Intelligent real-time reactive network management

Intelligent Network Management Framework

Final project studies – Guillaume Andreys – April/August 2004

Introduction

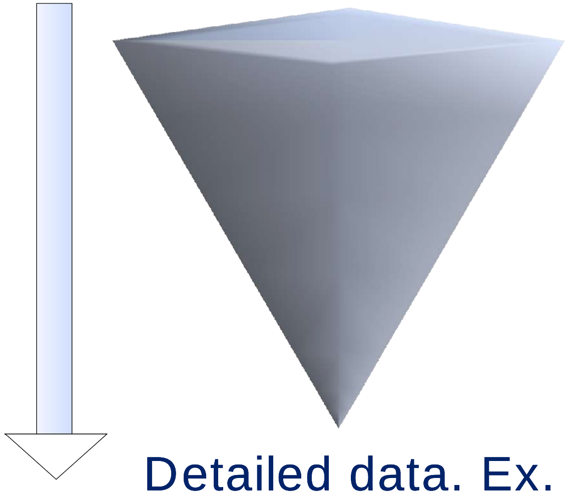
Motivation

- A lot of tools to collect network informations.
- But no choice :
  - Collecting only hight level data and manual intervention.
  - Running continuously hight resource consuming tools.
- Low automatic reaction possibility of such systems.

Principle

- From hight level data collection, we want to detect anomalies, and to (eventually) perform further data collection depending on rules and security policy.

Aggregated data. Ex.
Used Bandwidth



Detailed data. Ex.
User's informations

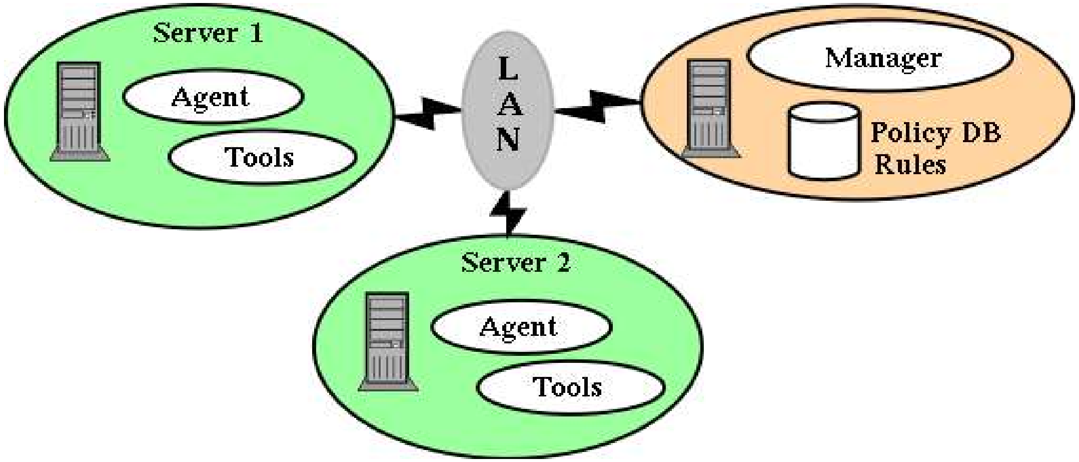
Features

- Hight level anomaly detection : Holt-Winters Forecasting algorithm.
- Managing various tools one various hosts on the network.
- Collecting data in a central point.
- Possibility for the user to write rules and define a security policy.
- Reacting from the collected data, rules and policy.

