23rd NMRG Meeting Summary

Jürgen Schönwälder

Jacobs University Bremen
Bremen, Germany

70th IETF Meeting 2007

Meeting Logistics

- 23. NMRG Meeting 08-09 November 2007
- Hosted by the University of Twente, Netherlands
- Seven participants from five different organizations
- Meeting information and slides:
  `http://www.ibr.cs.tu-bs.de/projects/nmrg/meetings/2007/enschede/`
- Minutes:
  `http://www.ibr.cs.tu-bs.de/projects/nmrg/minutes/minutes-023.txt`
- Sponsored by EMANICS WP7 "Scalable Management":
  `http://www.emanics.org/`

Main Topics

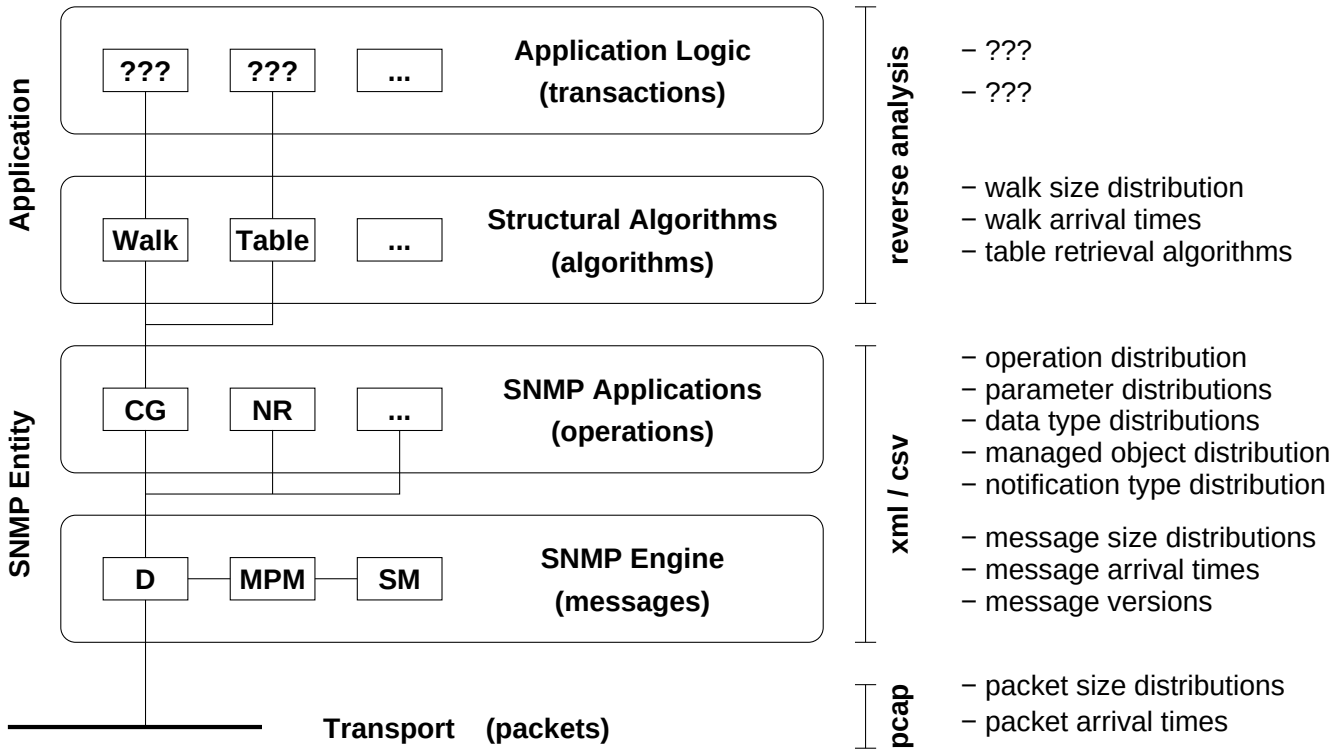
SNMP Trace Analysis

Goal: Find a common approach to split a potentially large SNMP packet trace into smaller meaningful portions that can be used to better understand and model the behaviour of management stations and notification originating agents.

