The using of fractal measures for network state monitoring and probabilistic network attack type determination

O Yu Gubareva[1], O V Osipov[1], A O Pocheptsov[1] and V V Pugin[1]

[1]Povolzhskiy State University of Telecommunications and Informatics, L. Tolstoy Street 23, Samara, Russia, 443010

Abstract. In the academic paper for network traffic analysis concerning risk assessment of network nodes infosecurity fractal analysis is used which takes into consideration system past history and makes it possible to randomly determine probable network attack types on the system of interest. There has been developed a network traffic analysis technique based on fractal measures set with a focus on network state analysis and probabilistic attack type determination. Following on from the thesis results there is possible the creation of network traffic analyzer (sniffer) for time estimate of infosecurity state as well as further computation of previously attacked devices and network nodes.

1. Introduction

Any organization when operating is liable to various infosecurity risks which one way or another affect particular business processes characteristics and can negatively influence on financial data as well as the opportunity for the organization to go on its activity. Current business requirements necessitate using well-grounded technical-and-economic methods and means in operation providing quantitative and qualitative infosecurity (IS) level determination both with assessing infosecurity cost efficiency. For the purpose of efficient organization infosecurity a serious, systematic and integrated approach is required.

Almost any infosecurity system building must start form risks analysis. Before infosecurity system designing one should specify what threatening (in other words conditions and factors which can become the reason for breaking system integrity, its security and privacy and also facilitating unauthorized access to it) exists for the given infosystem and to what extent it is potentially critical.

Telecommunications networks have numerous vulnerabilities arising both in system software development and in misconfiguration and equipment operation. The presence of security threat makes it possible for intruders to put into operation various types of network attack. Nowadays software tools development for infosecurity risks analysis by means of network traffic online analysis is of great interest. Clearing up possible threat aims makes the basis for providing safety-related system design. The threat aims show what should be protected. As a rule network state is analyzed with a focus on network administration problem solving, routing device monitoring, etc. To become aware of abnormal system behavior there is often used various statistic information collection and analysis via IP-traffic. In this paper for network traffic data accessing a free given software Zabbix under GNU GPL license was used. The

monitoring system in this case builds software set for current traffic measuring and software system of its analysis constructed with computing entries so called fractal measures which will be specified in the given paper.

2. The research objective and solution method

The research objective is network traffic analysis technique development based on fractal measures set aimed at network state analysis and probabilistic attack type determination. Resting upon the research described in this paper the authors are planning to create a network traffic analyzer (sniffer) currently left on a company server for its time estimate, consecutive defining of previously attacked devices and network nodes (network vulnerabilities) and as a result further IS risks assessment.

The paper [1] gives an overview of scientific research in the field of analysis real-time network traffic, and specific hardware and software solutions are considered.

In the work [2] the use of the Hurst index for the analysis of the traffic subject to anomalous intrusions in the form of DoS-attacks is considered. The studies conducted in [2] showed that traffic has the property of self-similarity during abnormal intrusions, which proves the possibility of determining traffic anomalies in real time.

To take the set goal in the academic paper the following challenges are met: running the process analysis of the infosystem in question (the infosystem of an academic institution was taken as a basis) as an object to protect; Hurst exponent assessment, power-density spectrum and network traffic fractal measures in normal state and in the time of attack on the infosystem resources; executing the attack on the system resources.

Fractal analysis is statistic in its nature and in addition it gives the possibility to find self-similarity markers in the traffic of interest. The fact permits first to become aware of minimal required time for making the experiment. Second, it makes it possible to rely on the opportunity to forecast the system behavior dynamics in the nearest future. Fractal model is a set of fractal parameters (measures) put in accordance with the current network traffic state. The fractal measures changes dynamics when involving a series of measurements of one and the same telecommunication node lets us estimate traffic condition dynamics that is about the presence or absence of attacks on infosystem resources. Jumping ahead we can mention that as a result of the performed experiment it was brought to light that in case of DoS-attacks the self-similarity network traffic level reduces as well as there takes place power-density spectrum transformation.

The experiment idea is the following: there is some telecom traffic which is network load to timing dependency diagram (figure 1). From mathematical analysis perspective the traffic in question represents univariate time series the observations of which are channel occupancy levels at different moments. The current series can be analyzed with various fractal measures calculating (Hurst exponent, etc.) as well as power-density spectrum.

At the first stage Hurst exponent and power-density spectrum were calculated for the normal network condition.

