Internet Service Delivery Control with Mobile Agents

Manuel Günter and Torsten Braun
Institute of Computer Science and Applied Mathematics
Neubrückstrasse 10, CH-3012 Bern, Switzerland
http://www.iam.unibe.ch/~rvs/

Introduction

The rapid growth of the transport capacity of the Internet and the global trend towards liberalisation of the telecommunication market forces the Internet service providers (ISP) to look for new revenues beyond pure connectivity offerings. Therefore, ISPs that control their own network try to introduce new Internet services including quality features such as premium transport or traffic privacy through encryption. However, before the customer will pay for such services the following two problems need to be addressed: (1) How can the provider prove that the desired service is really delivered to the customer? For example, it is difficult to show that the provider transfers the customer's data with strong encryption. (2) For services involving collaboration of providers (e.g. end-to-end QoS) the question is how to find out who is responsible when the service quality is less than guaranteed to the customer.

It is in the interests of the customers and of honest providers that the customer is able to verify the permanent quality of a network service and to locate problems when they occur. We refer to this process as *service delivery control* (SDC).

For today's Internet services there is only very limited support for service delivery control. If a customer happens to detect a problem (which usually happens when the customer needs that service badly and does not get it), phone-calls between administrators, local measurements, and manual browsing of log-files will eventually lead to the identification of the problem source. Unfortunately, it is also not uncommon that the involved parties will suspect each other and repudiate any guilt. Note, that this problem not only concerns the relation between customer and provider but also between providers themselves. It is to be expected that the problem becomes worse when new and more expensive network services are deployed that require provider collaboration.

We propose to use a generic service delivery control architecture based on mobile agents [Whi94, CHK97]. Mobile code allows the customer to test the service where it is delivered. Software agents as well-defined code entities facilitate the deployment of secured environments.

Mobility and Service Delivery Control

Mobile agents have been proposed for a wide range of tasks. However, code mobility has few provable advantages besides of being a catching metaphor. The following reasons describe why mobile agents are particularly useful for service delivery control agents.

Data source location. Network services are per-definition delivered *in* the provider network. It thus makes sense to (at least pre-) process the measurement data there (at the source).

Generic interface. By providing an agent platform at relevant sites the provider can give access in a controlled fashion.

Flexibility. A general-purpose agent programming language provides the expressive power needed to cope with the unforseeable IP services of the future.

Trust through source code. The customer sending the agents has insight to the agent's code. Therefore, the customer can verify what is being measured.

Cross checking. A misconducting provider can easily fool a customer that relies on the measurements published by the provider. In a a multi-provider service scenario the situation is even worse. SDC agents can be sent out to perform active measurements by producing and measuring traffic at different sites. Mobility allows the agents to virtually 'track-down' the problem source.

Performance. Mobile agents structure distributed computing thereby enabling the customer to collect computing power to analyse the traffic. Furthermore, mobile agents preprocess the measurement data where it is produced, thus reducing the network load.

Given these arguments we can say that even if the providers would allow their customers to access SNMP (IETF RFC 1157) agents of their equipment, the expressive power of a mobile agent based SDC approach exceeds by far what can be done by traditional SNMP based monitoring.

A Supporting Infrastructure for Service Delivery Control Agents

Agents are executed in protected node environments. We propose to locate these environments at the peering point between autonomous IP networks (see figure 1 left). The SDC architecture should not facilitate eavesdropping other customers' traffic, spoofing of foreign IP addresses or denial-of-service attacks. Given these requirements we foresee the following node architecture as shown in figure 1 (right): At the peering router, there is a *T-component* that serves as a high-performance and configurable packet copying mechanism. It adds a high-accuracy time-stamp to the packet. The T-component forwards the requested packet copies to the *Node environment*. Note, that for security reasons the agents do *not* have direct access to neither the T-component nor the packet copies. The node provides an execution environment (user-level thread in a 'sand-box') for each agent. The agent's execution environment contains an inbound and an outbound packet queue secured with a policy-based filter which ensures that the agent can only see traffic for which it is authorised.

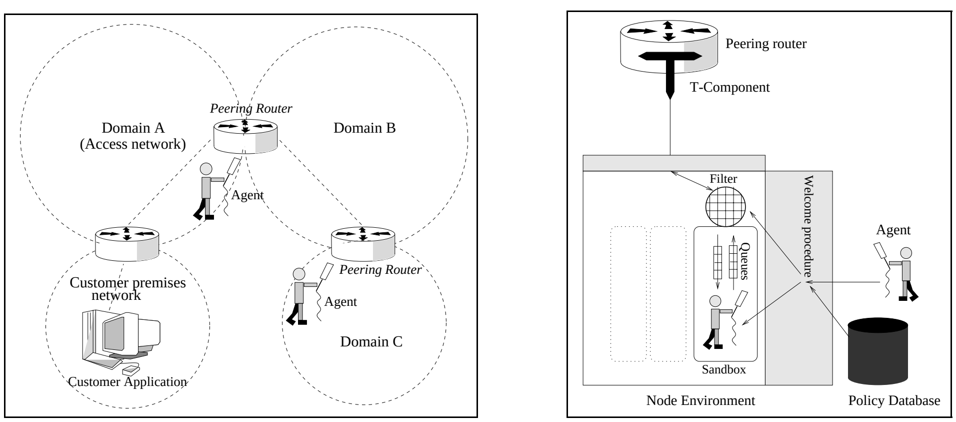

Figure 1: Measuring at peering points (left). The node environment (right).

Examples of Customer Controlled IP Services

IPSec (IETF RFC 2401) virtual private network control agents. We are developing SDC agents that perform the following checks: (1) Leaking of Intranet traffic into the public Internet. (2) IPSec protocol conformity. (3) Key exchange (IKE) activity survey. (4) Statistical tests on authentication and encryption quality.

Differentiated services (IETF RFC 2475) control agents. We are developing SDC agents that perform the following checks: active and passive measurement of packet loss, delay and jitter.

References

[CHK97] David Chess, Colin Harrison, and Aaron Kershenbaum. Mobile agents: Are they a good idea? In Jan Vitek and Christian Tschudin, editors, *Mobile Object Systems: Towards the Programmable Internet*, number 1222 in LNCS, pages 25–45. April 1997.

[Whi94] James White. Telescript technology: The foundation for the electronic marketplace. General Magic White Paper, 1994.