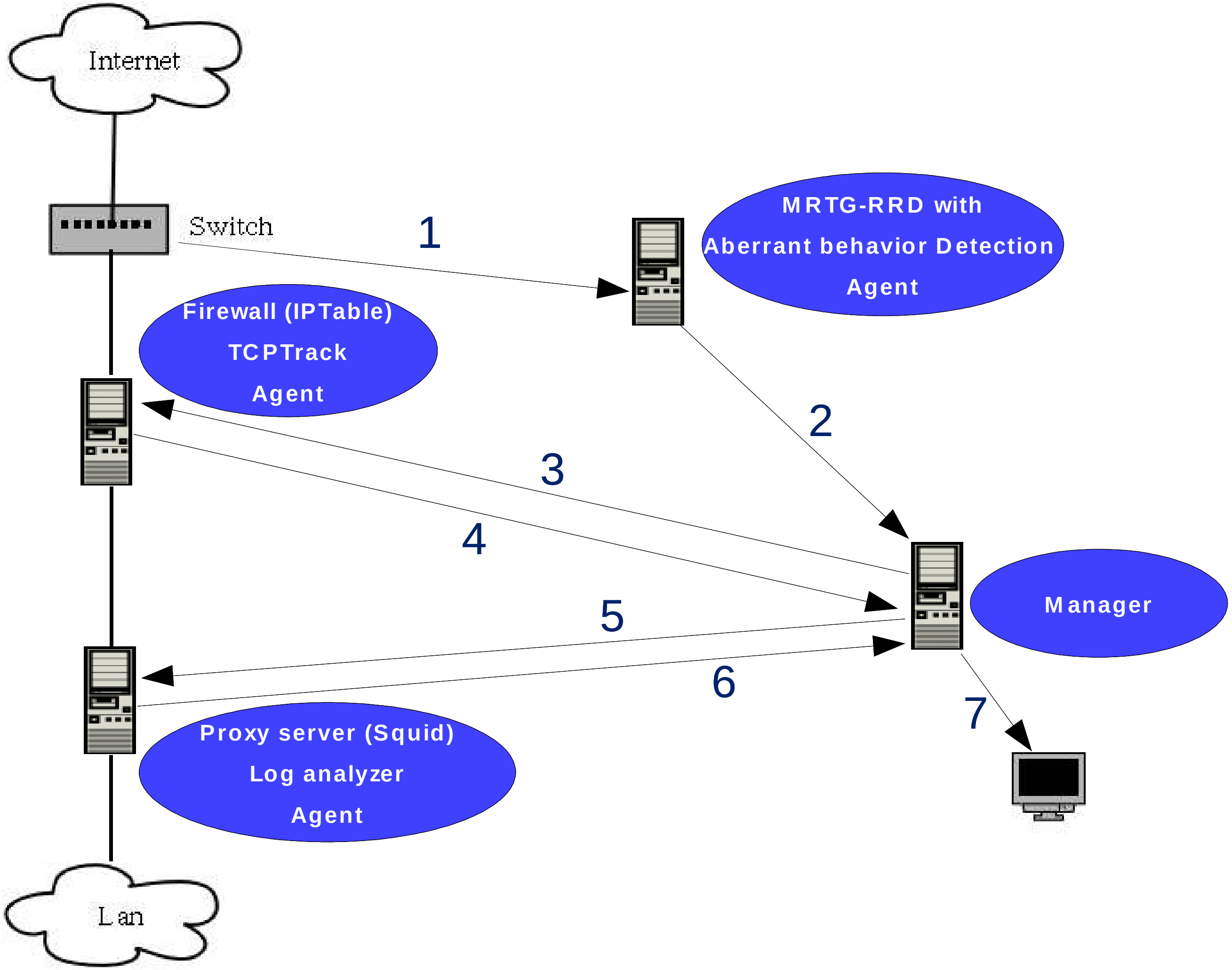
Architecture

Distributed architecture

- Agents installed on many hosts communicate with a central server via the network.