SNMP Trace Visualization

Goal: Find good and meaningful visualizations for SNMP packet traces that enable people to interactively explore the behaviour of SNMP traffic.

SNMP Trace Analysis Challenge



Trace analysis requires to "reverse engineer" from the individual packets upwards to some of the application logic

Need for Common Definitions

Driving Forces

- University of Twente is trying to understand the periodic and aperiodic behaviour of SNMP traffic and, for example, scheduling strategies used by polling engines.
- Jacobs University is trying to understand the way deployed applications implement "structural algorithms", such as walks and table retrieval.

Common Definitions

It would be nice to have common definitions so that we can (i) share some of the tools, (ii) exchange aggregated data for further analysis, and (iii) know precisely what we mean when we use a specific term.

Towards Common Definitions

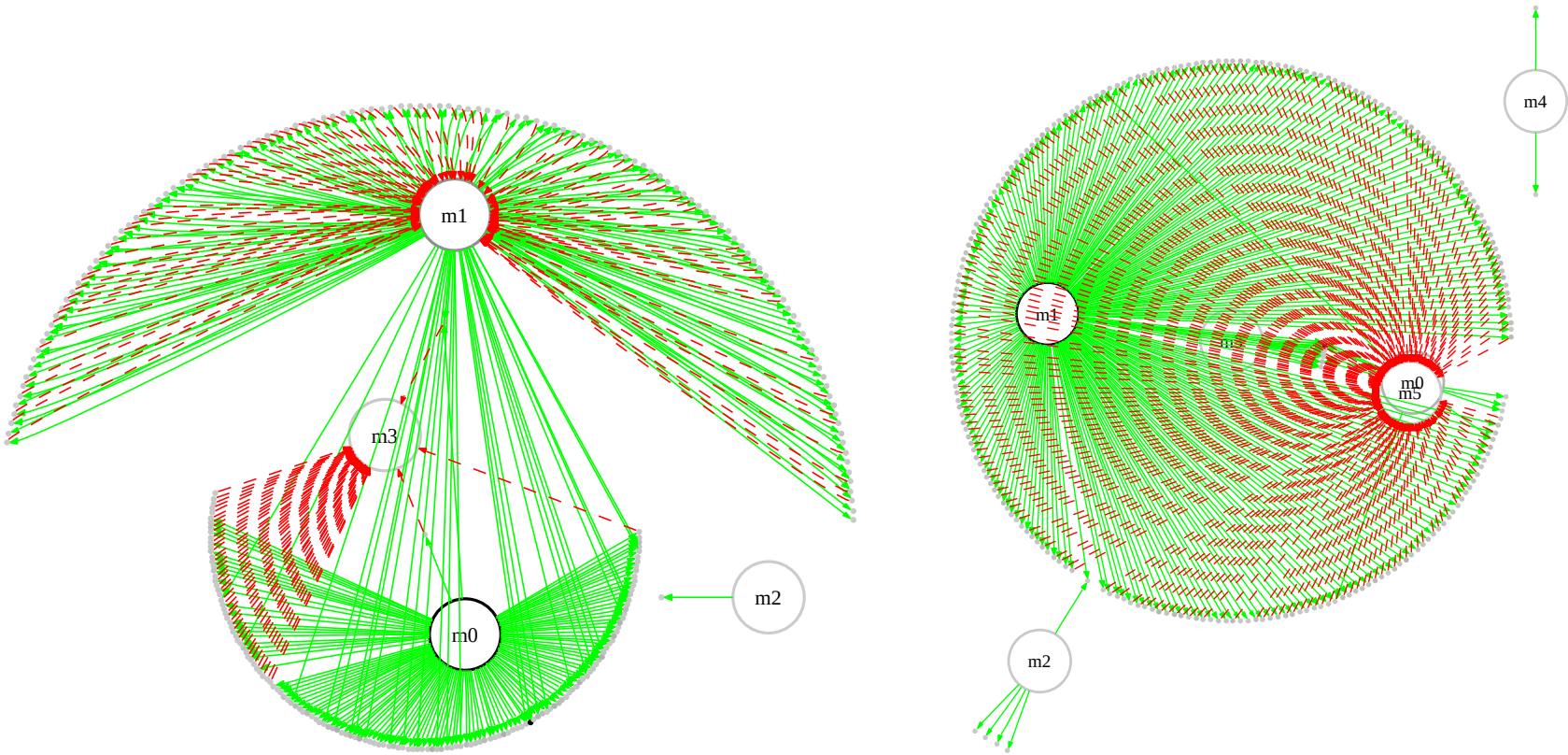
Approach

- Raw traces are split into flows
