

Revealing of informative multifractal properties of network traffic for anomalies detection

Y.N. Bardachev, A.A. Didyk

*Kherson National Technical University, Berislavskoye shosse, 24, 73008 Kherson, Ukraine.
adidyk@isdinci.org.ua*

Abstract. Usage of multifractal formalism for analysis of network traffic structure for the purpose of anomalies revealing are considered in this paper. Multifractal spectrums of normal and abnormal (with presence of some sorts of network attacks) traffics are presented. It's shown, that multifractal spectrums of two sorts of traffic considerably differ and that gives possibility to detect in due time abnormal activity in computer systems. Usage of such approach in detection intrusion systems will give possibility to raise level of information security of computer systems considerably.

Keywords

Network traffic, anomalies detection, multifractals, multifractal spectrum

1 Introduction

Modern intrusion detection systems (IDS) are capable to inspect in real time network and operating system activity to detect unauthorized operations and automatically react to them practically in real time. Besides, IDS can parse current events, taking into consideration already occurred events, that allows to identify carried in time attacks and, thereby, to predict future events.

Problem of intrusions/anomalies detection is important component of information security. Intrusions/anomalies detection is a process of identification of computing or network activity which is malicious or unauthorized. Most of systems of intrusion detection systems have similar each other structure and set of components. Each IDS consists of some set of sensors or agents which inspect one or more data sources, applying some type of detection algorithm, and then dispatch warnings or react definitely in case of attack or abnormal activity detection.

Therefore, revealing of the set of informative characteristics for detection of abnormal network activity is top priority problem for solving of the task of computer systems protection from unauthorized intrusions.

2 Definition and Methods

2.1 Multifractal spectrum

Since 1993 a number of researches [1, 2, 3, 4] has shown, that network traffic in a wide spectrum of real world situations is well modeled by self-similar processes, i.e. having fractal nature.

Special sense of fractal analysis of time series, that it considers system behaviour not only in measurement period, but also its background. Analyzing alternation of parts with various fractal dimensions and how the system is influenced by external and internal factors, it is possible to learn to predict system behaviour and to diagnose and predict unstable states.

Developed approach consists in the analysis of changes of network traffic multifractal characteristics values (multifractal singularity spectrum, fractal dimension, Holder exponent, Hurst exponent etc.) and definition on the given analysis basis of the moments when system loses stability and passes in unstable state, including network attacks.

For obtaining of multifractal spectrum of network traffic we used Legendre transform [5]:

$$\alpha = \frac{d\tau}{dq} = \tau'(q),$$

$$f(\alpha) = q \frac{d\tau}{dq} - \tau(q).$$

This multifractal formalism is the most attractive from computational point of view.

2.2 Dataset

Proposed approach was tested with network traffic data. The idea is to examine if the multifractal properties of network traffic with some attacks differ from multifractal properties of normal traffic. This dataset is a version of the 1999 DARPA intrusion detection evaluation dataset generated and managed by MIT Lincoln Labs [6]. This data represents both normal and abnormal information collected in a test network, in which simulated attacks were performed. The purpose of this data is to test the performance of intrusion detection systems. The datasets contain normal data (not mixed with attacks) obtained over a period of several weeks. This provides enough samples to train the detection system.

The dataset is composed of network traffic data (tcpdump, inside and outside network traffic), audit data (BSM), and file systems data. For initial set of experiments, only the inside tcpdump network data were used, and then the tool tcpstat were applied to get traffic statistics. First week Friday's data (attack free) and the second week Friday's data, which included some attacks, were used. These attacks are described in Table 1 and Table 2.

Tab. 1. Second-Week Attack List

Date	Attack name	Start
03/12/1999	Phf	08:07:17
03/12/1999	perl (console)	08:10:40
03/12/1999	ps (console)	08:16:46
03/12/1999	Pod	09:18:15
03/12/1999	Neptune	11:20:15
03/12/1999	Crashiis	12:40:12
03/12/1999	loadmodule	13:12:17
03/12/1999	perl (Failed)	14:06:17
03/12/1999	Ps	14:24:18
03/12/1999	Eject	15:24:16
03/12/1999	Portsweep	17:13:10
03/12/1999	ftp-write	17:43:18

