NETWORK FLOW IDENTIFICATION BY THE ENTROPY ANALYSIS METHOD

Bulakhov N.G., Kuznetsov V.S.

Tomsk State University,
Radiophysics faculty, dep. Quantum electronics and Photonics,
Russia, 634050, t. Tomsk, st. Lenin 36,
Tel.: +7-923-402-72-32,
E-mail: nik@rff.tsu.ru

IT departments of modern enterprises and Internet providers often face the problem of identification the network's information flows in order to establish their belonging to a particular class of software. Under present-day conditions the task is complicate due to the fact that the software can mask their network activity and encrypt the transmitted data.

The method of entropy analysis of the headers of data packets, which make these flows, allows to achieve a fundamentally new opportunities to identify network flows. The method consists of the analysis of the information entropy values of the headers of the data packets that are sent over the network. The calculation of entropy characteristics is carried out according to the formula of Shannon $H = -\sum P_i log_2 P_i$, where H is the information entropy, according to Shannon define, P_i is the probability of some event. This approach allows to analyze the packet headers without viewing their content. Using this feature, you can solve the problems associated with data encryption, as well as to increase the processing speed due to the low resource consumption of the method. It's necessary remark that the use of this approach gives us the high precision differentiation of the network flows (>95%), in particular in order to determine the type of software that generates network traffic and identify the spread computer worms on the network . The differentiation of the network flows can be made by measuring the information entropy of the IP- and MAC-addresses, TCP- and UDP-ports of the source and the destinations in communications packages transmitted on the network.

The software implementation of the differentiation the network flows that is used for network status monitoring of Radiophysical department of Tomsk State University has been developed by the authors. The program successfully helps to identify anomalies in the network status and to eliminate a large class of problems at an early stage of their occurrence.

References.

1. Bulakhov, N.G., Medvedev, M.D., Kuznetsov, V.S. Practical application of entropy analysis method of network flows // Russian Physics Journal, № 9/2, 2013, p. 244-246.