Prevention of attacks with distributed denial of service for information networks of cyberphysical systems

G I Korshunov\textsuperscript{1,2}, V A Lipatnikov\textsuperscript{3}, R G Omarov\textsuperscript{3} and A G Varzhapetian\textsuperscript{1}

\textsuperscript{1}Saint-Petersburg State University of Airspace Instrumentation, 67A, Bolshaya Morskaya Str., Saint-Petersburg, 190000, Russia
\textsuperscript{2}Peter the Great St. Petersburg Polytechnic University, 29, Polytechnicheskaya Str., Saint-Petersburg, 195251, Russia
\textsuperscript{3}S. M. Budjonny Military Academy of the Signal Corps, Tikhoretsky Prospekt, 3, Saint-Petersburg, 194064, Russia

E-mail kgi@pantes.ru

Abstract. The analysis of methods for protecting information networks of cyberphysical systems from the most relevant types of attacks based on the reflection and amplification of traffic is presented. The advantages and disadvantages are revealed. The directions for the development of effective methods of protection are shown. A method for protecting information networks from attacks with distributed denial of service with prediction is proposed.

1. Introduction
An information network (IN) has been introduced to exchange data in cyberphysical systems (CPS), which must be reliably protected. Currently, core IN assets can be subject to denial of service (DDoS) attacks. Therefore, the task of finding IP protection methods in cyberspace from DDoS attacks is relevant. Usually, after the start of an attack, reactive measures are used to counter the attack [1]. The introduction of additional resources is not a sufficient measure of protection against network attacks, it is associated with the problem of changing the hardware complex at the time the attack begins, maintaining excess resources is impractical while waiting for the attack. The problem is the creation of a method for ensuring cybersecurity (CS) of assets that allows for proactive resistance to attacks with the implementation of preventive measures before the invasion begins [2]. However, when proactively counteracting attacks, the features of DDoS attacks are not taken into account.

2. Systems for protecting information networks of cyberphysical systems from DDoS attacks
Elimination of the above drawbacks is achieved by providing remote hosting services [3] using flexible technologies that allow you to increase resources as needed. However, a cloud hosting client will need to pay additional resources for processing malicious requests. Known methods aimed at preventing the attack [3-10]. Such tools involve the protection of the entire network as a whole and are usually impractical for building protection for a single end resource. Another group includes tools that work at the level of attacked applications. It can be various plug-ins or additional modules, for example, for web-servers, databases, other network services. It is determined that the real traffic path is not monitored, and the request for blocking arrives at the source whose address is indicated in the
suspicious packet as the sender's address. Attention should be paid to solving the problem of tracking features of the real traffic path, which will allow predicting the actions of the intruder and identifying preparations for the invasion [11-13]. The approach [14] does not allow full protection against DDoS attacks based on the use of the event forecasting model. The aim of the article is to increase the efficiency of detecting the start points of DDoS attacks in the early stages. To this end, it was proposed to develop a method for preventing attacks with a distributed denial of service of CFS information networks with traffic control at the required reliability based on an algorithm that takes into account deviations in the load and predicting the onset of the attack. To achieve the goal, an approach based on neuro-fuzzy networks and cognitive modeling was developed before the situation became critical. For this, an appropriate assessment of high-level risks is provided.

3. The algorithm for determining the beginning of a DDoS attack and the allocation of malicious traffic

Figure 1 shows an algorithm diagram for determining the onset of an attack and the allocation of malicious traffic. This scheme, explains the algorithm for the allocation of malicious traffic and the formation of data on the grounds of preparing the intruder for the invasion. The organization of control over blocks of data of IN protocols is carried out using formal grammars.

![Algorithm Diagram](image)

**Figure 1.** Block diagram of the algorithm for the allocation of malicious traffic CPS and forecast the onset of attack.

The ability to set a limit, after which agents will be notified, activation of necessary modules, etc., is implemented in various network tools, both software and hardware level. The approach [14, 15] has several disadvantages. Firstly, seasonality is not satisfactorily time consuming. Secondly, a risk-based analysis of the actions of violations according to the forecast for a given horizon is not provided.

