energies

MDPI

Article

Method of Early Detection of Cyber-Attacks on Telecommunication Networks Based on Traffic Analysis by Extreme Filtering

Andrey Privalov [1], **Vera Lukicheva** [1], **Igor Kotenko** [2,*] **and Igor Saenko** [2]

[1] Emperor Alexander I Saint-Petersburg State Transport University, 9 Moskovsky pr., 190031 St. Petersburg, Russia; aprivalov@inbox.ru (A.P.); fireses@ya.ru (V.L.)

[2] Saint-Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS), 39, 14 Liniya, 199178 St. Petersburg, Russia; ivkote1@mail.ru

* Correspondence: ivkote@comsec.spb.ru

Received: 1 November 2019; Accepted: 12 December 2019; Published: 13 December 2019

Abstract: The paper suggests a method of early detection of cyber-attacks by using DDoS attacks as an example) using the method of extreme filtering in a mode close real time. The process of decomposition of the total signal (additive superposition of attacking and legitimate effects) and its decomposition using the method of extreme filtering is simulated. A profile model of a stochastic network is proposed. This allows to specify the influence of the intruder on the network using probabilistic-time characteristics. Experimental evaluation of metrics characterizing the cyber-attack is given. It is demonstrated how obtained values of metrics confirm the process of attack preparation, for instance the large-scaled telecommunication network, which includes the proposed method for early detection of attacks, has a recovery time of no more than 9 s, and the parameters of quality of service remain in an acceptable range.

Keywords: DDoS; detection of cyber-attacks; extreme filtering; signal decomposition; stochastic network conversion method

1. Introduction

For the period from 2019 to 2024, one of the national projects in Russia was the "Digital Economy" project, the main tasks of which were to ensure information security in the transmission, processing, and storage of data [1]. This task was fully valid for modern power supply systems and grids, especially in modern conditions, where smart electronic devices and software-defined networks are embedded in energy power infrastructures [2,3].

This fact confirms the relevance of information security and the need for diverse solutions in this area. References [4–15] describe the most common types of attacks, especially DDOS attacks. According to the Kaspersky Lab, in 2019 the total number of attacks and the number of smart attacks (i.e., attacks which require more thorough preparation and are directed on the most vulnerable network element) were increased. Moreover, despite a decrease in the average duration of DDOS attacks, the duration of smart attacks increased. The longest attacks that were employed lasted 509 h. The dynamics of the distribution of the total duration of attacks during the year had not changed much: those attacks that lasted no more than 4 hours dominate. At the same time, the cost of DDOS attacks was reduced due to their simple implementation [16]. However, if we take into account the fact that each year the implementation time of the longest attacks significantly increases (329 h in 2018 and 509 in 2019), the ever-increasing influence of these attacks on various organizations becomes obvious. Thus, the negative effect of attacks increases. Therefore, the issue of timely detection of such actions on the network in order to make decisions and minimize the consequences of the attack becomes increasingly urgent.

DDOS attacks are characterized by a sharp increase in the malicious traffic being processed. This results in denial of service to legitimate traffic [17–21]. As a result, when a DDOS attack is carried out, for example, at critical facilities, the result of such an attack will be not only financial loss and destruction of reputation, but also a threat to the life and health of the population, including the possibility of organizing a terrorist act.

To implement DDOS attacks, the intruder must fulfill training, which consists of carrying out a group of the following cyber-attacks [22]:

- Analysis of network traffic;
- Scanning of transfer protocols;
- Analysis of network and its vulnerabilities.

After carrying out this group of attacks, the attacker proceeds to the implementation of the last stage of a DDOS-attack, which is implemented faster than preparation for the attack, and which causes inevitable damage, as the decision to minimize the consequences of the attack is made after the start of its implementation. This indicates the need for early detection of this type of attacks during the cyber intelligence phase.

Currently, DDOS attacks are detected mainly by three kinds of methods: signature-based (SB), statistical analysis (SA), and machine learning (ML) [23–26]. At present, additional mechanisms are used to implement signature-based DDOS attack detection methods, for example, the fuzzy-genetic algorithms and game theory methods for performance evaluation [27], the inference mechanisms [28], and so on. This increases their effectiveness. However, signature methods are typically used for a limited number of protocols and do not allow real-time operation, which is critical when preparing un-targeted attacks. DDOS attack detection mechanisms based on machine learning use various classifiers [29,30] and deep neural networks [31] while analyzing various parameters, such as the distance between IP addresses [32], traffic entropy [33], intensity stream [34], and others. Machine learning methods tend to have high accuracy in detecting attacks. However, they require a lot of time for training. For this reason, they cannot be used efficiently for early detection of attacks. Statistical methods are usually based on various analytical models [35,36], which do not require large computational costs. For this reason, such methods can be used for early detection of attacks.

Table 1 demonstrates the main advantages and disadvantages of these cyber-attack detection methods. It can be seen that earlier detection of DDOS attacks is effective with statistical analysis methods. Given the nature of the damage caused by a DDOS attack in telecommunication networks, especially in networks of modern energy infrastructures, the possibility of early detection of DDOS attacks can increase the stability and continuity of telecommunication networks by reducing the network recovery time after the attack.

Table 1. Characteristics of cyber-attack detection methods.

##	Characteristics of Attacks	Methods		
		SB	**ML**	**SA**
1	Possibility of operation in real time mode	Yes/No	No	Yes
2	Accuracy	Middle	High	Middle
3	Possibility of early DDOS-attack detection	No	No	Yes

This paper suggests a new method of early detection of cyber-attacks (by using DDOS attacks as an example). The method suggested in the paper belongs to the group of statistical methods for attack detection. It works in real time, which is important for preparing un-targeted attacks. However, the impact of the intruder introduces some additional component into the network traffic. Using filtering methods, as well as knowing the model of the intruder's actions and their order, it is possible to identify this additional component and perform early attack detection. Therefore, one of the goals of the paper is to confirm the fact that the proposed method can significantly reduce the recovery time of telecommunication networks after DDOS attacks.

