ADAPTIVE TRAFFIC MODELLING FOR NETWORK ANOMALY DETECTION

by Dr Vassilios C. Moussas
May 2016

The GRNET Network

GRNET is the network of the Greek Educational, Academic and Research community:
213 Institutions, 9000 km opt. fiber, 500,000 Users (grnet.gr)

GRNET is the network of the Greek Educational, Academic and Research community:
213 Institutions, 9000 km opt. fiber, 500,000 Users (grnet.gr)
Network Monitoring (GRNET)

GRNET Backbone Links
- [https://mon.grnet.gr/rg/search/Backbone%20links](https://mon.grnet.gr/rg/search/Backbone%20links)
- GRNET Graphs __ Search Page.html

![GRNET Backbone Link Charts]

Network Monitoring (TEI–A)

TEI of Athens Backbone Link (Monthly & Weekly)

![TEI of Athens Backbone Link Charts]
Network Monitoring (SSE)

Hellenic Army Academy (ΣΣΕ/SSE) to GRNET Backbone Link (weekly traffic May 2–8 2016)

Network Monitoring (Sampling)

Yearly, Monthly, Weekly, Daily & Hourly Averages per: day, 2h, 30m, 10m, 5m
Network Traffic Modelling

- More **Abstract** Models use
  - Line Bandwidth
  - Resource Utilization
  - Long History Records available through MIB or Server Logs

- More **Detailed** Models use
  - Special traffic data provided by: agents, switches, routers, firewalls, hosts, or network sniffers
  - User behaviour, other types of data such as: transaction duration, size, inter-arrival, user habits, skills or position

Network Traffic data
Traffic Model Categories

- **Packet Pattern** modelling category (PP)
  - The most detailed models that describe the network traffic at packet level in full detail.

- **Task Pattern** modelling category (TP)
  - The less detailed models that distinguish the various categories of network traffic e.g., by application, protocol & user behaviour

- **Overall Utilization** modelling category (OU)
  - The most abstract models that observe only the overall utilization of network lines or components.

Traffic Model Requirements

- **Packet Pattern** (require detailed records from packet capturing applications and precise knowledge of the packet exchange procedures of the network – time & resource demanding)

- **Task Pattern** (server application logs, manager-agent monitoring tools, component MIBs, user behaviour statistics)

- **Overall Utilization** (require only the default data stored in component MIBs. These data are available on any network – faster/widely applicable)
Network Monitoring for Fault or Anomaly Detection

- **Packet Pattern** (not suitable for 24/7 all purpose anomaly detection. They should be used at a **second stage** for finer more detailed identification of an attack or a fault cause)
- **Task Pattern** (more suitable, may vary from more detailed (closer to PP) to less detailed (closer to OU))
- **Overall Utilization** (can be applied easily on any network, abstract but also much faster and less demanding, past utilization records always available to train them)
  - *Overall Utilization modelling is selected to be used due to: data availability & compatibility*

Adaptive Network Traffic Modelling

Modeling Bandwidth **Utilization** via:
- ARMA, S-ARIMA
- State–Space
- Other (lookup tables, NNs, etc.)

Model Identification via:
- MMPA Multi–model Partitioning algorithms
ARMA, S–ARIMA Models

\[
\varphi(B)\nabla^4\nabla^1 X_k = \theta(B)\Theta(B^{48})u_k
\]

\[
(1-\varphi_1 B)(1-B)(1-B^{48})X_k = (1-\theta_1 B)(1-\Theta_1 B^{48})u_k \quad \Rightarrow
\]

\[
X_k - (1+\varphi_1)X_{k-1} + \varphi_1 X_{k-2} - X_{k-48} + (1+\varphi_1)X_{k-49} - \varphi_1 X_{k-50} = u_k - \theta_1 u_{k-1} - \Theta_1 u_{k-48} + \theta_1 \Theta_1 u_{k-49}
\]

The autoregressive (AR) and moving average (MA) parameters of the model are: \(\varphi_1 = 0.413027, \theta_1 = 0.942437, \Theta_1 = 0.959323\)

ARMA, S–ARIMA Models

ARMA models predictions for workday & weekend
State-Space Models

- ARMA models transferred to state-space

\[ z_k + a_1 z_{k-1} + \ldots + a_n z_{k-n} = b_0 u_k + \ldots + b_m u_{k-m} \]

\[ x_{k+1} = \begin{bmatrix} -a_1 & I & \ldots & 0 \\ -a_2 & & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ -a_{n-1} & 0 & \ldots & 0 \\ -a_n & 0 & \ldots & 0 \end{bmatrix} x_k + \begin{bmatrix} b_1 \quad -a_1 b_0 \\ b_2 \quad -a_2 b_0 \\ \vdots \\ b_{n-1} \quad -a_{n-1} b_0 \\ b_n \quad -a_n b_0 \end{bmatrix} u_k, \quad z_k = [I \quad 0 \quad \ldots \quad 0] x_k + b_0 u_k \]

- Other state-space models (e.g. known cases)

\[ z_k = x_k + v_k, \quad \text{and,} \quad a) \ x_{k+1} = 10 \cdot x_k, \quad b) \ x_{k+1} = x_k \ (= 0) \]

Set (bank) of Models

A Collection of models describing typical utilization patterns creates the “model Bank”, e.g.:
Multi-Model Partitioning Algorithm

- MMPA contains a “filter Bank” corresponding to the available “model Bank” and adaptively selects the correct filter-model (highest weight factor)

Test Dataset

Utilization Data of a typical week (Sun – Sat) enriched with failure & abuse (peak) events
The MMPA algorithm detects all utilization conditions correctly and identifies the current one by giving a high value of ~1 to its weighting factor.

When an unknown case is present all weight factors have low or medium values indicating either an intermediate situation or an unknown anomaly.

Every new confirmed case is added to the Bank, and ARMA coefficients are periodically updated to meet current trends.

Progressively the MMPA learns all typical and/or known states of the network and offers more & more reliable alarms.

It can be expanded by introducing TP’s User Behavior modeling, to e.g., detect consistently “bad” users of a network.
Selected References


MRTG-RRDtool

TEI of Athens Case

MMPA Algorithm