

In this issue:

Research & Development

Measurement based QoS analysis of inter-domain scenarios using a fluid-based simulation model

Ch. Brandauer

Scenarios

Inter-domain QoS/SLA monitoring – different Approaches using INTERMON

I. Miloucheva

Measurement based QoS analysis of inter-domain scenarios using a fluid-based simulation model

Ch. Brandauer

The INTERMON project develops a toolkit that supports a network operator in tasks like performance monitoring, traffic measurements, and topology discovery. These modules provide the basis for the modelling and simulation tools that are also provided as part of the toolkit. The goal of these tools is to enable quality of service (QoS) studies. Simulations are typically employed in so called “what-if” scenarios: “What is the impact on delay if the load on transit link from domain A to B is increased by X percent?”

One of the simulation models developed within the project is a continuous signal flow simulator called RTC-FSIM (Rate and Time Continuous Fluid Simulation). The main objective of this simulation tool is to allow an easy and natural integration with traffic measurements and to enable high performance simulation of large scale inter-domain scenarios.

Obviously, the simulation of large-scale scenarios cannot be done by a per-packet simulation. Large topologies and high bandwidth links have a huge number of parallel packets in the simulation system. This requires an event based packet simulator to store a huge system state (memory intensive) and to process a very large number of simulation events (computationally intensive). Such a type of simulator does thus not scale well to large-scale scenarios.

The first step towards a scalable simulation model is an approach where traffic streams are modelled as chunks of fluid flows. The monitored individual packet arrivals are

aggregated to traffic load events, e.g. per 100 ms, and the simulation process is now triggered by these traffic load events instead of individual packet arrivals / departures.

In our approach we made a rigorous next step of traffic modelling by considering this discrete load process as a continuous “fluid” process. To keep the most important process characteristics - mean, variance, and autocorrelation - the continuous fluid process is derived from the discrete fluid process by a newly developed iterative algorithm. With this abstraction inter-domain links become continuous queuing systems and the dynamic relations between incoming fluid-traffic, service link rate, buffer occupation, loss rate, etc. are described by differential equations.

The implementation of this approach can be based on already existing, powerful simulation tools like Simulink. There we implemented the model of a server station as a new library object. The server station has three input signals and three output signals as depicted in figure 1.

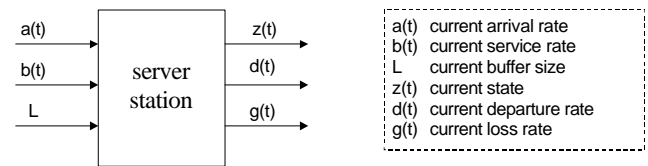


Figure 1: Rate and time Continuous Fluid model

Inside the server station are the implementations for computing the station’s current state, departure and loss rate. The underlying differential equations are shown in figure 2.

state

$$\frac{dz(t)}{dt} = \begin{cases} 0 & \text{if } (z(t)=0 \text{ and } a(t) \leq b(t)) \text{ or } (z(t)=L \text{ and } a(t)-b(t) \geq 0) \\ a(t)-b(t) & \text{else} \end{cases}$$

departure rate

$$d(t) = \begin{cases} \min\{a(t), b(t)\} & \text{if } z(t) = 0 \\ b(t) & \text{if } z(t) > 0 \end{cases}$$

loss rate

$$g(t) = \begin{cases} a(t)-b(t) & \text{if } z(t) = L \text{ and } a(t)-b(t) \geq 0 \\ 0 & \text{else} \end{cases}$$

Figure 2: Differential equations

We also developed extended versions of a server station that have support for QoS service models like priorities and weighted fair queuing.

To optimally support the network operator / planner, a high degree of automation is employed to create the simulation: topology information is imported from the BGP / traceroute / other tools that deliver topology structure. Traffic load information is imported from the monitoring database (IPFIX standard) into the simulation. The details of the Simulink model are completely hidden from the user who interacts only with the GUI. There the user can configure the scenarios of interest (“what-if”) by changing the traffic load or modifying the topology (e.g. deactivate a link to simulate the impact of link failure or add a new link to analyse the impact of a new peering agreement).

An example screenshot of the GUI is shown in figure 3:

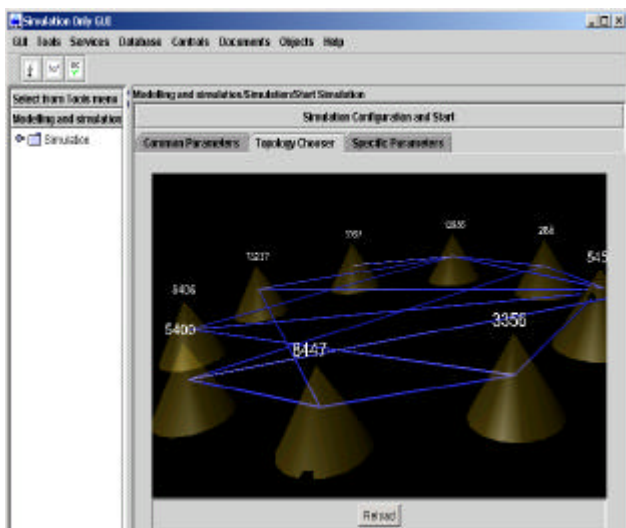


Figure 3: Simulation GUI

In general the fluid simulation algorithms run on a digital computer and the time progress of the differential equations will be approximated by discrete „sufficiently small“ time steps. The dependencies between simulation performance (accuracy, simulation time) and the size of the simulation time step will be investigated in the next project period. Running the fluid simulation with sufficiently small time intervals may be interpreted as a step backward to the granularity of the criticised per packet simulation but today’s powerful numerical processors are able to solve the approximations for differential equations very efficiently.

Finally, a very high degree of accuracy may not always be the main interest in large inter-domain scenarios and the ability to arbitrarily choose the trade-off between simulation accuracy and performance is a powerful feature.

Scenarios

Inter-domain QoS/SLA monitoring – different Approaches using INTERMON

I. Miloucheva

The inter-domain monitoring has the goal to obtain performance characteristics of inter-domain networking infrastructure – inter-domain topology and routing, connectivity based on border router and exchanges.

1. Differences in inter-domain and intra-domain monitoring

The interfaces between the ISPs, e.g. border router and exchanges as well as the inter-domain paths using these interfaces are the main focus of inter-domain monitoring in contrast to the intra-domain monitoring where the core router and the connections within an ISP provider are the primary interest.

In the most cases there are the same QoS and traffic measurement tools used in the intra- and inter-domain monitoring, but the tools are used in different monitoring strategies and situations, e.g. scenarios. In the intra-domain monitoring, the ISP provider has a full control on the monitored infrastructure, in the inter-domain monitoring this is not possible, only the ISP’s own border interfaces are controlled by the ISP provider.

This results in the *different monitoring strategies of inter-domain and intra-domain infrastructures*. Where in the intra-domain monitoring the direct measurement and monitoring of networking devices (e.g. core and access router) is in each case possible, in the inter-domain monitoring the direct measurements are completed by indirect measurement strategies based on inferencing of performance (e.g. network tomography [PMHN 03]). This means to obtain conclusions of performance of direct measurable border router or inter-domain paths, which are point of interest, based on direct measurements of other inter-domain connections or paths.

Inter-domain and intra-domain monitoring scenarios could support network engineering tasks in same areas, e.g. planning, fault management and connectivity optimisation, but with different goals and situations. The inter-domain monitoring scenarios are focussed to obtain useful information for planning and performance fault detection based on monitoring of QoS and traffic of inter-domain paths, at and between inter-domain interfaces, at

border router as well as monitoring of inter-domain routing activity and quality, where the intra-domain monitoring is aimed to support the planning and fault detection based on monitoring of core router connectivity. The optimisation of inter-domain connectivity (monitoring of QoS on multihoming paths and spatial QoS composition in inter-domain environment) is a goal of wide range of inter-domain monitoring scenarios in contrast to the optimisation of intra-domain connectivity.

Where the *QoS and traffic monitoring tools are almost the same in the inter-domain and intra-domain monitoring*, and only the monitoring strategies and scenarios are different, there is a *significant difference in the topology discovery and routing monitoring*. Where the inter-domain monitoring is aimed to discover inter-domain routing topology and BGP-4 behaviour, the focus of the intra-domain monitoring is intra-domain routing and OSPF protocol.

2. Inter-domain monitoring – different approaches in INTERMON

The inter-domain monitoring is aimed at different areas:

1. Inter-domain topology monitoring and discovery

- the inter-domain connection topology monitoring (e.g. changes of the topology of inter-domain paths, BGP-4 routing events of inter-domain paths, availability of the router of the inter-domain paths - inter-domain, intra-domain and access devices)
- discovery of inter-domain topology (e.g. possible inter-domain connections between two end systems, multi-homing topology monitoring)

2. QoS parameters and bandwidth monitoring of inter-domain connections (e.g. connections between border router and exchanges points)

- direct measurement of inter-domain QoS parameters, e.g. QoS parameters of connections connecting inter-domain devices (e.g. border router, exchange points)
- bandwidth measurement of inter-domain connections

3. Traffic and QoS monitoring of inter-domain devices

- direct measurement of traffic at inter-domain devices
- direct measurements of QoS and bandwidth provided by the inter-domain device

4. QoS parameters of end-to-end connections including inter-domain paths

- direct measurement of end-to-end QoS parameters, e.g. QoS parameters of connections connecting end-systems via inter-domain paths

- direct measurement of access QoS parameters, e.g. QoS parameter of connections connecting access systems via inter-domain paths.

INTERMON includes tools for performing of the inter-domain monitoring in the different areas which can be used separately or in the combination.