The method of early detection of cyber-attacks is suggested in the second section. The third section presents the results of experiments. The fourth section summarizes the main results and considers the direction of further research.

2. Method of Early Detection of Cyber-Attacks

Since the process of implementing a DDOS attack includes the preparation process, which in turn is a complex of attacks aimed at detecting the most vulnerable network elements, the early detection of a DDOS attack is aimed at finding the activity of the attacker that precedes the DDOS attack. This detection method is the most effective, since at the time of the start of a DDOS attack it is practically impossible to restore the network's performance due to the lack of tools to influence network elements. However, when a specific activity in the network is detected (traffic anomalies) at an earlier time, the possible consequences of an impending attack will be minimized.

The method of early detection of cyber impact on the network involves the traffic analysis in a time mode close to real, which imposes a number of requirements on the selected method, namely simplicity of mathematical calculations and small volume of the studied data.

As a method of detecting the change in traffic structure, the authors in [37,38] used the method of extreme filtering, which is based on parallel high-frequency and low-frequency filtering. The algorithm of operation within the selected method is quite simple to implement and does not require large computational costs. Therefore, it enables real-time data processing.

Let us represent the impact on the network as a time-ordered sequence of events (where the y-axis values depict the number of received packets per unit time), given as a time series, and select a time interval for analysis. The time interval must be selected so that it is equal to the time of the control cycle of the system. The selected gap is searched for extremes. Then, the operator smoothing the function by extreme alternating values:

$$y_{si} = 0.25y_{ei-1} + 0.5y_{ei} + 0.25y_{ei+1}\ , \tag{1}$$

where y_{si} is the value in the point i, relatively to which smoothing is performed, and y_{ei} is the extremum in the point i.

Then, the sign-variable component is separated:

$$y_{pi} = -0.25y_{ei-1} + 0.5y_{ei} - \ 0.25y_{ei+1}\ , \tag{2}$$

where y_{pi} is the value of sign-variable component in the point i.

Theoretical justification of extreme filtering, as well as proof that the coefficients used are the only possible ones, are given in [39].

Further calculations are made in a similar way with the "remainder" of the signal. At the first iteration, the highest frequency component is highlighted. Next, low frequency components are extracted. Thus, this decomposition procedure allows us to allocate components introduced into traffic, even minor components, to evaluate them relatively to the desired component, defined by the model of actions of the intruder and their order.

Using the given technique, in the environment of MatLab (The MathWorks, Inc., 1 Apple Hill Dr, Natick, MA 01760, United States), two variants of impact of the malefactor on the network are simulated: 1) determined, with identical intervals between phases of carrying out the attack, and 2) accidental, with accidental intervals. Let us spread out a summed signal to the making components.

During decomposition, the received components are compared to the noise (influence of the malefactor) imposed on a legitimate signal. As a desired signal, we use a random number generator with distribution of time of consistently received Internet Protocol (IP) packages to the normal law.

When modeling, we will accept the amplitude of the entered component commensurable with a signal amplitude. To define the values of sign-variable components, assessment of the sign of the received values should be made relatively mathematical expectation.

Let us apply the influence of the attacker additively to the traffic of the attacked node of the computer network.

To spread out the summed signal thus received, it is necessary to select the sign-variable components. For this purpose, values of a signal in a full form register in the form of a matrix of amplitudes and a matrix of values of the times corresponding to them. For a definition of an interval search of extrema, the values in a matrix of amplitudes are multiplied by couples consistently:

$$y_{ei} = y_{ei} \cdot y_{ei+1} \, . \tag{3}$$

Furthermore, we ran a search of negative values in the matrix. Two consecutive negative values defined the interval of the search of minima and maxima. Moreover, they correspond to intersections by function of a time axis. The maxima and minima found thus will be sign-variable extrema. The result of iteration in a full form is presented in the form of two matrixes—a matrix of extrema of amplitude and a matrix of the time points corresponding to them:

$$\begin{vmatrix} ye11 & ye12 & ye13 & \ldots & ye1n \\ yek1 & yek2 & yek3 & \ldots & yekn \end{vmatrix}, \tag{4}$$

$$\begin{vmatrix} xe11 & xe12 & xe13 & \ldots & xe1n \\ xek1 & xek2 & xek3 & \ldots & xekn \end{vmatrix}. \tag{5}$$

The results of each iteration are used to approximate cubic splines and remove the selected component from the total signal. The next iteration is performed with signal "remainder" values.

During the simulation, the time scale was set by readings (150 samples). The values analyzed at different points in time represent the number of packets transmitted over the protocol (for example, (Transmission Control Protocol (TCP)) per unit of time.

Let us assume that the violator influence happens with regular intervals between phases (a determined mode), and the volume of the entered packets in unit of time is a constant, that is it can be described by means of function with the equal periods, for example, a sinusoid. Let us impose it on a desired signal and decompose it according to the described algorithm. Let us compare initial influence to the selected component.

In Figure 1, the result received on the second iteration of decomposition is shown. This iteration has the highest coefficient of cross correlation among five consecutive iterations of one selection.

Figure 1a shows a similarity of initial influence and influence that was received by method of extreme filtering of a summed signal. Red color shows initial influence, and blue shows the selected component.

Figure 1b displays coefficient of cross correlation of two sequences discrete on time (initial and selected from a summed signal).

The analysis of this diagram allows us to draw a conclusion that on borders of the studied interval, both components have low correlation and, therefore, the reliability of detection of influence is also low. At the same time, in the middle of an interval, the coefficient of cross correlation reaches value 0.91, which demonstrates high reliability of detection of initial influence.

The diagram of a difference of functions (Figure 1c) shows a difference of amplitudes of two functions in discrete time points. It should be noted that the result of the carried-out iteration can be counted up the most reliable on an interval from 10th to the 80th counting on the general segment in 150 counting.

Let us assume further that the violator influence happens with accidental intervals between phases (an accidental mode). Then, it is possible to present this influence in the form of pulse sequences with a different frequency of following.