Tab. 2. Attack Description

Attack name	Description
crashiis	A single, malformed http request causes the webserver to crash.
eject	Buffer overflow using eject program on Solaris. Leads to a user->root transition if successful.
ftp-write	Remote FTP user creates .rhost file in world writable anonymous FTP directory and obtains local login.
loadmodule	Non-stealthy loadmodule attack which resets IFS for a normal user and creates a root shell
neptune	Syn flood denial of service on one or more ports.
phf	Exploitable CGI script which allows a client to execute arbitrary commands on a machine with a misconfigured web server.
pod	Denial of service ping of death
portsweep	Surveillance sweep through many ports to determine which services are supported on a single host.
Ps	Ps takes advantage of a racecondition in the ps command in Sol. 2.5, allowing a user to gain root access.

Number of packets parameter was selected to obtain multifractal characteristics of network traffic. This parameter was sampled each second (i.e. number of packets per second), using tcpstat.

3 Results

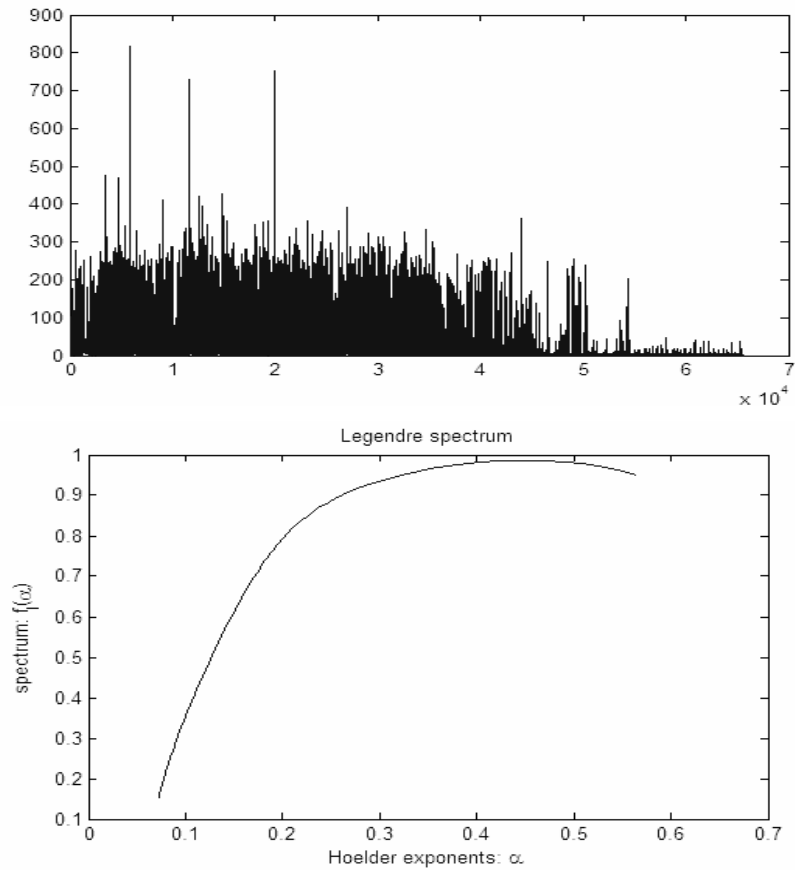
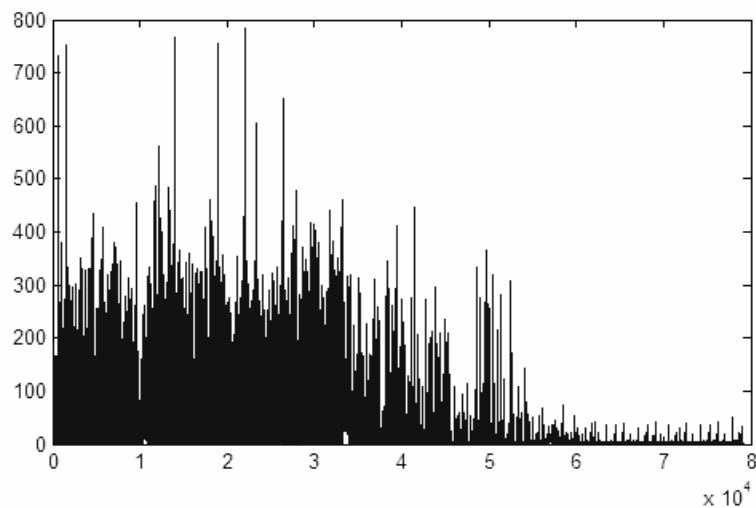


