Information technology of traffic monitoring and analysis in computer networks

V. Kordyak, I. Droniuk, O. Fedevych

Automated control systems Department, Lviv Polytechnic National University, S. Bandery Str., 12, Lviv, 79013, UKRAINE

This article analyzes the known methods of monitoring traffic of computer networks. The notable methods of monitoring and focused on routers active and passive monitoring techniques that are not focused on routers were reviewed. Network monitoring is an important practical problem. This term was defined the constant observation of network with the goal of finding broken or slow systems, detection of problems with giving the message about them to their network administrator. These tasks are an important subset of network management tasks.

During the performance the following instruments were used: Hping3 - program for generating DoS and DDoS attacks of different types; Wireshark – the software for analyzing of Ethernet network packets and other networks (sniffer) with open source; Ptraf - a small program that can monitor all network activity of your computer; Tables - a utility for command line, standard interface for management of the internetwork screen (firewall); Netfilter – an internetwork screen (firewall) that is built into the Linux kernel of version 2.4; information technology of network monitoring developed by us.

Since monitoring methods are closely related to the objectives of maintaining efficient equipment, the uninterrupted work of the network and preventing of hacker attacks on the network, the issues, discussed in the article have a great practical importance. For effective management of the network the computer program – a network analyzer that monitors traffic was developed. Monitoring is done in accordance to the following parameters: the number of packets per time unit, the number of bits per time unit, delay time on each client point. Network analyzer consists of a server (PHP, HTML, CSS, JS) and customer (C ++ / QT) parts. The server component is analyzing the data and displaying the results. In turn, client part is collecting and processing data in network. The software released under the GNU GPL.

Active monitoring reports about problems in the network, collecting all measurements between two endpoints. Unlike active monitoring, passive collects information about only one point in the network.

Analyzer of the computer network, which is designed for providing an automated collection of information from network devices and ensuring of work process control of the communication channels, was created. It involves an automating of the process for collection and analysis of network characteristics and their displaying in a convenient format for the administrator.

Using a computer network monitoring system allows:

a) Significantly save time;

b) Automatic and round-the-clock collecting of data (jitter, delay, speed) from network devices;

c) Real-time monitoring of the network work.

DDoS attack types, their modeling methods and the problems that arise when they occur were considered, analyzed and studied. The modeling of different types of attacks and analysis of data of corresponding monitoring implemented by means of established software were carried out. The monitoring results were also compared with data of monitoring of traffic behavior, received during the DDoS attacks obtained using Wireshark. Based on these conclusions, the recommendations for prevention of DDoS attacks with the help of certain network settings were set out. For example, the attack power reduction can be achieved by limiting the number of new network connections per second. Visualization of the load on the network port of terminal equipment (webserver in intranet) was implemented.

A monitoring of network equipment was performed and rules to combat DDoS attacks was designed. A multiple algorithms for performing the help of implementation of protection from attacks or significantly reduce their negative impact were proposed. The effectiveness of the proposed methods was proved experimentally, by modeling DDoS-attacks and network monitoring, using the developed information technology of traffic analysis. For performing the experiments, despite the developed informational technology, following tools were used: hping3 - DoS and DDoS generation program for attacks of various types; iptraf - a small program, that can monitor whole network activity of the computer; iptables - command line utility, a standard interface for work management of internetwork screen (firewall) Netfilter for Linux kernels from version 2.4; netfilter – internetwork firewall, built into the Linux kernel from version 2.4. As a result, traffic data of endpoint of network equipment are visually depicted on the graph, where we can observe a significant reduction (approximately in four times) of harmful traffic after its filtering by server (router) with customizable firewall according to the developed rules. The experiments were illustrated by figures and graphs.