First they determine Hurst exponent for calculating network traffic self-similarity level. For its determination they find average channel occupancy value $\langle U \rangle_{\mathrm{N}}$ for N tick marks [3, 4]:

$$\langle U \rangle_{\mathrm{N}} = \frac{1}{N} \sum_{n=1}^{N} U(n). \tag{1}$$

Then they define $X(n, N)$ which is accumulated divergency $U(n)$ from average value $\langle U \rangle_{\mathrm{N}}$, which is determined with the help of the following total (union):

$$X(n, N) = \sum_{p=1}^{n} \{U(p) - \langle U \rangle_{N}\}, \tag{2}$$

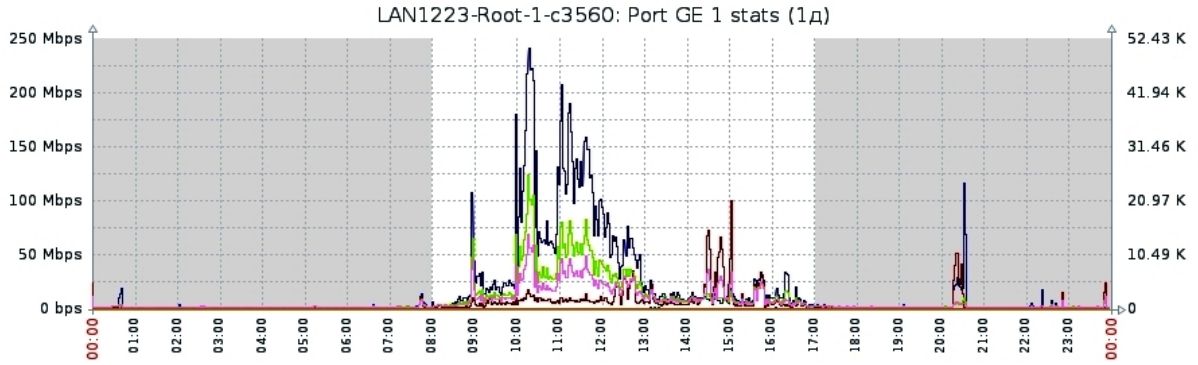

Figure 1. Network load to timing dependency diagram.

where the average value $\langle U \rangle_{\mathrm{N}}$ is defined by the formula (1).

According to standardized Hurst range [3, 4], the divergence range is determined via minimal and maximal values of the accumulated divergence $X(n, N)$ (2):

$$R(N) = \max_{1 \le n \le N} X(n, N) - \min_{1 \le n \le N} X(n, N). \tag{3}$$

The standard divergence $S(N)$ can be computed with the following known formula via dispersivity [3, 4]:

$$S(N) = \left\{ \frac{1}{N} \sum_{n=1}^{N} [U(n) - \langle U \rangle_N]^2 \right\}^{1/2}. \tag{4}$$

For most timing series the observed standardized range R/S is described by empiric relation and with the help of (3) and (4) appears as [3, 4]:

$$R/S = (\alpha N)^H, \tag{5}$$

where H is the Hurst exponent; α is an arbitrary parameter (constant).

The described procedure in scientific literature got the name of R/S-analysis.

In figure 2 there is shown R/S telecom traffic dependency in normal state upon N in log-log scale. The axis of ordinate shows the value of $\lg(R/S)$, on the x-axis — $\lg N$.

Hurst exponent value for the traffic in question in normal condition turned out to be equal 0.68. In accordance with the theory of fractals if the got Hurst exponent value $H < 0.5$ then the under study series has "short" memory. In other words it is antipersistent. It means that recent events in the begetter system produce much more influence on the following system behavior than less recent events. If $H > 0.5$ the timing series is persistent and has fractal nature. With the value $H = 0.5$ the signal represents stochastic noise and doesnt have any useful information. As can be seen from the above, it was proved that the traffic in question in normal state is self-similar and has fractal nature.

Further in the paper there was made power-density spectrum estimation which represents rapid inverse Fourier transform of autocorrelation function.

The network traffic autocorrelation function is determined by the following formula:

$$R(j) = \frac{1}{N} \sum_{i=1}^{N-j} U(i)\, U(i+j), \tag{6}$$

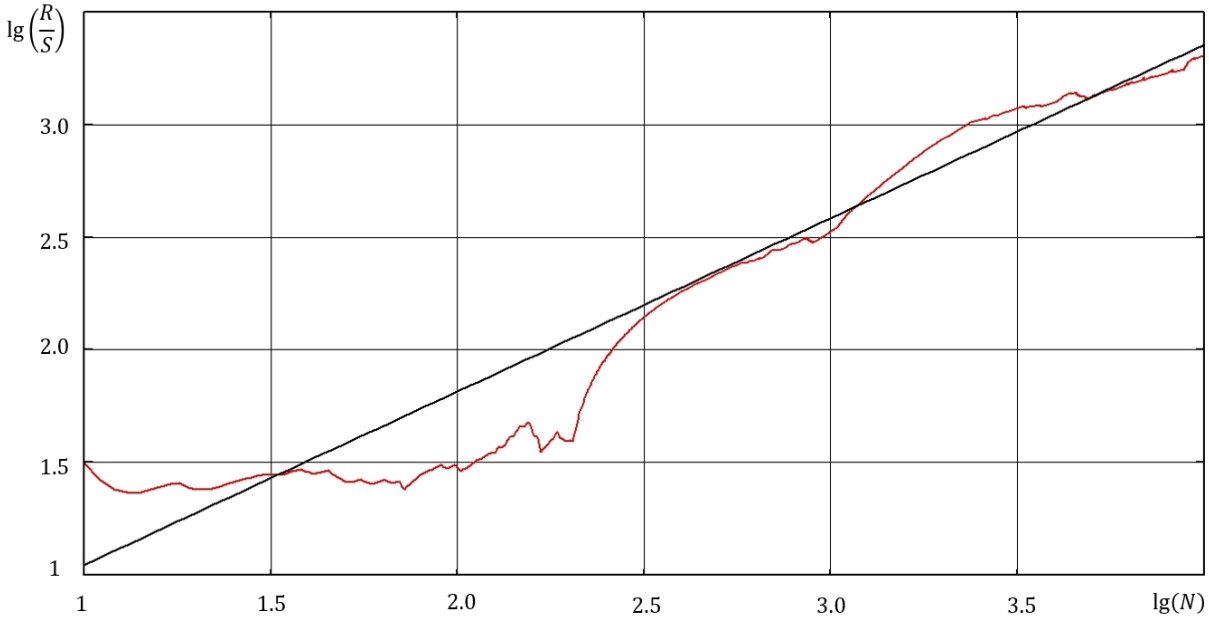

Figure 2. The R/S dependency of telecom traffic on the number of timing counts.

where N is the total number of network traffic tic marks. The signal power-density spectrum is defined by direct inverse Fourier transform of autocorrelation function (6):

$$S_k = \frac{1}{N^2} \sum_{i=1}^{N} \sum_{p=1}^{N-i} U(p)\, U(p+i) \exp\left[-\mathrm{j}\frac{2\pi k i}{N}\right], \ \left(k = \overline{0, N-1}\right). \tag{7}$$

In figure 3 there is introduced network traffic power-density spectrum $S(f) = S_k(U)$ in normal state (with no network attack).

On the second stage there were studied fractal measures and network traffic power-density spectrum with DoS-attack.

During the DoS attack, the channel was fully loaded at 70 MB per second. It is worth noting here that the use of fractal measures (in particular, the parameter R/S) allows to guarantee the scalability of the obtained results in the case of higher channel utilization.

For this a before vulnerable web-system which before-known IP-address was developed. To perform DoS-attack there was used the software which is similar to LOIC program that allows to execute an attack of the given in advance IP-address with variable transactions amount. In addition to that simultaneously with this there was executed an attack on MySQL-server using SQL-injection implementation through get-parameter of the vulnerable system.

To do that they used an enquiry with SQL-function benchmark (n, q) that gives the possibility to do n times function q [5].

For attacking SQL-server there was written a script which given number of times issued such requests in cycle. After executing DoS-attack network traffic was taken during its time which was again analyzed about fractal measures and power-density spectrum. Hurst exponent for the traffic in question in the time of attack equaled 0.54 that speaks of sharp decrease self-similarity level of the traffic of interest.

Currently, experiments are being conducted on the backbone network with a load of 1.2 GB

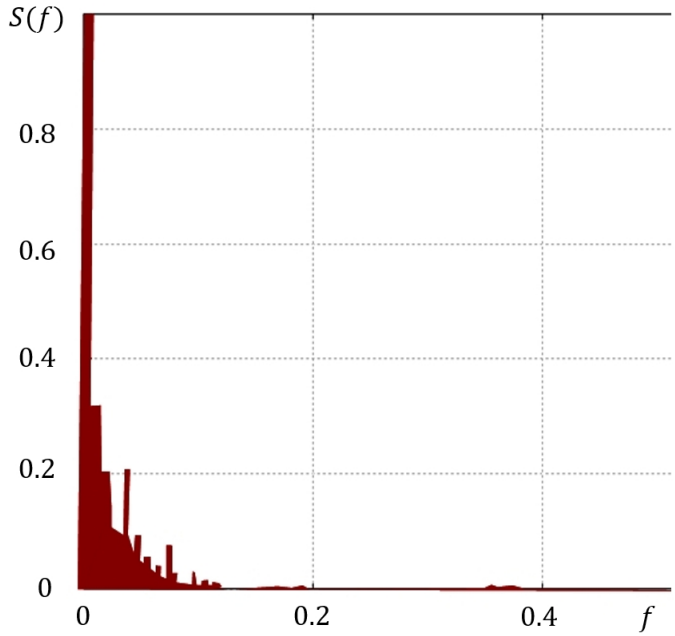

Figure 3. Network traffic power-density spectrum in normal condition.

per second with a time sample duration of 24 hours (86,000 calculated values of the channel load).