In Figure 2, the result of decomposition on the first iteration is shown. This iteration has the highest coefficient of cross correlation among five consecutive iterations of one selection.

Figure 2a allows us to analyze phase coincidence and amplitudes in the imposed component and selected from a summed signal. On an interval [0–60], the phase of two signals almost completely matches; their amplitudes are approximately identical. On the subsequent counting, it is visible that the imposed influence matches on a phase at the moments of "activity" of the violator, but amplitudes can significantly differ. At the same time, at moments of long absence of "activity" of the violator, the selected component saves frequency.

On the basis Figure 2b,c, it can be judged that the coefficient of cross correlation and the amplitude difference of functions do not display these patterns, as their values are not informative for influence detection confirmation.

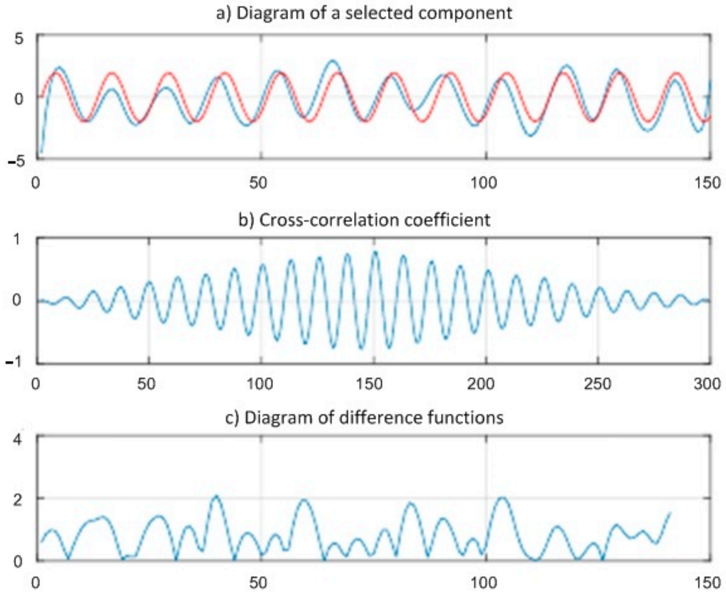

Figure 1. Results of simulation of impact detection by extreme filtering method in the determined mode (red color shows an impact, blue shows a highlighted component).

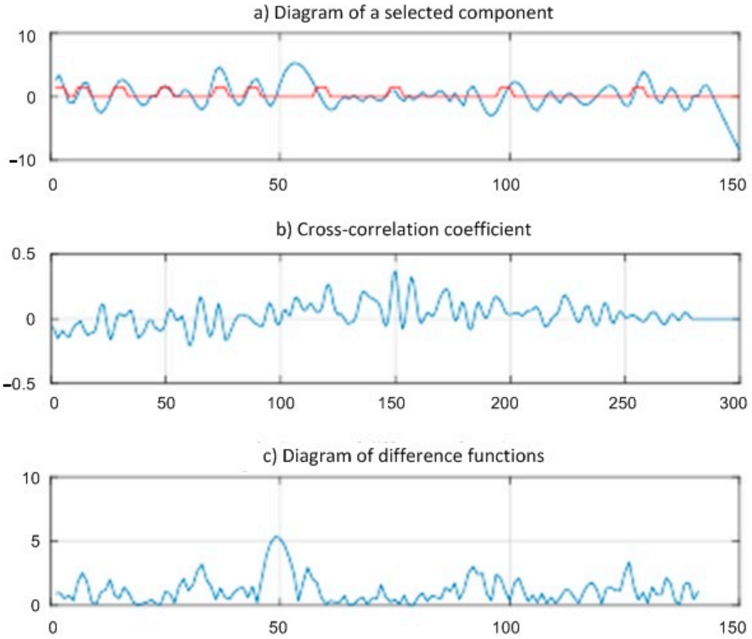

Figure 2. Results of detection of impact by extreme filtering method in the accidental mode.

Thus, analysis of the calculation results shows that in the above embodiment of the attacker's impact on the network, detection of a given function is performed with very high accuracy (Figure 1). However, in the case where the pause intervals between the series of packets of the intruder are random (Figure 2), the detection accuracy of a given function is reduced by the extreme filtering method.

To set the attack function of the intruder, consider the process of preparation of DDOS-attack from the point of view of the stochastic network conversion method [22]. Let us present this process as a sequence of events, each characterized by a distribution function, average time, and variance. These indicators make it possible to determine with a given degree of probability the number of packets transmitted by an attacker at the moments of exposure to the network and the time intervals between these actions. They allow one to specify mathematically the process of influencing the network in order to collect data on the network architecture, its elements installed on the elements of software components in order to identify vulnerabilities through which it is possible to affect the network.

A complete description of the DDOS attack model is presented in [40], which shows that the DDOS attack profile model consists of the following steps (Figure 3):

- Carrying out the attack "The analysis of network traffic" with probability P_1 for average time $\bar{t}_1$ with time distribution function $D(t)$;
- Carrying out the attack "Scanning of data transfer protocols" with probability P_2 for average time $\bar{t}_2$ with time distribution function $N(t)$;
- Carrying out the attack "Scanning of network and its vulnerabilities" with probability P_3 for average time $\bar{t}_3$ with time distribution function $V(t)$.

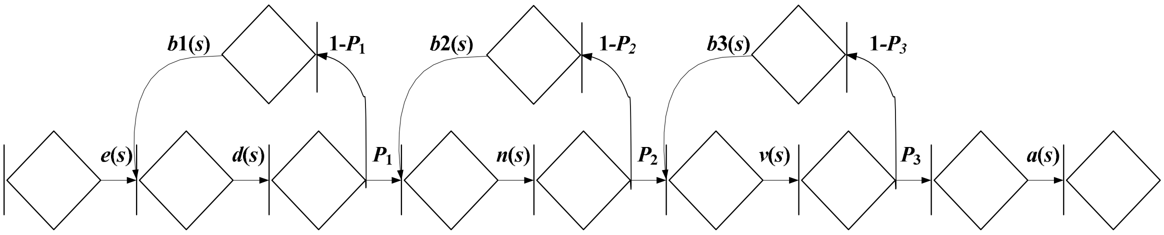

Figure 3. The stochastic network of the sequence of equivalent cyber-attacks in the preparation of the DDOS attack.