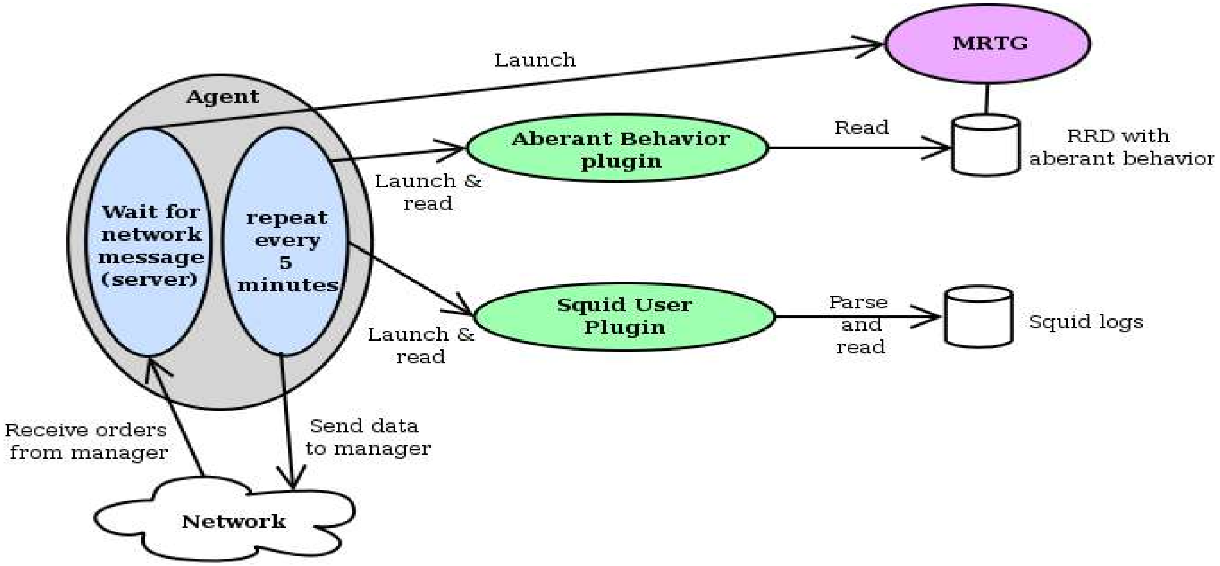


Example of scenario



The Agents

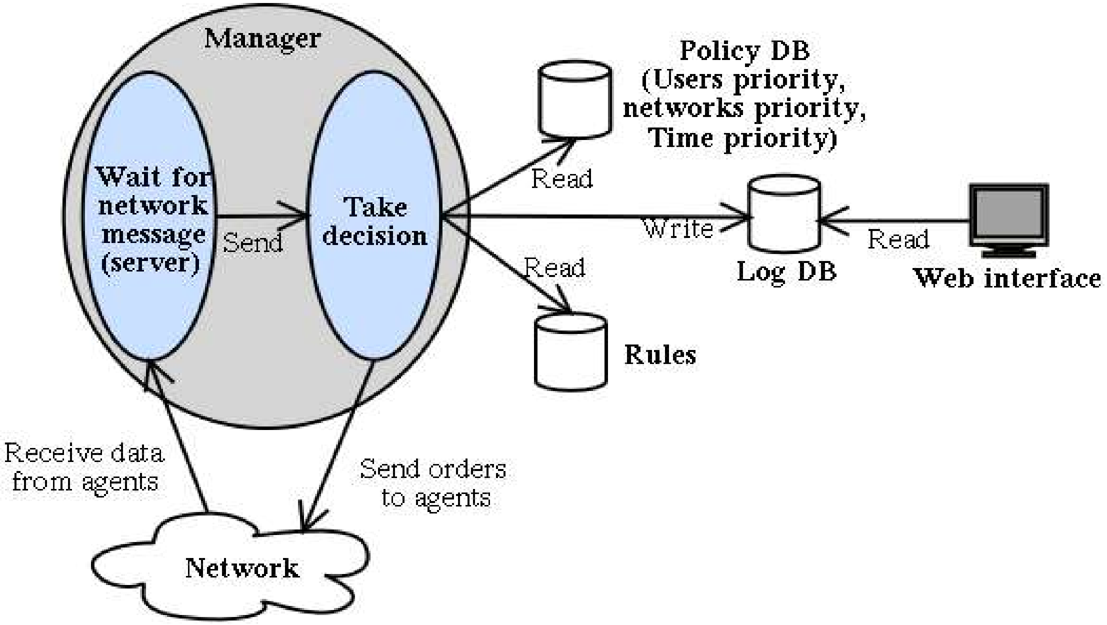
- Managing tools (Launching/Stopping) from Manager orders.
- Collecting data and sending it to the manager.