In figure 4 there is shown power-density spectrum for the case in question which allows to visually classify the signal in question as "brown" noise.

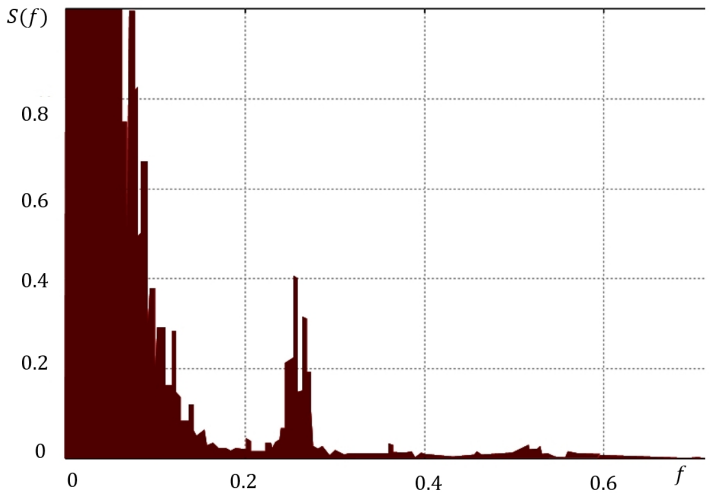

Figure 4. Network traffic power-density spectrum at the time of attack.

Consequently as a result of the experiment in real network fractal measures changing and power-density spectrum were proved with DoS-attack.

Not without interest are studying of fractal measures and network traffic power-density

spectrum while various network attacks are that can lead to creation of some on-line "patterns" database (library) of power-density spectra and fractal measures values. In other words it is referred to the opportunity to make some fractal network-status indicator for the time of high probability to determine the threat type. Worth making a point in this regard is that subtle fractal analysis allows to reveal minimal traffic changing despite full channel occupancy in case of network attack. However, here we need further experimental research aimed at revealing specific attacks and building "patterns" of fractal characteristics.

Note that Hurst exponent computing of network traffic with 10000 time samples takes around 1,5 seconds when using Intel Core i5 and power-density spectrum calculation takes about 4 seconds.

3. Conclusion

In conclusion, let us dwell on the main conclusions of the work done. Fractal network indicator led has to perform the following functions:

- saving channel occupancy entries sampling for certain time windows that are enough for network condition diagnostics;
- fractal measures and power-density spectrum calculation for every set timing series for the definite interval times for the purpose of further comparison with ¡¡patterns¿¿ from the information base (using neural networks);
- finding of network state totally in the current and precedent time points;
- probability forecast about the network attack nature in the future.

Thus, in the paper for network traffic state analysis (including DoS-attacks) there is offered to use fractal measures and power-density spectrum which allow by indirect hints for agreeable time limit to determine threat level.

The algorithms developed in this work may be useful for the analysis of "smartlink connections" [6]. Another object of the fractal technique is the stochastic network [7].

In conclusion, we note that the proposed method is the basis for creating a fractal indicator for analyzing the state of the network, while specialized software (iptables, ipwf, etc.) should be used to determine the sources of the DoS attack.

4. References

[1] Get'man A I, Markin Yu V, Evstropov E F and Obydenkov D O 2017 Analysis of network traffic in the mode real-time: overview of applied tasks, approaches and solutions *Trudy ISP RAN* **29(3)** 117-150 (in Russian)

[2] Shelukhin O I and Antonyan A A 2014 Analysis of changes in the fractal properties of telecommunications traffic caused by abnormal intrusions *T-COMM: Telecommunications and transport* **8(6)** 61-64 (in Russian)

[3] Feder J 1991 *Fractals* (Springer Science + Business Media, LLC) 305 p

[4] Golovko V A 2005 Neural network methods for processing chaotic processes *VII All-Russian scientific-technical conference "Neuroinformatics"* 43-91 (in Russian)

[5] Nizamutdinov M F 2005 *The tactics of protecting and attacking WEB applications* (SPb.: BHV-Peterburg Publisher) p 432 (in Russian)

[6] Nikitin V S, Semyonov E I, Solostin A V, Sharov V G and Chayka S V 2016 Modeling the "smartlink connection" performance *Computer Optics* **40(1)** 64-72 DOI: 10.18287/2412-6179-2016-40-1-64-72

[7] Agafonov A A, Myasnikov V V 2016 Method for the reliable shortest path search in timedependent stochastic networks and its application to GIS-based traffic control *Computer Optics* **40(2)** 275-283 DOI: 10.18287/2412-6179-2016-40-2-275-28