If the equivalent attack is not realized, then repeated performance happens for the average time $\bar{t}_{\text{repeat}}$ with time distribution functions $b1(t)$, $b2(t)$, and $b3(t)$.

To describe the profile model, let us consider the sequential implementation of these events.

Each phase of the equivalent attack can be presented in the form of several simpler implementations. To carry out "The analysis of network traffic", it is necessary to carry out the analysis of packets at the data link layer (with probability $P_{1.1}$ and with an average time of $\bar{t}_{1.1}$) and at the network layer (with probability $P_{1.2}$ and with an average time $\bar{t}_{1.2}$). For an implementation the attack "Scanning of transfer protocols", it is necessary to scan for an attack by a TCP packet with SYN flags (with probability $P_{2.1}$ and an average time $\bar{t}_{2.1}$), FIN (with probability $P_{2.2}$ and an average time $\bar{t}_{2.2}$), ACK (with probability $P_{2.3}$ and an average time $\bar{t}_{2.3}$), XMAS (with probability $P_{2.4}$ and an average time $\bar{t}_{2.4}$), NULL (with probability $P_{2.5}$ and an average time $\bar{t}_{2.5}$), UDP packets (with probability $P_{2.6}$ and an average time $\bar{t}_{2.6}$) and ICMP (with probability $P_{2.7}$ and an average time $\bar{t}_{2.7}$). For an implementation of the attack "Scanning of network and its vulnerabilities", scanning is carried out in the protocols RIP, OSPF, SNMP, HTTP, SAMBA, TELNET, POP3, NNTP, FINGER, FTP, TFTP, RLOG-IN, IDENT, MAC, and RPC.

Let us assume that the effects of the intruder (the time intervals between incoming non-concrete packets) are subject to the exponential law of distribution. According to the stochastic network conversion method, the stochastic network is closed by a dummy branch that connects the end of the last node and the beginning of the first node. Then, the equivalent function of the stochastic network is as follows:

$$Q(s) = \frac{e(s) \cdot d(s) \cdot p1 \cdot n(s) \cdot p2 \cdot v(s) \cdot p3 \cdot a(s)}{1 - x(s) - y(s) - z(s) + x(s) \cdot y(s) + x(s) \cdot z(s) + y(s) \cdot z(s) - x(s) \cdot y(s) \cdot z(s)}, \tag{6}$$

where $x(s),\ y(s),$ and $z(s)$ are calculated by following formulas:

$$x(s) = d(s) \cdot (1 - p1) \cdot b1(s), \tag{7}$$

$$y(s) = n(s) \cdot (1 - p2) \cdot b2(s), \tag{8}$$

$$z(s) = v(s) \cdot (1 - p3) \cdot b3(s). \tag{9}$$

Given the exponential law of private process allocation, the probability of execution of the *k*-th attack process is determined by the following formulas:

$$e(s) = \int_0^\infty \exp(-st) d[E(t)] = \frac{e}{e + s}, \tag{10}$$

$$d(s) = \int_0^\infty \exp(-st) d[D(t)] = \frac{d}{d + s}, \tag{11}$$

$$n(s) = \int_0^\infty \exp(-st) d[(N(t)] = \frac{n}{n + s}, \tag{12}$$

$$v(s) = \int_0^\infty \exp(-st) d[V(t)] = \frac{v}{v + s}, \tag{13}$$

$$a(s) = \int_0^\infty \exp(-st) d[A(t)] = \frac{a}{a + s}. \tag{14}$$

Let us substitute the expression (8)–(15) in (7) and bring the equivalent function of the stochastic network to the following form:

$$Q(s) = \frac{e \cdot d \cdot n \cdot v \cdot a \cdot p1 \cdot p2 \cdot p3 \cdot (b1 - s) \cdot (b2 - s) \cdot (b3 - s)}{(a - s) \cdot (e - s) \cdot (s^6 + A \cdot s^5 + B \cdot s^4 + C \cdot s^3 + D \cdot s^2 + E \cdot s + H)}. \tag{15}$$

Coefficients A, B, C, D, E, and H correspond to the numerical coefficients of the polynomial. To define the integral function of time distribution, we use the Heaviside decomposition [41]:

$$Q(s) = \sum_{k=1}^{8} \frac{f(s_k)}{\varphi'(s_k)} \cdot \frac{1}{s - s_k}. \tag{16}$$

To define deductions in poles, we will find roots of the polynom $s^6 + A \cdot s^5 + B \cdot s^4 + C \cdot s^3 + D \cdot s^2 + E \cdot s + H$, considering that $e = 1/\bar{t}_{\text{query}}$, $d = 1/\bar{t}_{\text{traffic}}$, $n = 1/\bar{t}_{\text{scan}}$, $v = 1/\ \bar{t}_{\text{vuln}}$, $a = \bar{t}_{\text{report.}}$, $b1$ (2; 3) = $\bar{t}_{\text{repeat}}$, which correspond to the following intensities: sending requests with the average time $\bar{t}_{\text{query}}$ and the time distribution function *E*(*t*); the analysis of traffic with the average time $\bar{t}_{\text{traffic}}$ and the time distribution function *D*(*t*); scanning of data transfer protocols with the average time $\bar{t}_{\text{scan}}$ and the time distribution function *N*(*t*); search of vulnerabilities with the average time $\bar{t}_{\text{vuln}}$ and the time distribution function *V*(*t*); drawing up the report with the average time $\bar{t}_{\text{report}}$ and the time distribution function

$A(t)$, repetition of the private attack with the average time $\bar{t}_{\text{repeat}}$ and the time distribution function $B1$ (2; 3) (t).