- Flows are further split into slices
- Slices can be typed based on their properties (slice types)
- Related slices can be aggregated into slice sets
- Some slices represent walks
- Walks can be typed based on their properties (walk types)
- ...

Status

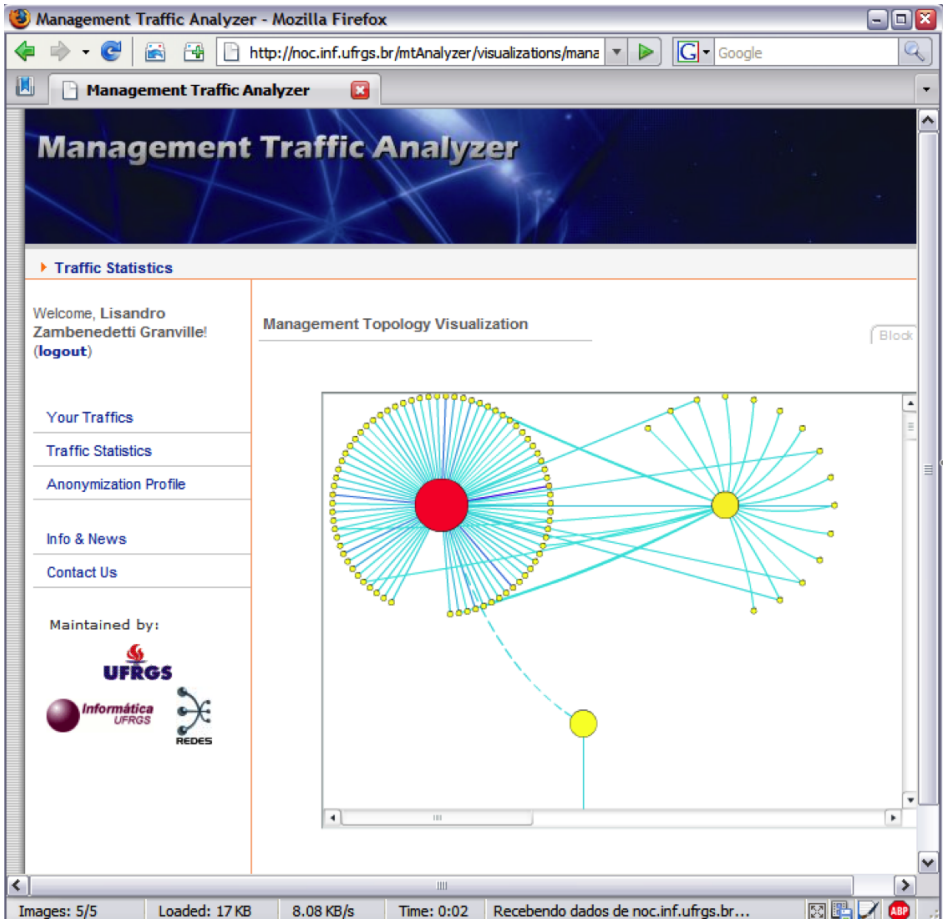
- Semi formal definitions are being worked out based on the work already done at Twente and Jacobs University
- Details will be posted as an Internet-Draft for discussion

SNMP Trace Visualization



Initial work on visualizing flows has been published at IM 2007

Online Flow Visualization



Federal University of Rio Grande do Sul (Brazil) is working on an interactive online SNMP flow visualization tool

More visualizations and tools needed for slices, slice sets, walks, ...

Conclusions

- Meeting was successful in moving work forward
- Internet-Draft with common definitions is being worked on
- Expect to see some research papers coming out in 2008
- Future work on suitable visualizations needed
- Additional traces are always welcome...