INTERMON: an Architecture for Inter-domain Monitoring, Modelling and Simulation

Elisa Boschi[1], Salvatore D'Antonio[2], Paul Malone[3] and Carsten Schmoll[1]

[1] Fraunhofer FOKUS,
Kaiserin Augusta allee, 31 10589 Berlin, Germany
{elisa.boschi, carsten.schmoll}@fokus.fraunhofer.de
[2] Lab. ITEM – Consorzio Interuniversitario Nazionale per l'Informatica (C.I.N.I.)
Via Diocleziano, 328 80125 Napoli, Italy
salvatore.dantonio@napoli.consorzio-cini.it
[3] Telecommunications Software and Systems Group, Waterford Institute of Technology
Cork Road, Waterford, Ireland
pmalone@tssg.org

Abstract. In this paper we present a flexible architecture providing a communication platform between heterogeneous components for inter-domain QoS and traffic analysis in large-scale, multi-domain Internet infrastructures.

1 Introduction

Performing traffic analysis and guaranteeing inter-domain Quality of Service, or QoS, in large-scale, multi-domain Internet infrastructures is a challenging task. It involves performing real traffic measurements, analysing that traffic, ideally combining that data with routing information to match it to the network structure.

INTERMON provides different domains with a common infrastructure that offers several facilities used to gain a complete knowledge of network status as well as to perform QoS analysis in an inter-domain environment. For the user, INTERMON provides modelling, simulation and visualisation capabilities. In particular, a QoS modelling toolkit supports the analysis of network behaviour and various simulation techniques are used to study performance by proposing "what if" scenarios for traffic and topology. A visualisation component performs filtering, mapping and rendering to display resources and traffic flows for QoS planning.

2 The INTERMON Architecture

The INTERMON architecture specifies the interaction of the system components. It allows the system to monitor the current state of processing of measurement and simulation tasks and to store that state so that it is accessible to tools and users.

Figure 1 shows the logical "intra-domain" architecture setup (i.e. these components are present in each domain) highlighting the four layers of which it is composed: user interface, central control and storage, tools adaptation, and the tools layer. The architecture is built around a central server component called a Global Controller (GC). The Global Controller's main role is to coordinate interaction between the attached components such as clients, visualisation, measurement and simulation and to maintain the status of currently active tasks.

For communication between Autonomous Systems (ASes) the GC integrates methods for Authentication, Authorization and Accounting -secured communication [1]. More details on the inter-domain communication and the architecture prototype implementation are to be found respectively in [2] and [4].

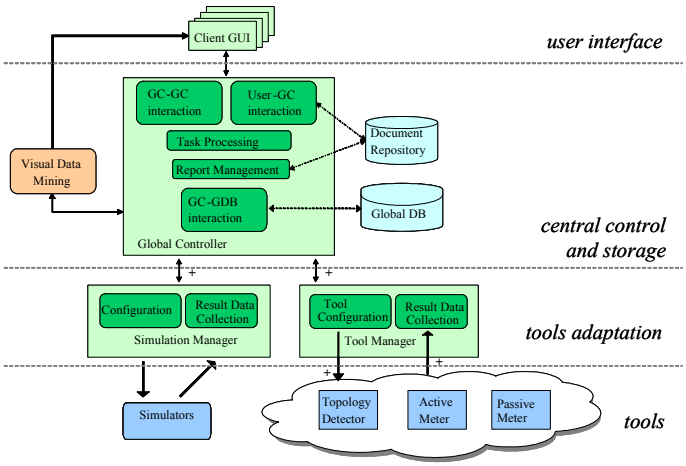

Fig. 1. The INTERMON Architecture

3 Scenario 1: SLA Violation Analysis

In this scenario a violation of an SLA has occurred and has been reported to the provider by the customer.

1. The provider performs a topology discovery for the period in which the violation occurred. The INTERMON database maintains a history of BGP-4 routing data and can be queried for the topology at the time of the violation. The result of such a query is an XML representation of the BGP topology and the visualisation of the topology showing the autonomous systems involved as well as whatever border routers have advertised their updates to the external repository. All of these tasks are performed through the use of the INTERMON tool *InterRoute*.
2. The *QoS Pattern Analyser* is used to compare end-to-end QoS data measured at the time of the violation (if available) with the violation and the BGP-4 topology. It has been shown in the project that there can be a relationship between frequent

route changes (which can be seen by observing BGP-4 updates) and degradation in QoS measurements.