The Manager

Architecture

- Centralize all the collected data.
- Accede to the rules and security policy.
- Send appropriate decision to the appropriate Agent.
- User interface.



Decision process

Rules

- The user is defining rules to make a decision tree.
- We provide functions to get data information, set decision, alerting ...
- Actually, rules hard-coded with C++ language.
- In future, specific language using XML.
- Advantage of XML :
  - Syntaxes verification.
  - Comprehensible both by human and machine.
  - We can provide “ Hight-Level” verification.

Security policy

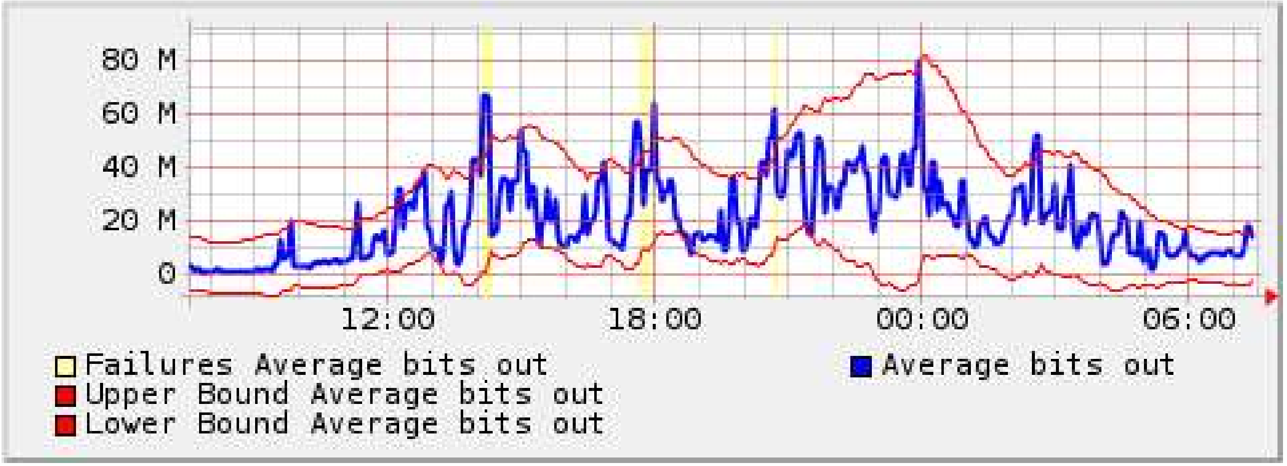
- Depending on some security policy we don't want to perform the same action.
- We allow to put priority on :
    - Users or user group (not implemented yet)
    - IP or networks
    - Time of the day
- Functions can be used in the rules to get the priority of some objects.

Tools

Anomaly Detection with Holt-Winters Forecasting Algorithm

Tools

- Algorithm who try to predict future values from older values.
- Implemented for Rond Robin Database, so compatible with all softwares who use those DB (ntop, MRTG, Cricket ...).
- Low false positive alarms.



Other tools

- MRTG for collecting aggregated data (compatible with RRD).
- TCPTrack to lock at actuals connections (port, bandwidth, IP).
- Different log analyzer for Squid (Proxy server) and Qmail (Mail server).
- Multilog to optimize the log analyze

Conclusion

Conclusion

- We just have a prototype version.
- A paper have been produced and submitted.
- Improvement are possible, especially on the decision process, the rules and making the configuration easier.
- It can interest the Open Source community and we may find people to give contribution on it.
- The project is actually on inmf.sourceforge.net