The following table shows the relationships of the INTERMON tools to the different tasks and requirements for direct monitoring of inter-domain devices (border router, exchange point, etc):

Inter-domain monitoring tasks	INTERMON tools	Direct Inter-domain Device Monitoring
Connection topology of inter-domain path - Router availability and changes of the inter-domain path - BGP-4 routing events, inter-domain routing changes and discovery of inter-domain topology (multiple paths, multi-homing) which include exchange points	CM Toolset Traceroute InterRoute	Not required Not required (RIPE access)
QoS parameters and bandwidth monitoring of inter-domain connections	MRCollector	Required
Traffic and QoS monitoring of inter-domain devices	IPFIX meter (traffic) QoS (MRCollector)	Required
QoS parameters of end-to-end connections including inter-domain paths	CM toolset	Not required

Table 1: INTERMON tools for performing of inter-domain monitoring tasks

Using the tools in combination allows to perform new tasks. An example is obtaining of spatial inter-domain QoS composition based on end-to-end QoS monitoring combined with inter-domain monitoring of connections. A main problem of the inter-domain monitoring is the direct access and control of inter-domain devices. Some of the monitoring tasks require such control, as for instance:

- QoS parameters and bandwidth monitoring of inter-domain connections (e.g. connections between border router and exchanges points)
 - Traffic and QoS monitoring of inter-domain devices
- The ISP provider or customer interested in inter-domain monitoring does not have control to all inter-domain devices, in case of ISP provide there is a control only to the own devices and in case of customer there is no control at all. Therefore there is a sense to differentiate between scenarios based on tools aimed at direct monitoring of inter-domain devices and connections and scenarios based on tools which do not need to have access and control to inter-domain devices. The second group of scenarios are in each case of interest for the customer and ISPs interested to obtain inter-domain monitoring data for network infrastructures which do not belong to them. The monitoring data obtained by the indirect inter-domain monitoring over end-systems and egress points is not so exact as the data obtained by direct monitoring. However, in case of long term measurement and modelling, inferencing of end-to-end monitoring data over inter-domain paths could be done with topology and inter-domain routing changes.

3. Example scenario for end-to-end QoS monitoring

Here, for instance an example of INTERMON measurement of end-to-end connection between Brazil (Sao Paulo) and Austria (Salzburg).

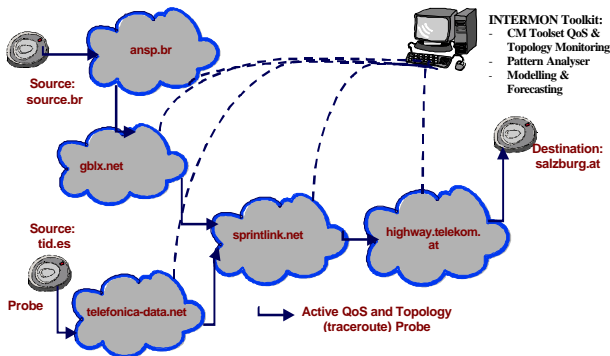


Figure 1: End-to-end QoS monitoring trial of inter-domain path

In the long term measurement, obvious were the QoS outliers (e.g. abnormal extreme values) for end-to-end mean and maximum delay (shown in figure 2) which could not be explained with the observed behaviour in the long term measurement (2 months).

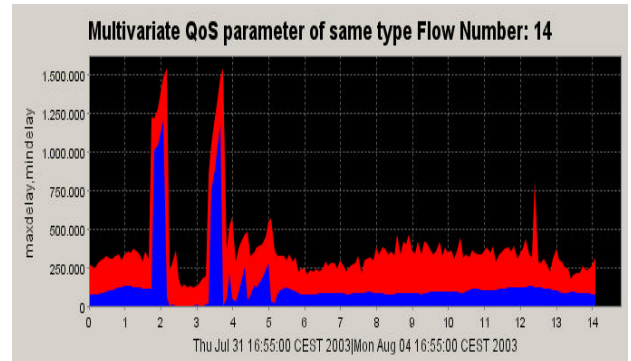


Figure 2: QoS outliers for maximum and mean delay

Looking in the topology data base obvious was the unsteady behaviour of an intermediate router of the end-to-end connection. In this case only the Traceroute topology discovery could be used, because InterRoute is based on discovery of inter-domain topologies including exchange points.

Based on the end-to-end QoS monitoring data, scenarios for complex SLA/QOS monitoring and analysis are possible using further INTERMON tools:

- QoS Visualisation and Data Mining Application on top of CM Toolset
- Spatio-Temporal Pattern Analyser
- Modelling and Forecasting using ARIMA.

4. References

[PMHN 03] T. Pfeiffenberger, I. Miloucheva, U. Hofmann, A. Nassri, Inferencing of inter-domain path characteristics, IPS, <http://www.ist-intermon.org/workshop>, Salzburg, 2003.