It is necessary to use an assessment characterizing the current network activity to solve these problems and to establish a dynamic border relevant for the period of the possible start of an attack based on this assessment [16]. However, this approach also has a potential vulnerability due to the fact
that an attacker can gradually increase the power of a DDoS attack, while shifting the boundary of the standard deviation. It’s possible to eliminate this vulnerability by taking into account abnormal fluctuations. Let the network resource experience an abnormal daily load [17]. Each row of the matrix includes data on the number of queries. The first line reflects the data of the current timestamps, in this regard, it may not be completely filled. A stochastic model with a probability density function matching the Gaussian function is assumed. The standard deviation is calculated. If check is in the i-period, you can calculate the boundary for the i + 1 period using the value of i + 1 column. The assessment associated with the given check cycles then excludes rows that correspond to the results of preliminary studies using the Wald sequential analysis procedure [18]. The developed solutions in their entirety provide an increase in the values of timeliness indicators. The method allows you to get the choice of protection strategies against DDoS attacks. The process of the impact of DDoS attacks on IP over time can be considered as a stream of random events (attacks) with a distribution density \( w_A(t) \), and the protection measures taken by the proactive cyber-intrusion protection management body as a stream of random events with a distribution density \( w_p(t) \) [17]. It is possible to determine the value of the probability of IN protection \( P_3(T) \) as

\[
P_3(T) = \int_{0}^{T} w_3(\tau) \left[ 1 - \int_{0}^{\tau} w_A(t) dt \right] d\tau
\]

(1)

The flows of random events of the above processes have an exponential distribution, the intensities for the actions of the system administrator and the actions of the attacker are as follows: \( \lambda = 1 / T_3 \) and \( \lambda = 1 / T_A \), where \( T_3 \) is the average time required to implement the protective measures, and \( T_A \) - the average time required to carry out the attack [18]. When substituting intensity expressions, the value of \( P_3(T) \) will be equal to:

\[
P_3(T) = \frac{1}{1 + \frac{T_3}{T_A}} \left[ 1 - \exp\left(\frac{T(1 + \frac{T}{T_A})}{T_3}\right) \right].
\]

(2)

Let the set \( T \) be the set of client requests received before the attack. The set of client requests arriving after the start of the attack is the union of the sets \( H \) - malicious client requests and the set \( T_2 \) - trustworthy client requests. Thus, in order to obtain a sample characterizing malicious traffic, it will be necessary to divide the traffic received after the start of the attack into two groups. The clustering algorithm defines the strategy for implementing DDoS attacks in mixed use. The algorithm has the accuracy and high speed necessary for the primary separation. The algorithm has the accuracy and high speed necessary for the primary separation, unlike [19]. The algorithm makes it possible to distinguish two clusters and calculate them based on the characteristics of protocol data blocks. The security indicator will fall below the required value of \( P_3(T) \). The method for detecting and countering information security threats during DDoS attacks has been improved.

4. Modular hybrid time series forecasting system

Due to the modularity of redundancy, it has additional stability. This system operates as part of an intelligent risk assessment. IS risk assessment is presented in figure 3.
This system is based on three main modules that carry out the forecasting task: a neuro-fuzzy network (NFN), a fuzzy cognitive map (FCM) and a neural network (NN), which makes a final forecast. The system simultaneously processes the received information on a hybrid NFN and FCM, which increases both quantitative and qualitative characteristics, while the results of the work of these blocks pass through the verification stage, confirming the adequacy of the forecast. The terminal block, implemented by the NFN taking into account [5], gives the resulting forecast, which is input to the external processes of the lower level decision-making module, the data storage module, and the IP security status assessment module and the internal forecast assessment process. The proposed block, unlike the well-known approaches, allows you to limit the speed of processing requests by a given key or, as a special case, the speed of processing requests from one IP address.

5. Cognitive map of improving the qualitative component of the forecast of DDoS attacks and risk management

In this case, the CM allows you to qualitatively and clearly assess the impact of certain factors on risks, and the FCM determines the quantitative risk profile - the probability of their implementation. The final forecast is carried out at the FCM, which determines the results of risk treatment for a certain forecasting horizon. To improve the quality component of risk analysis and processing, it is proposed to use the CM presented in figure 3.

Figure 2. Block diagram of a modular time series forecasting system for risk assessment.

Figure 3. CM of increasing the qualitative component of the forecast of DDoS attacks and risk control.
The concept group $C_{11}$ - $C_{13}$ describes the events occurring in the IN of CPS - current parameters and changes in the settings of telecommunication equipment. Events in this group include messages about increased load on the CPU, memory and data transmission channels; signs of a broadcast storm; violations in data transfer protocols. The concept group $C_{21}$ and $C_{22}$ describes the degree to which threats exist in the IN, and $C_{31}$-$C_{33}$ describes the probability of exploiting vulnerabilities that lead to the implementation of threats. Suppose the following circumstances: lack of redundancy of telecommunication equipment; incorrect network equipment settings. The concept group $C_{41}$ - $C_{43}$ describes a decrease in the degree of ownership of the threat when using protective equipment aimed at preventing the implementation of threats. For example - protection tools, firewalls, antivirus protection. Objects of protection are the assets of the organization. The assets of the organization are represented by concepts $C_{51}$ - $C_{53}$, which describe IP objects for supporting business processes and concepts $C_{61}$ - $C_{64}$, which are non-information assets that depend on information assets. Concepts represent the degree of ownership of the implementation of the negative impact on the asset. The $C_{71}$ - $C_{74}$ concept group displays negative options for the consequences of threats and impacts on assets. DDoS attack implementation; emergency shutdown of the CPS telecommunication device; implementation of the man-in-middle attack. Concept Group $C_{81}$ - $C_{84}$ describes the necessary risk management options. Therefore, all concepts are linguistic variables (LV) of the situation factors with the described scales of their corresponding fuzzy variables. Prediction itself is carried out by means of the macrostrangular composition of the weight matrix and the vector of initial attribute increments.