Let us integrate (16) and make calculations. As basic data, we will accept $\bar{t}_{\text{query}}$ = 2 min, $\bar{t}_{\text{traffic}}$ = 7 min, $\bar{t}_{\text{scan}}$ = 7 min, $\bar{t}_{\text{vuln}}$ = 5 min, $\bar{t}_{\text{report.}}$= 6 min, $\bar{t}$ $_{\text{repeat}}$ = 4 min, $p1$ = 0.3, $p2$ = 0.5, $p3$ = 0.8. The time distribution function $F(t)$ is presented in Figure 4.

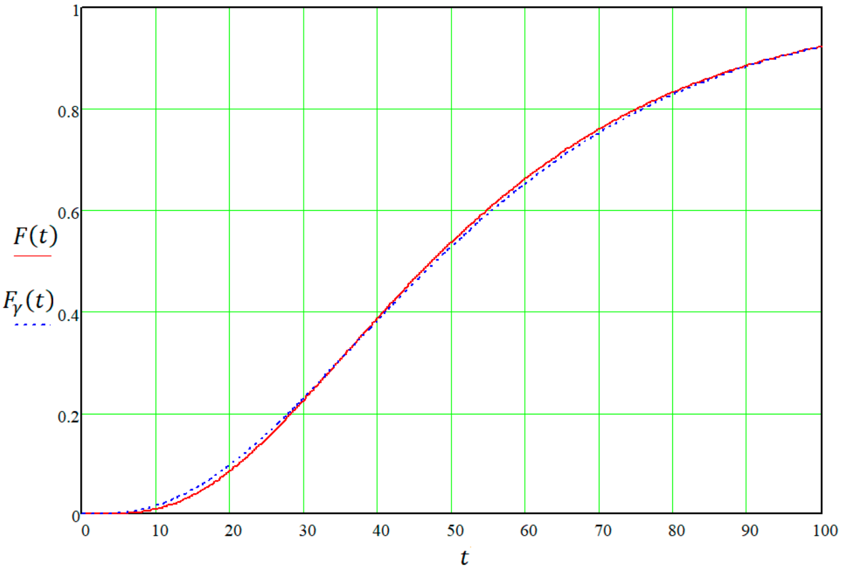

Figure 4. The time distribution functions for implementation of separate attacks during DDOS attack preparation.

The distribution function $F(t)$ can be approximated by an incomplete gamma function:

$$F_{\gamma}(t) = \frac{\mu^{\alpha}}{\Gamma(\alpha)} \int_0^t t^{\alpha-1} \cdot e^{-\mu t} dt \,, \tag{17}$$

where $\mu = \frac{T(P_n)}{D(P_n)}$, $\alpha = \frac{T(P_n)^2}{D(P_n)}$ are parameters of the scale and the form of an incomplete gamma function; $T(P_n)$ is the average time for attack implementation; and $D(P_n)$ is the variance of the attack implementation time.

The average attack implementation time is determined by the following function:

$$T(P_n) = -\frac{d}{ds}\left[\frac{Q\,(s, P_n)}{Q(s=0,\ P_n)}\right]_{s=0} . \tag{18}$$

The variance of the attack time is determined by the following function:

$$D(P_n) = \frac{d^2}{ds^2}\left[\frac{Q\,(s, P_n)}{Q(s=0,\ P_n)}\right]_{s=0} - \left\{-\frac{d}{ds}\left[\frac{Q\,(s, P_n)}{Q(s=0,\ P_n)}\right]_{s=0}\right\}^2 . \tag{19}$$

The function $F_{\gamma}(t)$ as a result of the approximation is also presented in Figure 4.

Knowing the time distribution function, it is possible to determine the function of probability density $h(t)$, as well as the intensity λ(t), using the following expressions:

$$F(t) = \int_0^t h(t) dt \,, \tag{20}$$

$$\lambda(t) = \frac{h(t)}{1 - F(t)} . \tag{21}$$

Thus, preparation of the DDOS attack can be presented in the form of the sequence of incoming packets on interfaces of the firewall or the server. At the same time, this sequence of requests is characterized by the following functions: $F(t)$-the quantity of the arrived illegal packets in unit of time (amplitude of the imposed noise); λ(t)-the time between series of requests of the malefactor. Thus, the presented model allows to formalize implementation process of the attack and to define function which is required to be found in the set period.

3. Experimental Results

In order to increase the accuracy of the method considered and reduce the number of false positives, we propose to consider indirect supporting signs of attack, namely network characteristics. [42–47] describe the metrics by which cyber-attacks are indirectly detected. As an example, there is a model of a telecommunications network operating in an attack mode consisting of two steps, each of which violates the operation of the system with the probability p_i. As initial data, we will accept:

- The average time to repair of a system after cyber action t_d = 2 s,
- The average time of successful implementation of the first attack $t_{\mathrm{r}1}$ = 400 s,
- The average time of successful implementation of the second attack $t_{\mathrm{r}2}$ = 300 s,
- The average volume of a data packet V = 0.25 Mbit,
- The data transmission rate R_v = 150 Mbit/s,
- The flow is self-similar with Hurst index equaled 0.71,
- The entering flow of packets is characterized by Veybull's distribution.

We will use the method of transformation of stochastic networks in modeling the behavior of the intruder.

In the simulation process, we determine the dependence of the average packet delay time, the probability of packet loss, and the packet delay time jitter on the incoming flow rate (λ_1 = 10 packet/s and λ_2 = 13 packet/s). The results are summarized in Table 2.

Table 2. Simulation data for variable incoming flow intensity.

Metrics	Metric Values at Different Incoming Flow Intensities	
	$\lambda_1 = 10$	$\lambda_2 = 13$
The average packet delay time, sec.	0.788	1.23
The probability of packages losses	0.195	0.25
The packet delay time jitter, sec.	0.811	1.268

Let us evaluate the network characteristics at the incoming flow intensity λ = 10 and the varying average volume of the data packet. The results are presented in Table 3.

Table 3. Simulation data at changing probabilities of system failure at computer attack stages.

