Computer Networks 53 (2009) 810–820

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Architecture and scalability of a high-speed traffic measurement platform with a highly flexible packet classification

Detlef Saß *, Simon Hauger, Martin Köhn

Universität Stuttgart, Institute of Communication Networks and Computer Architecture (IKR), Pfaffenwaldring 47, 70569 Stuttgart, Germany

ARTICLE INFO

Article history:
Received 1 May 2008
Received in revised form 16 October 2008
Accepted 6 November 2008
Available online 3 December 2008

Keywords:
Passive traffic measurement
Packet classification
Architecture
Scalability analysis
Prototype
Hardware acceleration

ABSTRACT

Evolving network technologies, new web services and changing usage patterns continuously change traffic characteristics. But a thorough understanding of the traffic is the basis for many applications in networking. Thus, it is crucial to analyze up-to-date traffic traces collected by passive measurements in many relevant network contexts. As the traces' quality defines the significance of such analysis, the measured data is required to be complete, temporally accurate and reliable. This is especially challenging for measurements on high-speed links.

In this paper, we present a scalable architecture for a high-speed, passive measurement platform for obtaining highly accurate packet traces. Its functional blocks are distributed to a specialized hardware unit and a commodity PC unit according to their specific requirements. For pre-processing, the hardware unit integrates a protocol-aware classification and filtering module which allows an easy definition of classification and filtering rules. We analyze the platform's scalability and support this by a implementation with current FPGA technology and a standard server PC.

1. Introduction

In recent years, the penetration of fixed and wireless broad-band Internet access has increased all over the world. While less then 10 years ago, the access to the Internet was dominated by dial-up access with low bit rates, today there is a strong trend towards always-and-everywhere-connected users. Due to this, users change their behavior as well as their usage patterns. On the one hand they still use established services but in a different way, e.g. more frequently. On the other hand, they use new upcoming services with new usage paradigms. For the future, it is according to e.g. [1] foreseeable that such changes will happen due to the introduction of new services and the Web2.0 boom.

Within the networks this shift has changed the traffic characteristics with respect to both the temporal behavior as well as the protocols used and protocol stacks. Examples for this today are the well known self-similarity [2,3] or the long range dependence [4] that is even present in the Internet backbone [5] as well as a partial shift from Peer-to-Peer traffic back to web traffic induced by the broad usage of e.g. video services like YouTube [6].

Clearly, a deep understanding of the traffic characteristics is the basis for many applications in networking. This ranges from the design and evaluation of new network architectures to the management of operational networks. This understanding as well as corresponding models are provided by *traffic characterization* and *traffic modeling*.

Traffic characterization analyzes the current traffic and extracts the relevant characteristics. For this, commonly characteristic properties and metrics are derived from traffic traces that are captured on relevant network links. For generalization, sets of traces are analyzed that are captured at different locations and/or at different instants of time.

* Corresponding author. Tel.: +49 711 68569003; fax: +49 711 68559003.
E-mail address: detlef.sass@ikr.uni-stuttgart.de (D. Saß).

1389-1286/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.comnet.2008.11.010

Traffic modeling derives from these characteristics mathematical or algorithmic models of the traffic for certain scenarios. These models are capable of being parametrized by the user to adapt them to their needs.

Obviously, the determined characteristics and models can only reflect the behavior of the underlying traces. Accordingly, it is crucial to analyze sufficiently detailed traffic traces collected in many relevant contexts. This leads to a major trade off: to elaborate the balance between traced details and data volume or capturing rate. This is especially important for long-term traces at the packet level in high-speed networks, as simply recording all packets entirely would lead to trace sizes of several terabytes in a short time.

Beyond dumping the raw data, more intelligent solutions pre-process the packet stream before recording in non-volatile memory. This contains e.g. filtering to reduce the captured data volume and rate, or further processing operations to preserve the users' privacy.

In this paper, we present the architecture of our high-speed passive measurement platform, the I^{2}MP (IKR Internet Measurement Platform). We discuss major scalability aspects supported by numerical results of fittings to current FPGAs (Field Programmable Gate Arrays). We tailored the design to support long-term capturing of packet traces on high-speed metro and core network links lasting for days. We realized the performance critical and time critical tasks in a dedicated hardware unit and implemented complex post-processing operations as well as storage on commodity PCs. With this, we enable high-precision and high-performance traffic capturing while keeping the complexity low.

To reduce the data volume on the fly, we integrate a hardware Classification and Filtering unit. This unit extracts arbitrary user-defined byte areas of the packets for recording and discards the remaining data. For this, it automatically decodes the protocol stack of each packet on the basis of a configurable set of arbitrary protocols. It then applies for each protocol layer separately the classification rules as well as the filter rules. Our architecture allows the flexible adaptation of both rule sets as well as of the protocol definitions, even during operation.

The rest of the paper is structured as follows: Section 2 reviews the traffic measurement principles, the relating relevant functional blocks and suitable platforms for measurement systems. Section 3 introduces the architecture of our measurement platform I^{2}MP. In Section 4, the scalability of the architecture with respect to the throughput as well as the number of classification rules is discussed. Realization aspects, implementation results and the deployment are shown in Section 5. Finally, the paper closes with conclusions and an outlook to future work.

2. Traffic measurement

In the literature as well as in practice traffic measurement is widely discussed and used. In the following, we will discuss the different aspects and the scope of traffic measurement, present its common fundamental functional building blocks and review the various approaches for the realization of traffic measurement on different platforms.

2.1. Principles

Traffic measurements differ with respect to the measured data as well as the measurement methods. The measurement purposes span a large scope and determine the methods to obtain the measured data. In the following, we will briefly discuss the fundamentally different measured data types, describe the main measurement methods and, finally, discuss the major measurement purposes.

Measured data is based on packets either from the entire traffic or from a filtered subset of it. It is classified to either unmodified sections of packets, e.g. protocol headers, or to processed values of them. Processed values are for example statistical data calculated from the packet data (e.g. histograms for packet sizes) or data on a higher abstraction level than packet-level (e.g. flow-level).

In addition to the measured data, also time information is recorded when each datum is collected. The required accuracy of this time information varies largely for different measurement purposes. This has to be carefully examined which is a challenging task for many purposes [7].

Measurement methods are classified into passive and active methods. Passive measurements collect traffic without impacting the traffic of the observed links. Active measurements inject additional traffic on the link. Both methods are performed at either a single link or spatially distributed at multiple links simultaneously.

The major *measurement purposes* are network management, network control and traffic characterization and modeling. These purposes possess rather different requirements on traffic measurement.

For network management, measurements are performed for health monitoring, troubleshooting and accounting. The measured data is mainly counter statistics and flow data from multiple network nodes [8]. For network control various different data is measured by a broad range of methods depending on the specific needs. Common to these applications are that the measured data is usually not stored but immediately used for decisions or further processing steps [9].

The purpose of traffic measurement focused on in this paper is traffic characterization and modeling. Here, the main target is to enlarge the understanding of the traffic and derive appropriate traffic models for analysis, simulation or emulation. The requirements for such measurements vary heavily and depend on context and objectives of the analysis or the modeling. However, for an accurate understanding of the traffic behavior with its underlying principles, sets of measured data are necessary that are rich in detail and that cover a long time span. Such measured data is collected by passive measurements.

These measurements usually result in huge sets of measurement data, especially when recording high-speed links. So, special requirements are imposed on these measurements, which lie in particular on the correctness of the measured data with respect to time, completeness, storage and post-processing.

In the following we will focus on passive traffic measurement at high-speed links for the purpose of traffic characterization and modeling. Subsequently, we will simply use the term traffic measurement for it.