The practical significance of the proposals is to increase the efficiency of providing IS, by reducing the time required to analyze and process risks based on intelligent services for protecting information from DDoS attacks.

6. Construction of a deep neuro-fuzzy classifier

To solve the analysis problem, an apparatus of fuzzy logic and neural networks was used. Five linguistic variables are created to formalize the knowledge of experts about the DDoS attack. Each of which characterizes one of the components of the parameter vector.

The fuzzy inference for determining the degree of confidence in an attack will consist of the following predicate rules:

- ИМЯ И ИНИЦИАЛОВ;
- If “Packet arrival time” is “small” and “Percentage of various external ip addresses” is “small” and “Percentage of various ports” is “small”, then “Confidence in attack” is “medium”;
- If “Packet arrival time” is “small” OR “Packet arrival time” is “medium” AND “Percentage of various external ip addresses” is “large” OR “Percentage of different ports” is “large” or “Percentage of packets with damaged headings "is" great ”, then” The degree of confidence in the attack "is” high ";
- If the “packet arrival time” is “long”, then the “degree of confidence in the attack” is “low”; Based on fuzzy inference, a fuzzy classifier was constructed with the structure shown in figure 4.
Construction of a variation series

Figure 4. Fuzzy classifier for DDoS attack detecting.

Here, the symbol \( \lor \) denotes a fuzzy OR neuron, the symbol \( \land \) denotes a fuzzy I-neuron, the symbol \( S \) denotes a classical neuron, \( X_1, X_2, X_3, X_4 \) are the corresponding inputs, and \( t\text{Little} \) (packet arrival time is short), \( t\text{Middle} \) (packet arrival time is average), \( t\text{High} \) (packet arrival time is long), \( \text{extraLittle} \) (percentage of different external ip addresses is small), \( \text{extraLots} \) (percentage of different external ip addresses is large), \( \text{pLittle} \) (percentage of different ports is small), \( \text{pLots} \) (percentage of different ports is large), \( \text{dhLots} \) (packet percentage with corrupted headers are great respectively). Thus, the constructed fuzzy classifier should determine the degree of confidence in a DDoS attack based on the data submitted to the input. This fuzzy system can be represented in the form of a multilayer neural network with direct signal propagation. A neural network that implements a fuzzy classifier will have a structure identical to that shown in figure 1. This network contains neurons of the following types: I-neurons that calculate the value of the fuzzy conjunction function, OR-neurons that calculate the value of the fuzzy disjunction, neurons that calculate the values of the membership functions of the fuzzy sets, and S-neurons that calculate the output of the fuzzy classifier. The novelty of the method for preventing attacks with a distributed denial of service of CPS information networks is determined by the fact that, in contrast to the known solutions [14, 15], it is proposed to provide protection with traffic control at the required reliability based on an algorithm that takes into account deviations in the load and predicting the onset of the attack. In addition, a cognitive map is being implemented to improve the quality component of the forecast for DDoS attacks and risk management.

7. Results and practical significance
The proposed method provides high accuracy in the classification of the current and forecasted state of the IS CPS. The developed solutions in their entirety provide an increase in the timeliness indicators. The study of the DDoS – attack model allowed us to create a method for early detection and counteraction to attacks of medium and low intensity. The method is universal, takes into account both regional features and other factors, and can be used to detect and counter attacks of various types and various capacities. It also can be used to detect abnormal data in various fields of activity. In contrast to the well-known approaches, the method of calculating CM in accordance with the dynamics of events during DDoS attacks occurring in the IP displays a qualitative component of the forecast, and an acceptable option for processing risk. The neural network provides information on the probabilistic component of CS risks. A distinctive feature of the CS control method in systems of heterogeneous networks of critical infrastructures is the prediction of risk changes in accordance with the dynamics of the intruder’s actions and changes, as well as the data accumulated earlier, which allows to increase the accuracy of the forecast and the accuracy of the risk processing method.
8. Conclusion
The basic programs for preventing DDoS attacks have been investigated, most of them are not applicable for small networks or providers. An improvement of the methodology for identifying and countering cyberphysical information security threats during DDOS attacks is proposed. Attack graphs are determined by analyzing the sequences of attacking actions of the intruder in the analyzed IP, using information about various types of possible attacks, service dependencies, network configuration, and security policies used.