Metrics	Metric Values at Different Average Volumes of Packets V	
	$\lambda_1 = 10$ $V_1 = 0.2$	$\lambda_1 = 10$ $V_2 = 0.27$
The average packet delay time, sec.	0.749	0.805
The probability of packages losses	0.19	0.197
The packet delay time jitter, sec.	0.776	0.827

The findings results suggest that the metrics given are sensitive to minor changes in both flow intensity and average packet volume. In both cases, with increasing intensity of incoming flow and average volume of packets, average delay time of packets, and jitter of delay time of packets change most clearly, probability of packet loss changes less appreciably. This confirms the conclusion that the selected metrics allow additional traffic analysis to early detect cyber-attacks in computer networks.

The system, which includes a complex to detect an attack at an early stage (at the stage of preparation), has less recovery time during retransmission or preparation time for the next stage of the attack. Table 4 presents the simulation results (network characteristics) in a system where only the recovery time from the attack phase will change.

Table 4. Simulation data with varying system recovery times after computer attack phases.

Metrics	Metric Values at Different Recovery Times	
	$\lambda = 10$ $tr_1 = 3$ s	$\lambda = 10$ $tr_2 = 9$ s
The average packet delay time, sec.	4.403	18.253
The probability of packages losses	0.327	0.801
The packet delay time jitter, sec.	5.476	36.28

The given data confirm that the system, which includes the proposed complex of early detection of cyber-attacks, has significantly better metrics with equal effects from the violator. This means reducing the impact of cyber-attacks on system performance.

Table 5 shows the results of a comparative evaluation of the proposed method with well-known approaches in terms of accuracy and duration of attack detection.

Table 5. Comparison of the proposed and known methods for the accuracy and duration of DDOS attack detection.

Attack Detection Method	Accuracy	Duration, Sec.
Signature-based [27]	0.75	10
IP distance-based [32]	0.99	100
Kolmogorov complexity based [36]	-	10
Extreme filtering:		
- determined mode	0.9	1.5
- accidental mode	0.8	7.5

Table 5 demonstrates that none of the known methods for DDOS attack detection has such a small value of the detection duration as the extreme filtering method has. Moreover, this method has fairly good attack detection accuracy. This is a fair result, since the method of extreme filtering allows one to quickly process the flow of data arriving at the network element, and at the same time, it is not demanding in terms of the power of hardware resources. The advantage of the method in comparison with the signature analysis is the lower number of false positives during the same detection time. Machine learning requires additional hardware resources (which leads to an increase in the cost of the attack detection complex) and has a significant detection time, which does not allow analysis in a time mode close to real, but the detection accuracy is very high. Therefore, the proposed method is most suitable for implementing early detection of DDOS attacks. In addition, the extreme filtering method can be used in combination with machine learning methods at the stage of preprocessing of the data stream on network elements.

Thus, the proposed system of early detection of cyber-attacks using the method of extreme filtering, functioning in "real time," allows to minimize the effect of carrying out cyber-attacks.

4. Discussion

As was shown by the experimental results, the proposed method of extreme filtering allows, with high and fairly fast accuracy, to detect equal periodic actions of the intruder, which may correspond to the initial stages of the DDOS attack implementation. This is an essential advantage of the proposed method. At the same time, it should be noted that if the intruder generates his requests at random intervals, then the probability (accuracy) of network traffic detection is slightly reduced.

The conducted simulation scenario corresponded to a case of a rather strong DDOS attack. In this scenario, the amplitude of the superimposed signal was comparable to the amplitude of the desired signal. In other words, the number of incoming illegitimate packets to the attacked ports of the communication node per unit time was comparable with the total number of packets entering the server.

At the same time, the secondary features of cyber-attacks were used in the work. As main secondary features, it was proposed to use such network characteristics as the times of the successful implementation of the first and second attacks, the recovery time of the system after the attack, the volume of the data packet, the data transfer rate, and the distribution law to which the network flow follows. Using these features allows one to successfully detect a DDOS attack at an early stage of its spread and, thereby, minimize its consequences.

The suggested profile model of the stochastic network for the initial stage of the DDOS attack implementation allows in real-time one to obtain the probability-time characteristics of this process. All the necessary mathematical calculations and transformations that must be performed during the processing of the stochastic network of the analyzed process are quickly performed on the modern means of mathematical calculations, for example, in the MatLab (The MathWorks, Inc., 1 Apple Hill Dr, Natick, MA 01760, United States) system.

The proposed model of the process of the DDOS attack implementation allows one to estimate the network recovery time after an attack if the proposed attack detection mechanism is used in the security system. Based on the results of the experimental assessment, it is possible to conclude that the network recovery time lies in the range from 3 s to 9 s. At the same time, the parameters of quality of service remain in an acceptable range.

It should be noted that the realized studies thus far only demonstrate the potentiality and effectiveness of the proposed attack detection method. The practical implementation and further improvement of this method, its distribution to other types of cyber-attacks, as well as its interaction in the security system with other methods, determine further areas of research.

5. Conclusions

The method of extreme filtering succeeded with high accuracy to find equally periodic actions of the violator which can correspond to implementation of preparation of the DDOS attack in the simplest option. When using accidental intervals between the violator's requests, the probability of detection of network traffic decreases. When modeling amplitude of an alias signal was comparable to amplitude of a desired signal, that is the quantity of the entering illegitimate packets on the attacked ports of hub site for unit of time was comparable to a total quantity of the packets entering on the server.

The advantage of the proposed method is its low resource consumption, which allows detecting cyber-attacks in real time, as well as the ability to detect DDOS attacks in the early stages of their development. The latter factor is very important for telecommunication networks of the energy infrastructures, since it allows maintaining high stability and uninterrupted functioning of energy power grids under the influence of cyber-attacks.

The proposed profile model of the stochastic network of the DDOS attack preparation process and the probability-time characteristics obtained by it allow one to set the function to be detected by the proposed method based on the stochastic network transformation.

