the interval (0, t).

Thus, the task is to simulate attacks on key nodes of the computer network, which are servers, and to assess their vulnerability to DDoS attacks. As a result of the simulation, the decision-maker receives information about the probability of server failure, sufficient to take a number of organizational and
technical measures to reduce the risk. These measures include server redundancy, improving server performance, limiting the bandwidth of the channel. In case of a high probability of server failure due to DDoS attacks, insurance may be the solution.

The issues of simulation of DDoS attacks have been considered in a number of papers. Thus, in [20] a system for simulating DDoS attacks in the OMNeT++ modeling environment on computer networks consisting of a large number of machines is presented and various protection mechanisms are also considered. In [21] simulation modeling was used at the level of network packets. As a defense, the authors proposed a bioinspired approach that includes a distributed mechanism for collecting and processing information that coordinates the actions of the main devices of a computer network. In [22], the simulation modeling of a network for testing security methods with the possibility of connecting real nodes to the test bed is considered.

The simulation model is based on the random nature of the arrival of requests at each moment of time. The further servicing of requests and the release of channels is described by using logical expressions. The percentage of successful DDoS attacks equal to the probability of server failure is calculated as the ratio of failures to the total number of requests. The parameters of the initial model are the intensity of receipt of applications $\lambda$ and the intensity of service $\mu$, the maximum waiting time for an application in the queue, the length of the queue, the number of channels, as well as the time step $dt$, which is set to 0.1 seconds. The model was tested at various values of the ratio $\lambda$ to $\mu$, which is the load factor. The analysis showed that even in a situation where the intensity of receipt of requests exceeds the intensity of service by 6.25 times, the probability of a successful DDoS attack is estimated at 51.32%, and if the intensity of receipt of requests is exceeded by 10 times, the probability of server failure increases to 70% (figure 7).

![Figure 7. The dependence of the probability of server failure on the server load factor.](image)

To assess the probability of server failure with a large number of iterations and any number of channels, a program for evaluating the server's security against DDoS attacks is used. The program accepts statistics on the receipt of requests to the server, the length of the queue and the maximum waiting for a request in the queue [23]. Request receipt statistics is loaded as an Excel file, in which the first column corresponds to the receipt of requests to the server, the subsequent columns correspond to the service of the request by the first and subsequent channels. The occurrence of the request receipt events and its service by the channel is indicated in the cell by the number 1, the opposite event is indicated by the number 0. The program outputs the probability of failure, which is calculated as the ratio of the number of refusals to the total number of requests. A distinctive feature of the software model is its versatility, due to the flexibility of changing parameters. The program has
enough computing resources for $10^6$ iterations, after which the data can be uploaded to disk. Figure 8 shows the program interface.

![Program interface](image)

**Figure 8.** Program interface.

Experiments conducted with the model showed that in conditions of high intensity of requests and a large ratio of $\lambda$ to $\mu$ ($\rho=1000$), which corresponds to a DDoS attack, the probability of failure decreases by 4-6% with an increase in the number of channels by five units (figure 9). Increasing the service queue by 100 units reduces the probability of failure by 1%. So, with an initial failure probability of 80% and a queue length equal to one, it took an increase of the queue to 3000 units to reduce the probability of failure to 50% (figure 10). The results indicate that the most effective way to reduce the probability of failure is to increase the performance of the server by increasing its service channels.

![Graph](image)

**Figure 9.** The dependence of the probability of server failure on the number of channels.
5. Conclusion
As a result of the conducted research, the expediency of using simulation modeling with the use of elements of the Monte Carlo method to assess the probability of server failure in the conditions of DDoS attacks is shown. It was concluded that the server can be considered as a queuing system, but the flow of incoming requests in the conditions of DDoS attacks is not Poisson, so the use of analytical expressions to assess the probability of failure is incorrect. The simulation allows the decision-maker to assess the probability of server failure and take organizational and technical measures to increase the level of security. Analysis of the simulation results showed the effectiveness of improving server performance by increasing service units. Thus, the developed tool will be useful in conducting an audit of the information security of an organization in the interests of insuring information security risks to justify the insurance premium. The directions of further research are to study the issue of security of a computer network, taking into account the features of a specific topology.

Acknowledgements
The work was carried out with the support of the Vladimir Potanin Charitable Foundation for Master's Degree teachers.

