Monitoring for anomalous behaviour in massive traffic time series

David Rios Insua[1], Roi Naveiro Flores[1], Simon Rodríguez Santana[1]

[1]*ICMAT-CSIC, Madrid, Spain*

Abstract

We describe a system to monitor large amounts of Internet traffic time series so as to forecast anomalous behaviour for safety and security systems. The system essentially obtains performance readings from numerous IP connected devices in a nonintrusive manner and displays graphically the readings per device. A forecasting module is incorporated to issue:

- Short-term forecasts to detect whether critical values will be likely reached in the near future or detect anomalous behaviour.
- Long-term forecasts to detect when critical values would be likely reached.

The system covers discrete and continuous performance measures. In the continuous case, the generic model considered is a trend + seasonal DLM combined with an outburst process. In the discrete case, the generic model considered is a non-homogeneous Markov chain.

We describe various modeling issues and outline implementation details to cope with large amounts of time series.