As secondary features of cyber-attack, it is proposed to use network characteristics that are sensitive to the occurrence of additional incoming flow and sharply deteriorate if the preparation stage is successful. Thus, with the proposed method, it is possible to detect DDOS attacks at an early stage (preparation stage) and thus minimize its consequences.

The main directions of further research are the comprehensive experimenting with using the approach suggested for different kinds of attacks and its practical implementation in existing cyber security systems of energy power grids.

Author Contributions: A.P. was responsible for conceptualization; V.L. conceived and designed the experiment; I.K. and I.S. analyzed the data; all authors wrote the paper.

Funding: Research is carried out with support of Ministry of Education and Science of the Russian Federation as part of Agreement No. 05.607.21.0322 (identifier RFMEFI60719X0322).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ershova, T.V.; Hohlov, Y.E. Russian Digital Economy Program. *IAC Online J.* **2018**, 35–38.
2. Rosas-Casals, M.; Valverde, S.; Solé, R.V. Topological Vulnerability of the European Power Grid under Errors and Attacks. *Int. J. Bifurc. Chaos* **2007**, *17*, 2465–2475. [CrossRef]
3. Wang, D.; Guan, X.; Liu, T.; Gu, Y.; Shen, C.; Xu, Z. Extended Distributed State Estimation: A Detection Method against Tolerable False Data Injection Attacks in Smart Grids. *Energies* **2014**, *7*, 1517–1538. [CrossRef]
4. Worldwide Infrastructure Security Report, 2014. Available online: https://www.checkpoint.com/downloads/product-related/report/2018-security-report.pdf (accessed on 12 December 2019).
5. Chadd, A. DDoS attacks: Past, present and future. *Netw. Secur.* **2018**, *2018*, 13–15. [CrossRef]
6. Zargar, S.T.; Joshi, J.; Tipper, D. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 2046–2069. [CrossRef]
7. Darwish, M.; Ouda, A.; Capretz, L.F. Cloud-based DDoS attacks and defenses. In Proceedings of the International Conference of Information and Communication Technology (ICoICT), Bandung, Indonesia, 20–22 March 2013; IEEE: Bandung, Indonesia, 2013. [CrossRef]
8. Vlajic, N.; Zhou, D. IoT as a Land of Opportunity for DDoS Hackers. *Computer* **2018**, 26–34. [CrossRef]
9. Gillani, F.; Al-Shaer, E.; Lo, S.; Duan, Q.; Ammar, M.; Zegura, E. Agile virtualized infrastructure to proactively defend against cyber attacks. In Proceedings of the IEEE Conference on Computer Communications (INFOCOM), Hong Kong, China, 26 April–1 May 2015; IEEE: Hong Kong, China, 2015. [CrossRef]
10. Bawany, N.; Shamsi, J.; Salah, K. DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions. *Arab. J. Sci. Eng.* **2017**, *42*. [CrossRef]
11. Abdullah, A. Detection of Distributed Denial of Service Attacks Using Artificial Neural Networks. *Int. J. Adv. Comput. Sci. Appl.* **2017**, *8*, 306–318.
12. Suresh, M.; Anitha, R. Evaluating Machine Learning Algorithms for Detecting DDoS Attacks. In Proceedings of the Advances in Network Security and Applications. CNSA 2011 Communications in Computer and Information Science, Chennai, India, 15–17 July 2011; Wyld, D.C., Wozniak, M., Chaki, N., Meghanathan, N., Nagamalai, D., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; Volume 196.
13. Singh, P.; Rehman, S.; Manickam, S. Enhanced Mechanism to Detect and Mitigate Economic Denial of Sustainability (EDoS) Attack in Cloud Computing Environments. *Int. J. Adv. Comput. Sci. Appl.* **2017**, *8*. [CrossRef]
14. Galtsev, A.; Sukhov, A. Detecting network attacks at flow level. *Telecommun. Radio Eng.* **2013**, *72*. [CrossRef]
15. Top 8 Network Attacks by Type in 2017. Available online: https://www.calyptix.com/top-threats/top-8-network-attacks-type-2017 (accessed on 12 December 2019).
16. DDoS attacks in Q3 2019. Available online: https://securelist.com/ddos-report-q3-2019/94958/ (accessed on 12 December 2019).
17. Purwanto, Y.; Kuspriyanto; Hendrawan, T.; Rahardjo, B. Traffic anomaly detection in DDos flooding attack. In Proceedings of the 8th International Conference on Telecommunication Systems Services and Applications (TSSA), Kuta Bali, Indonesia, 23–24 October 2014; IEEE: Kuta Bali, Indonesia, 2014. [CrossRef]
18. Kalkan, K.; Alagöz, F. A distributed filtering mechanism against DDoS attacks: ScoreForCore. *Comput. Netw.* **2016**, *108*, 199–209. [CrossRef]
19. Kwon, C.; Liu, W.; Hwang, I. Security analysis for Cyber-Physical Systems against stealthy deception attacks. In Proceedings of the American Control. Conference, Washington, DC, USA, 17–19 June 2013; IEEE: Washington, DC, USA, 2013. [CrossRef]