Mechanisms for responding to an attack have been developed — by identifying traffic when implementing an adaptive IP with filtering-based forecasting. An intelligent traffic filtering complex is proposed.

The proposed method allows to obtain a methodology and algorithm for ensuring the security of network resources of cyberphysical systems from DDoS attacks that allow for proactive opposition directly on the side of the attacked resource.

In addition, the developed approaches do not take into account the formation of a system-analytical core for technological support of the design processes for the mathematical support of design bureaus of large-scale heterogeneous network systems that ensures compliance with security guarantees. These directions were deduced by the authors in the field of further research.

References
[1] Prevention of attacks with distributed denial of service (DDoS) Retrived from http://www.cisco.com/web/RU/products/ps5887/products_white_paper0900aecd8011e927_.html
[2] Lipatnikov V A, Tikhonov V A and Shevchenko A A 2019 Cyber security management method in critical infrastructure systems, based on intelligent information protection services Technologies for the construction of cognitive transport systems. Materials of the All-Russian scientific-practical conference with international participation pp 207–14
[3] Cisco Guard DDoS Mitigation Appliances Retrived from http://www.cisco.com / web / RU / products / ps5888 / index.html
[4] mod_evasive - protection against DOS and DDoS attacks Retrived from http://muff.kiev.ua/content/mod_evasive-zashchita-ot-dos-i-ddos-atak
[5] Module ngx_http_limit_zone_module Retrived from http://nginx.org/en/docs/http/ngx_http_limit_zone_module.html
[6] Ferguson P 2000 Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing Retrived from http://tools.ietf.org/html/rfc2827.html
[7] Li J 2002 SAVE: Source address validity enforcement protocol Twenty-First Annual Joint Conf. of the IEEE Computer and Communications Societies. Proceedings IEEE 3 1557-66
[8] Chen R, Park J M and Marchany R 2006 TRACK: A novel approach for defending against distributed denial-of-service attacks Retrieved from http://www.researchgate.net/profile/Jung-Min_Jerry_Park / publication / 228471222TRACK_A_Novel Approach for Defending Against Distributed Denial of Service_Attacks / links / 0a85e53454bbb9a d32000000.pdf
[9] Argyraki K and Cheriton D R 2009 Scalable network-layer defense against internet bandwidth-flooding attacks IEEE ACM Transactions on Networking (TON) 17 1284-97
[10] Furfaro A 2014 Modeling and simulation of a defense strategy to face indirect DDoS flooding attacks Internet and Distributed Computing Systems Conf. (Calabria, Italy) pp 263–74
[11] Navaz A S S, Sangeetha V and Prabhadevi C 2013 Entropy based anomaly detection system to prevent DDoS attacks in cloud Intern. J. of Computer Applications 62(15) 42–7
[12] Lipatnikov V A and Shevchenko A A 2016 Vulnerability control method when scaling an automated enterprise management system with integrated structure Information Systems and Technologies 2(94) 128-40
[13] Lipatnikov V A, Chepelev K V and Shevchenko A A 2019 A way to protect the computer network from intruders Patent of the Russian Federation No 2705773 vol 32 (Moscow: Rospatent)

[14] Ternovoy O S and Shatokhin A S 2012 Earlier detection of DDoS attacks by statistical methods with seasonality taken into account Notes of Tomsk State University 1/2(25) 104-8

[15] Ternovoy O S and Shatokhin A S 2012 Reducing the detection error of DDoS attacks by statistical methods when seasonality is taken into account Polzunovsky Bulletin 3/2

[16] Lipatnikov V A and Shevchenko A A 2018 Model of a distributed information network information protection system based on vulnerability control. Actual problems of information and telecommunications in science and education VII International Scientific-Technical and Scientific-Methodological Conference (SPb.: SPbSUT) pp 569-74

[17] Ternovoy O S 2013 The use of Bayesian classifier to obtain training samples in determining malicious traffic at short intervals Proceedings of the Altai State University pp 104-8

[18] Korshunov G I, Lipatnikov V A and Shevchenko A A Decision support systems for information protection in the management of the information network Proceedings of the II International Scientific and Practical Conference "Fuzzy Technologies in the Industry - FTI 2018" (Ulyanovsk, Russia) pp 418-26