Classification of Network Traffic with Attacks

Mārtiņš Liberts[1], **Raivis Bēts**[1] **and Jūlija Asmuss**[2]
[1] Institute of Mathematics and Computer Science, University of Latvia
[2] Telecommunications institute, Riga Technical University, Latvia

The amount of network bandwidth is growing rapidly in telecommunications networks. More resources are needed to support the growing bandwidth. Different approach is needed to manage these resources. Detection of illegitimate traffic or attack in telecommunications networks is very important task. The aim of the work is to develop a mathematical framework for attack detection in telecommunications networks.

Generated and real network traffic data are used in the study. The first task was to generate artificial data representing a network traffic according to the nine classes (see table 1). The traffic time series are generated by fractional Gaussian noise (see figure 1 for examples).

Process with	No attack	Rapid attack	Slow attack
Constant trend	1-A	1-B	1-C
Growing trend	2-A	2-B	2-C
Declining trend	3-A	3-B	3-C

Table 1: Classification of network traffic

The network traffic information has to be compressed to reduce the size of it. The idea is to use Symbolic Aggregate Approximation (SAX) for this task. The aim is to find the approximation with minimal information loss. Finally the classifier has to be build that allows real-time classification of incoming network traffic. The idea is to use different data mining approaches to solve this task.

This work has been supported by the European Social Fund within the project 2013/0024/1DP/1.1.1.2.0/13/APIA/VIAA/045.

Keywords: Attack detection, Network security, Statistical detection.

References:

Xia Z., Lu S., Li J., Tang J. (2010) Enhancing DDoS Flood Attack Detection via Intelligent Fuzzy Logic. *Informatica* 34(4) (pp. 497–507). Slovenia

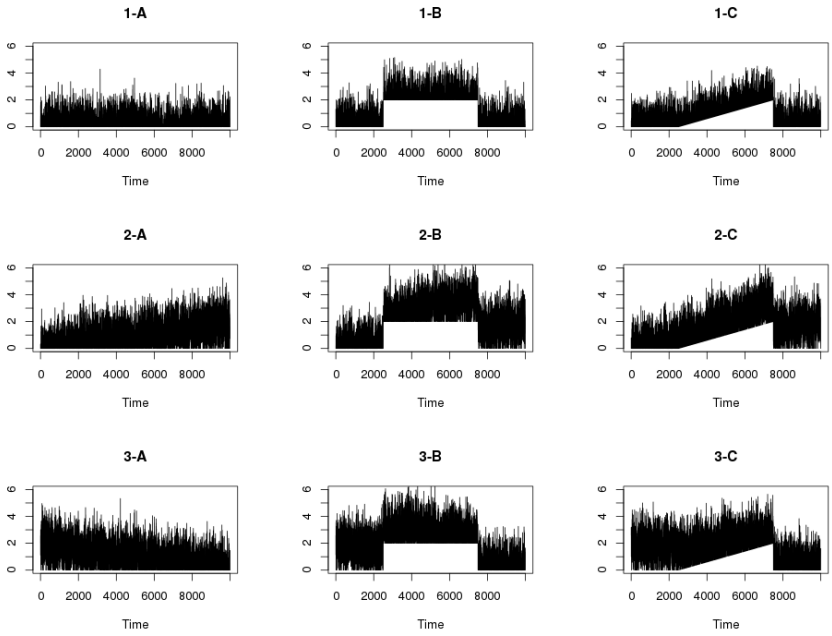

Figure 1: Examples of network traffic with attacks