20. Hoquea, N.; Kashyapb, H.; Bhattacharyya, D.K. Real-time DDoS attack detection using FPGA. *Comput. Commun.* **2017**, 48–58. [CrossRef]
21. Bekeneva, Y.; Shipilov, N.; Borisenko, K.; Shorov, A. Simulation of DDoS-attacks and protection mechanisms against them. In Proceedings of the IEEE NW Russia Young Researchers in Electrical and Electronic Engineering Conference (EIConRusNW), St. Petersburg, Russia, 2–4 February 2015. [CrossRef]
22. Kotenko, I.; Saenko, I.; Lauta, O. Modeling the Impact of Cyber Attacks. *Cyber Resil. Syst. Netw.* **2019**, 135–169. [CrossRef]
23. Modi, C.; Patel, D.; Borisaniya, B.; Patel, H.; Patel, A.; Rajarajan, M. A survey of intrusion detection techniques in Cloud. *J. Netw. Comput. Appl.* **2013**, 42–57. [CrossRef]
24. Swami, R.; Dave, M.; Ranga, V. Software-defined Networking-based DDoS Defense Mechanisms. *ACM Comput. Surv.* **2019**, *52*, 28. [CrossRef]
25. Peng, T.; Leckie, C.; Ramamohanarao, K. Survey of network-based defense mechanisms countering the DoS and DDoS problems. *ACM Comput. Surv.* **2007**, *39*, 1–42. [CrossRef]
26. Imran, M.; Durad, M.H.; Khan, F.A.; Derhab, A. Toward an optimal solution against denial of service attacks in software defined networks. *Future Gener. Comput. Syst.* **2019**, *92*, 444–453. [CrossRef]
27. De Assis, M.V.O.; Hamamoto, A.H.; Abrao, T.; Proenca, M.L. A game theoretical based system using holtwinters and genetic algorithm with fuzzy logic for DoS/DDoS mitigation on SDN networks. *IEEE Access* **2017**, *5*, 9485–9496. [CrossRef]
28. AlEroud, A.; Alsmadi, I. Identifying cyber-attacks on software defined networks. *J. Netw. Comput. Appl.* **2017**, *80*, 152–164. [CrossRef]
29. Ashraf, J.; Latif, S. Handling intrusion and DDoS attacks in Software Defined Networks using machine learning techniques. In Proceedings of the National Software Engineering Conference (NSEC), Rawalpindi, Pakistan, 11–12 November 2014; IEEE: Rawalpindi, Pakistan, 2014. [CrossRef]
30. Alshamrani, A.; Chowdhary, A.; Pisharody, S.; Lu, D.; Huang, D. A defense system for defeating DDoS attacks in SDN based networks. In Proceedings of the 15th ACM International Symposium on Mobility Management and Wireless Access (MobiWac'17), Miami, FL, USA, 21–25 November 2017; ACM: New York, NY, USA, 2017; pp. 83–92. [CrossRef]
31. Niyaz, Q.; Sun, W.; Javaid, A.Y. A deep learning based DDoS detection system in software-defined networking (SDN). *Arxiv* **2016**, arXiv:1611.07400. [CrossRef]
32. You, Y.; Zulkernine, M.; Haque, A. Detecting Flooding-Based DDoS Attacks. In Proceedings of the IEEE International Conference on Communications (ICC), Glasgow, UK, 24–28 June 2007; IEEE: Glasgow, UK, 2007. [CrossRef]
33. Qin, X.; Xu, T.; Wang, C. DDoS Attack Detection Using Flow Entropy and Clustering Technique. In Proceedings of the 11th International Conference on Computational Intelligence and Security (CIS), Shenzhen, China, 19–20 December 2015; IEEE: Shenzhen, China, 2015. [CrossRef]
34. Aziz, M.Z.A.; Okamura, K. Leveraging SDN for detection and mitigation SMTP flood attack through deep learning analysis techniques. *Int. J. Comput. Sci. Netw. Secur.* **2017**, *17*, 166–172.
35. Li, L.; Lee, G. DDoS Attack Detection and Wavelets. *Telecommun. Syst.* **2005**, *28*, 435–451. [CrossRef]
36. Kulkarni, A.; Bush, S. Detecting Distributed Denial-of-Service Attacks Using Kolmogorov Complexity Metrics. *J. Netw. Syst. Manag.* **2006**, *14*, 69–80. [CrossRef]
37. Rilling, G.; Flandrin, P.; Goncalves, P. On empirical mode decomposition and its algorithms. In Proceedings of the IEEE-EURASIP Workshop on Nonlinear Signal and Image Processing, Trieste, Italy, 8–11 June 2003; Available online: http://perso.ens-lyon.fr/patrick.flandrin/NSIP03.pdf (accessed on 12 December 2019).
38. Myasnikova, N.; Beresten, M.; Tsypin, B.; Myasnikova, M. Application of empirical mode decomposition on the basis of differentiation and integration to information and measurement systems. In Proceedings of the International Scientific Conference Proceedings "Advanced Information Technologies and Scientific Computing", Samara, Russia, 28 August–1 September 2017; pp. 435–438.
39. Myasnikova, N.; Beresten, M.; Dolgih, L. Processing of ECG Signals Detected by Portable Devices. *Biomed. Eng.* **2016**, *50*, 175–178. [CrossRef]
40. Singh, K.; De, T. Mathematical modelling of DDoS attack and detection using correlation. *J. Cyber Secur. Technol.* **2017**, *1*, 175–186. [CrossRef]
41. Pristker, A.A.B.; Harp, W.W. GERT: Graphical Evaluation and Review Technique. Part 1. *J. Ind. Eng.* **1966**, *6*, 293–301.

42. Iglesias, F.; Zseby, T. Analysis of network traffic features for anomaly detection. *Mach. Learn.* **2015**, *101*. [CrossRef]
43. Yaar, A.; Perrig, A.; Song, D. Pi: A path identification mechanism to defend against DDoS attacks. In Proceedings of the Symposium on Security and Privacy, Berkeley, CA, USA, 11–14 May 2003; IEEE: Washington, DC, USA, 2003. [CrossRef]
44. Kaur, G.; Saxena, V.; Gupta, J.P. Anomaly Detection in network traffic and role of wavelets. In Proceedings of the 2nd International Conference on Computer Engineering and Technology, Chengdu, China, 16–18 April 2010; IEEE: Chengdu, China, 2010. [CrossRef]
45. Behal, S.; Kumar, K. Trends in Validation of DDoS Research. *Procedia Comput. Sci.* **2016**, 7–15. [CrossRef]
46. Hosseini, S.; Azizi, M. The hybrid technique for DDoS detection with supervised learning algorithms. *Comput. Netw.* **2019**, 35–45. [CrossRef]
47. Singh, K.; Dhindsa, K.S.; Bhushan, B. Deployment of agent T-BASED distributed defense mechanism against DDOS attacks in multiple ISP networks. *Int. J. Inf. Technol. Secur.* **2017**, *9*, 123–134.