Abstracts of MMA2015, May 26–29, 2015, Sigulda, Latvia

REAL-TIME NETWORK ATTACK DETECTION[1]

PETR HURTIK[1], PETRA HODAKOVA[1], IRINA PERFILIEVA[1,2], MĀRTIŅŠ LIBERTS[2] and JŪLIJA ASMUSS[3]

[1] :*Institute for Research and Applications of Fuzzy Modeling, University of Ostrava, Czech Republic*
[2] :*Institute of Mathematics and Computer Science, University of Latvia, Latvia*
[3] :*Institute of Telecommunication, Riga Technical University, Latvia*

petr.hurtik@osu.cz; petra.hodakova@osu.cz; irina.perfilieva@osu.cz,
E-mail: pm90015@lu.lv, julija.asmuss@rtu.lv

The goal of our work is to create a software for real time network attack detection and classification. We consider the network traffic specified by three different amounts of incoming data : normal, medium and huge. By the attack we denote the medium and the huge amounts of the traffic. This type of attack is known as DoS/DDoS [1]; it consists in an unusual amount of traffic delivered to the server with the aim to shoot the server down. We combine these three traffic amounts with three different trends: constant, growing and declining. Therefore, we obtain the nine classes for classification of the traffic. For a simulation a real network traffic we create artificial data using Fractional Gaussian Noise (FGN).

The traffic is generally represented by a function $z : T \to V$ where $T = \{1, ..., t_{max}\}$ is a discrete set of regular time moments and V is a certain range. We generate by FGN several representative traffic functions per each class and from them we form a reference database $\boldsymbol{z^{ref}} = \{z_1^{ref}, ..., z_\ell^{ref}\}$ where $\ell \geq 9$. Finally, we generate one input traffic time series z^{in} which is analyzed and classified in the following way. In each time moment, we take an extraction (pattern) z^P of input traffic z^{in} and compare z^P with all representatives from $\boldsymbol{z^{ref}}$. The comparison is done by computing the value of closeness. The class with the lowest closeness is assigned to the actual extraction z^P.

Naive approach is based on the pointwise comparison of entries in z^P with corresponding entries of all representatives in the reference database $\boldsymbol{z^{ref}}$. The main idea of our approach is to reduce lengths of all involved traffic time series by applying to them the F-transform [2]. We compare these reduced representations and classify each pattern of the actual data with respect to the defined nine classes.

To verify the designed algorithm, we created the input z^{in} in such a way that it contains 900 sequentially-ordered time series (100 for each class). The reference database $\boldsymbol{z^{ref}}$ is composed by 27 representatives z_i^{ref} (3 of each class) where the length of each z_i^{ref} is 10000. We processed z^{in} and made 17961 classifications. All classifications were successful; each classification takes 0.015ms of computation time. Finally, we implemented two applications: the first application runs on a client and sends UDP packets through network with frequencies given by z^{in}. The second one runs on a server, monitors number of packets and classifies the state of server in the real time.

REFERENCES

[1] C. Douligeris and A. Mitrokotsa. DDos attacks and defense mechanisms: classification and state-of-the-art. *Computer Networks*, **44** 643–666, 2004.

[2] M. Holčapek and T. Tichy. Discrete fuzzy transform of higher degree. In: *Fuzzy Systems (FUZZ-IEEE) IEEE International Conference, 2014*, doi=10.1109/FUZZ-IEEE.2014.6891848, 604–611.

[1]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