3. The provider can use the visualised topology obtained in step 1 to configure a monitoring probe called *MRCollector*, which can help the provider discover monitoring probes in the network. If a probe exists on the queried network element then a list of interfaces, which can be monitored on the element, is returned to the INTERMON GUI. The provider can then use the INTERMON GUI to configure a "campaign" to monitor activity on that interface.
4. QoS/Traffic measurements are evaluated. Through the integration of the above-described tools it is possible for the provider to gain an insight into the behaviour of the network to aid in identification of the cause of the reported violation.

4 Scenario 2: "What if" Analysis

Modelling and simulation of network configurations allows operators to conduct "what if" type analyses of current or planned systems. Four separate inter-domain network simulators were developed and integrated into the INTERMON architecture (Cf. [3]). In order to validate them, a test bed was set up as in Fig 2 and a comparison of simulation results was made with the actual measured results from the test bed.

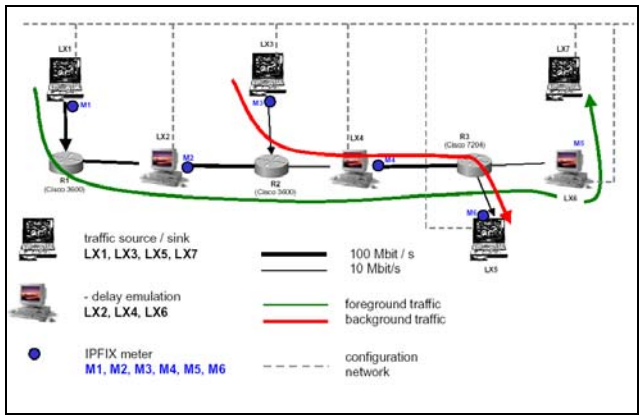

Fig. 2. The INTERMON test bed

The test bed consists of three Cisco routers, three Linux PCs configured to emulate network delay and four Linux end systems for traffic sources and sinks. The basic scenario is that delay sensitive foreground traffic is transmitted from LX1 to LX7. While this is happening, background traffic is transmitted from LX3 to LX5. Depending on the amount of traffic from LX3 to LX5 a bottleneck is created. The foreground traffic for this control scenario was 10 G.711 VoIP flows with a payload of 160Bytes every 20ms on each flow. The background traffic is high quality MPEG-4.

To start the simulation through the INTERMON GUI, the user must select the simulation tool to be used, choose the BGP topology representing the test bed between a set of previously stored ones, specify parameter values. When the simulation

job is complete the user can retrieve a visualisation of the result by requesting this from the Visual Data Mining Module where filters are applied to the data and it is transformed to visual format.

For each of the implemented simulators, the results were compared with the measured data described above. One of these comparisons for the NS2-Hybrid simulator is shown in Fig. 3. A comprehensive evaluation of the individual simulation approaches is provided in [5].

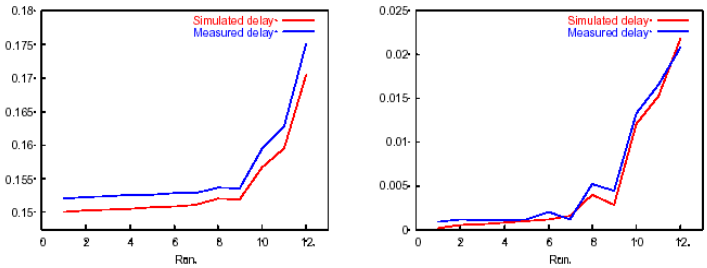

Fig. 3. Comparison of testbed measurements with NS2 Hybrid simulation

5 Conclusions

In this paper we have presented the INTERMON architecture, which integrates tools to study the impact of traffic and topology for end-to-end QoS in an inter-domain environment. The system comprises active and passive meters, topology detection components, and a modelling and simulation toolkit. The INTERMON system has been implemented, and subsequently validated through the scenarios shown in this paper.

6 Acknowledgements

This work has been performed under the partial financial support of IST project INTERMON IST-2001-34123, http://www.ist-intermon.org

7 References

[1] AAA, IETF web page: http://www.ietf.org/html.charters/aaa-charter.html
[2] Elisa Boschi, Salvatore D'Antonio, Giorgio Ventre, «Inter-domain Communication and Data Exchange», In Proceedings of IPS 2004, Budapest, Hungary, March 2004.
[3] INTERMON Deliverable 11: "Integration of the Inter-Domain Modelling and Simulation toolkit", 2003, InterMon project homepage: http://www.ist-intermon.org
[4] INTERMON Deliverable 15: "Final Architecture Specification", 2004
[5] INTERMON Deliverable 19: "Evaluation of Inter-Domain QoS Modelling, Simulation and Optimization", 2004