Real-time Detection of Anomalies in High-speed Computer Networks

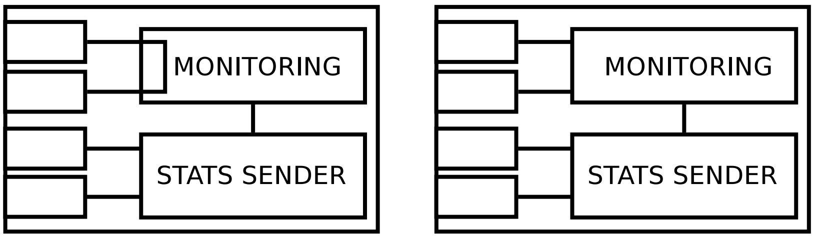
Tomas Cejka and Rudolf B. Blažek
FIT, Czech Technical University in Prague,
Thákurova 9, 160 00 Prague, Czech Republic
{cejkato2,rblazek}@fit.cvut.cz

9. 5. 2013

This paper deals with a method for detection of anomalies (e.g. attacks) in high-speed computer networks in real-time — with minimal delay while the false alarm rate is controlled at a prescribed low level. In addition, our vision is to create a monitoring system that can dynamically adapt its parameters to change its focus on more detailed information about traffic relevant to the anomaly. It will be able to dynamically increase the frequency of sampling in a subset of the observed network traffic characteristics, and start storing more information for forensic analysis.

The detection delays of the method are minimized using non-parametric sequential change-point detection. The system then precisely localizes anomalies via comparison of single line and "Broken-stick" linear models. The target of the method is detection in high-speed computer networks working at 100 Gbps speeds. With the proposed real-time detection method the system has a promise for timely reconfiguration and more sophisticated analysis of and reactions to attacks even in ultra high-speed networks.

As a proof of concept, we are currently developing the detection system using the COMBOL-1G4 card. The card is equipped with four 1 Gbps Ethernet interfaces and a VIRTEX 5 FPGA chip. We use two interfaces for monitoring and/or forwarding the traffic, and other two for management and transmission of calculated aggregate values of the observed characteristics. The two monitoring ports can be configured either as a wire-tap, or to monitor two different Ethernet lines terminated in the COMBOL card. Usage of the card interfaces is shown in Fig. 1. The card is deployed as a stand-alone monitoring probe. It is pre-loaded with our hardware design that currently counts the numbers of packets of specific types. The aggregate values (currently packet counts) from one or more probes are used as input for the detection method that is deployed on a remote detection machine. The detection system consisting of this hardware card and software will be deployed and tested on our faculty network to detect anomalies.



(a) The traffic on the Ethernet line flows through the COMBOL-1G4 card.

(b) Two separate Ethernet lines terminated in the COMBOL-1G4 card.

Figure 1: Monitoring probe: Usage of the COMBOL-1G4 card with our hardware design to monitor computer network traffic on one or two Ethernet lines.