Detection of traffic anomalies in multi-service networks based on a fuzzy logical inference

Igor Saenko[1] , Sergey Ageev[2], and Igor Kotenko[1]

St. Petersburg Institute for Informatics and Automation
of the Russian Academy of Sciences (SPIIRAS),
14-th Liniya, 39, Saint-Petersburg, 199178, Russia

[1] {ibsaen,ivkote}@comsec.spb.ru, [2] serg123_61@mail.ru

Abstract. Methods and algorithms for detection of traffic anomalies in multi-service networks play a key role in creating the malware intrusion detection and prevention systems in modern communication infrastructures. The major requirement imposed to such systems is the ability to find anomalies and, respectively, intrusions in real time. Complexity of this problem is caused in many ways by incompleteness, discrepancy and variety of distribution laws at streams in a multi-service traffic. The paper represents a new technique for traffic anomaly detection in multiservice networks. It is based on using modified adaptation algorithms without identification and fuzzy logical inference rules. Results of an experimental assessment of the technique are discussed.

Keywords: multiservice networks, traffic anomalies, detection and prevention of invasions, stochastic approximation, pseudo-gradient algorithm, fuzzy logical inference.

1 Introduction

Nowadays, the high-speed telecommunication and next generation network technologies have a successful implementation in various information and communication infrastructures (control systems, mobile systems, transport, power supplement, economy, etc.). Progress in development of these technologies has led to the concept of a multi-service network (MSN), which kernel are the basic IP networks integrating services of speech, data and multimedia transmission, and realizing the principle of convergence of telecommunication services [1-3].

The set of main services provided to users by MSN is well known [1-3]. However, emergence of a large number of additional services in MSN make rather sharp the problem of ensuring its information security. This problem increases by following reasons: realization of procedures of dynamic change of the MSN topology; addition or exception of various, a priori uncertain, numbers of network subscribers; dynamic change of spatial arrangement of subscribers; interacting and interfacing MSN with each other, etc. Therefore, the response efficiency of the MSN control system under external and internal destructive influences is of particular importance for the network

C. Badica et al. (eds.), *Intelligent Distributed Computing X*,
Studies in Computational Intelligence 678, DOI 10.1007/978-3-319-48829-5_8

security. The normal behavior of network traffic is one of the criteria of safe functioning MSN. At the same time, it is considered that the normal traffic corresponds to a network security policy.

The traffic in the MSN is rather various [2]. It consists of multimedia traffic that is very sensitive to delays, data transmission traffic, alarm information transmission traffic, e-mail traffic, etc. At the same time, the given requirements to the quality of services (QoS) have to be fulfilled completely.

However, there are objective difficulties in creating a MSN management system and protecting the network and subscriber information. These difficulties are caused by complexity of MSN structures, MSN heterogeneity, need to analyze a large number of various network and information parameters. Therefore, fast detection of network traffic anomalies is one of the key problems of the MSN management and represents an actual scientific problem.

The paper presents a novel approach to traffic anomaly detection in a multi-service network based on fuzzy logical influence. At the same time, the rules of fuzzy logical influence are used together with the modified adaptation algorithms without identification and allow to increase stability and convergence of parameters of algorithms. The main theoretical contribution of this paper consists in the following. First, the models for the description of a multi-service traffic are offered. Secondly, the technique of traffic anomaly detection in MSN is developed. At last, experimental confirmation that the developed technique possesses almost greatest possible speed is received. The further structure of the paper is as follows. In section 2 the review of related work is given. The description of the technique of traffic anomaly detection in MSN is provided in section 3. In section 4, experimental results are discussed. Conclusions about the received results and the directions of future research are presented in section 5.

2 Related work

The main architectural decisions for MSN are considered in many works, for example, in [1-3]. These works emphasize that an important feature of the MSN structure consists in a strong segmentation of the network topology and in the existence of several points for interfacing of one MSN with other networks. As a result, the general traffic in the MSN cannot be controlled from one network point.

The technology of intelligent agents for traffic control in networks similar to MSN is proposed in [4, 5]. Intelligent agents carry out network traffic data collection, preliminary processing and transmission of data into the central devices of the control system. In such way, intelligent agents independently develop and realize the part of control functions.

[6] notes the high importance of a problem to ensure that the traffic anomaly detection systems may operate nearly in real time. This work suggests using mixed centralized-decentralized structures for implementation of the MSN control systems. Such structures allow to increase considerably the efficiency of decisions making on