References
[1] Data Breach Investigations Report Available at: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf [Visited June 5, 2021]
[2] RFC 4732. Internet Denial-of-Service Considerations. 2006
[3] RFC 8612. DDoS Open Threat Signaling. 2019
[4] Report on Network security and Availability in 2020 Available at: https://qrator.net/presentations/2021/QRatorLabs_Network_Security_Availability_in_2020_RU.pdf [In Russian. Visited June 5, 2021]
[5] Denial of service: how businesses evaluate the threat of DDoS attacks Available at: https://media.kasperskycontenthub.com/wp-content/uploads/sites/45/2018/03/08234158/IT_Risks_Survey_Report_Threat_of_DDoS_Attacks.pdf [Visited June 5, 2021]
[6] Alomari E, Manickam S, Gupta B, Karuppayah S and Alfaris R 2012 Botnet-based Distributed
Denial of Service (DDoS) Attacks on Web Servers: Classification and Art. *Int. J. Comput. Appl* 49 pp 24–32

[7] State Standard GOST R 59516-2021. Information technology. Information security management. Guidelines for cyber-insurance. Moscow, Standartinform Publ., 2021 [in Russian]

[8] ISO/IEC 27102:2019. Information security management — Guidelines for cyber-insurance

[9] Makarenko S I 2018 Audit of Information Security — the Main Stages, Conceptual Framework, Classification of Types *Systems of Control, Communication and Security* (1) pp 1–29 [in Russian]

[10] C. Douligeris and A Mitrokotsa 2003 DDoS attacks and defense mechanisms: a classification. *Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology* pp 190-193, doi: 10.1109/ISSPIT.2003.1341092

[11] De Donno M, Dragoni N, Giaretta A and Spognardi A 2018 DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation *Security and Communication Networks* 2018 pp 1–30 doi: 10.1155/2018/7178164

[12] Cika P and Clupek V Stress 2019 Tester and Network Emulator in Apache JMeter. *Computer Science, 2019 Photonics and Electromagnetics Research Symposium* - Spring (PIERS-Spring) pp 3722-3726 doi: 10.1109/PIERS-Spring46901.2019.9017650

[13] Mustafa M E 2017 Load Balancing Algorithms Round-Robin (RR), Least-Connection and Least Loaded Efficiency *Computer Science and Telecommunications* 1(1) pp 25–29

[14] Hohlachev E N 2012 *Organization and Technology of Decision-Making in the Control of the System and Signal Troops. Part I. Methodological Foundations for the Development of Military Management Decisions* (Moscow: Military Academy of Strategic Rocket Forces) [in Russian]

[15] Solnyshkina I V 2015 *Queueing system theory. Textbook* (Komsomolsk-on-Amur: Komsomol'ska-Amure State University) [in Russian]

[16] Voevodin V A, Cherniaev V S and Burenok D S 2021 On the application of a simulation model for estimating the probability of server failure in the context of DDoS attacks *Proceedings of the 76-th All Russian Conference «The radio-electronic devices and systems for the infocommunication technologies»* pp 390-393

[17] Lee J L and Hong C S 2013 Nonparametric Detection Methods against DDoS Attack *Korean Journal of Applied Statistics* 4 pp 291-305

[18] Leian Ch and Xiaodong W 2020 Quickest attack detection in smart grid based on sequential Monte Carlo filtering *IET Smart Grid* 3 pp 686 – 696

[19] Aliev T I 2009 *Fundamentals of modeling discrete systems* (Saint Petersburg: SPbGU ITMO) [in Russian]

[20] Bekeneva Ya A, Shipilov N N, Borisenko K A and Shorov A V 2015 Investigation of DDoS Attacks by Hybrid Simulation *Proceedings of the 2015 IEEE North West Russia Section Young Researchers in Electrical and Electronic Engineering Conference* (Proc. LNCS 9357)

[21] Kotenko I V and Shorov A V Simulation of Protection Mechanisms Against Infrastructure Attacks Based on the ‘nervous Network system’ Approach *SPIRAS Proceedings* 3(22) pp 45-70 https://doi.org/10.15622/sp.22.3

[22] Borisenko K A, Bekeneva Ya A, Shipilov N N and Shorov A V 2015 Hybrid modeling system for DDoS attacks protection methods development and testing. *Proceedings of Saint Petersburg Electrotechnical University* 6 pp 22-29 [in Russian]

[23] Voevodin V A, Burenok D S and Cherniaev V S 2021 The program for assessing the security of the server from DDoS attacks The Certificate of on Official Registration of the Computer Program No 2021615403