A P2P-Based Framework for Distributed Network Management

Andreas Binzenhöfer¹, Kurt Tutschku¹, Björn auf dem Graben¹, Markus Fiedler², and Patrik Arlos²

¹ Department of Distributed Systems, Institute of Computer Science, University of Würzburg, Am Hubland, 97074 Würzburg, Germany
{binzenhoefer, tutschku, adgraben}@informatik.uni-wuerzburg.de

² Dept. of Telecommunication Systems, School of Engineering, Blekinge Institute of Technology, 371 79 Karlskrona, Sweden
{markus.fiedler, patrik.arlos}@bth.se

Abstract. In this paper we present a novel framework supporting distributed network management using a self-organizing peer-to-peer overlay network. The overlay consists of several Distributed Network Agents which can perform distributed tests and distributed monitoring for fault and performance management. In that way, the concept is able to overcome disadvantages that come along with a central management unit, like lack of scalability and reliability.

So far, little attention has been payed to the quality of service experienced by the end user. Our self-organizing management overlay provides a reliable and scalable basis for distributed tests that incorporate the end user. The use of a distributed, self-organizing software will also reduce capital and operational expenditures of the operator since fewer entities have to be installed and operated.

1 Introduction

A peer-to-peer (P2P) system is a highly distributed application architecture. The underlying technology has so far only received a doubtful reputation due to its use in file sharing applications. P2P algorithms, however, might be highly helpful in implementing novel distributed, self-structuring network management concepts. In this work we suggest the application of a current generation, structured P2P overlay network for fault and performance management with the aim of enhancing conventional management functions.

In general the goal of Network Management is “to ensure that the users of a network receive the information technology services with the quality that they expect” [1]. However, monitoring and provisioning of that quality in an end-to-end manner as perceived by a user [2] is rarely achieved. The monitoring is usually carried out by rather centralized entities (Network Management Systems) and only in those parts of the network a provider is responsible for. Coordination of the monitoring among different administrative domains is rarely achieved, which also affects possibilities to locate faults and to evaluate end-to-end QoS.
A central fault testing and QoS monitoring architecture typically results in additional, complex entities at the provider. The operator has to ensure the reliability of the entities and assess their scalability. The systems have to scale with $O(N^2)$ due to the $N(N-1)$ potential relationships among $N$ end systems. In addition, relaying monitoring data consumes bandwidth, delays its availability, and might get lost in case of a network failure. A decentralized QoS monitoring, as for example, located on the user’s end system, might avoid these disadvantages. The use of a distributed, self-organizing software will reduce capital and operational expenditures (CAPEX and OPEX) of the operator since fewer entities have to be installed and operated. Scalability can be achieved by re-using resident resources in conjunction with local decisions and transmission of less data.

We propose a new, distributed, self-organizing, generic testing and QoS monitoring architecture for IP networks. The architecture will complement today’s solutions for central configuration and fault management such as HP OpenView [3] and IBM Tivoli [4]. The architecture is based on equal agents, denoted as Distributed Network Agents (DNA), which form a management overlay for the service. In this context the word agent is not to be understood as an agent as used by the Artificial Intelligence community, but rather as a piece of software running on different peers, like, e.g., an SNMP-Agent. The self-organization of the overlay is achieved by Kademlia [5], a P2P-based Distributed Hash Table (DHT).

The suggested architecture facilitates the autonomic communication concept [6] by locally determining the perceived QoS of the user from distributed measurements and by exploiting the self-organization capabilities of the DHT for structuring the overlay. It will be able to communicate with standard-NMS via well-established interfaces. Thus, it can be seen as a QoS-enabling complement of existing Network Management solutions.

The remainder of the paper is structured as follows: Section 2 introduces the architecture of a DNA and shows how the framework can be used for local and distributed tests. In Section 3 we give an overview of the current P2P generation and motivate why we chose Kademlia as the basis of the DNA overlay. Some details about the implementation of our prototype will be given in Section 4. The functionality of the DNA is validated by simulation in Section 5. Section 6 finally concludes the paper and summarizes our future work.

2 The DNA Framework

The DNA framework represents an independent distributed application intended to support the central network monitoring station. In general a central monitoring entity has three major disadvantages:

- It is a single point of failure. Once the single central monitoring unit fails, the network will lose its control entity and will be without surveillance. The same problem could, e.g., be caused by a distributed denial of service attack. That is, the functionality of the entire network management depends on the functionality of a single central unit.