Fig. 1. Normal network traffic (upper) and its multifractal spectrum (lower)



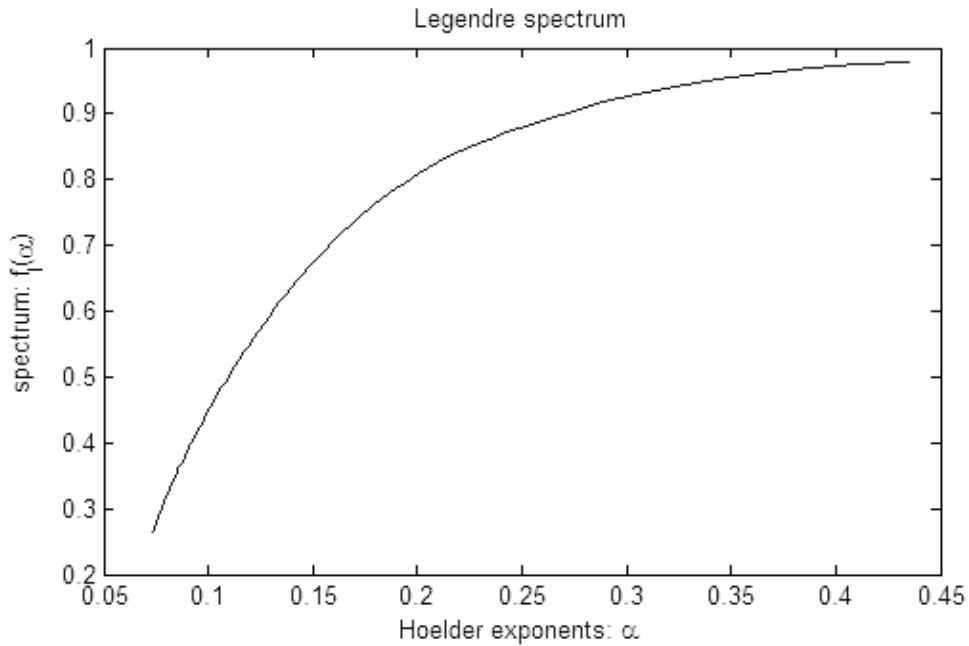


Fig. 2. Abnormal traffic (with attacks) (upper) and its multifractal spectrum (lower)

4 Conclusion

As follows from the experiment results, presented in figures 1 and 2, multifractal spectrums of two sorts of network traffic have considerable differences. Thus, multifractal formalism can be used for analysis of network traffic for purpose of revealing of abnormal network activity. Being uniform geometrical image, multifractal spectrum can be used as express diagnostic tool of network traffic structure, on which basis it is possible to compare structure of different sorts of traffic. Usage of multifractal spectrums represents as perspective tool of analysis of essential changes in network traffic under influence of malicious or unauthorized activity in the computer systems.

References

- [1] Leland, W.; Taqqu, M.; Willinger, W.; and Wilson, D. «On the Self-Similar Nature of Ethernet Traffic (Extended Version). *IEEE/ACM Transactions on Networking*, February 1994.
- [2] Crovella, M., and Bestavros, A. «Self-Similarity in World-Wide Web Traffic: Evidence and Possible Causes». *Proceedings, ACM Sigmetrics Conference on Measurement and Modeling of Computer Systems*, May 1996.
- [3] Duffy, D.; McIntosh, A.; Rosenstein, M.; and Willinger, W. «Statistical Analysis of CCSN/SS7 Traffic Data from Working CCS Subnetworks». *IEEE Journal on Selected Areas in Communications*, April 1994.
- [4] Borella, M., and Brewster, G. «Measurement and Analyses of Long-Range Packet Dependent Behavior of Internet Packet Delay». *IEEE INFOCOM'98*, April 1998.
- [5] Божокин СВ., Паршин Д. А. Фракталы и мультифракталы. Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001.
- [6] 1999 DARPA intrusion detection evaluation, MIT Lincoln Labs, 1999. [Online]. Available: <http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/index.html>