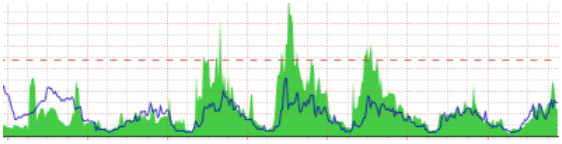
ADAPTIVE TRAFFIC MODELLING FOR NETWORK ANOMALY DETECTION



by Dr Vassilios C. Moussas

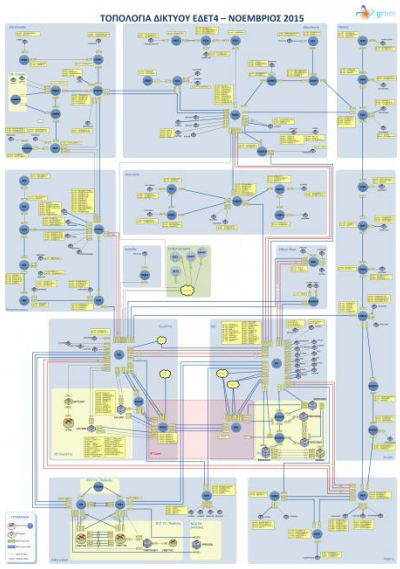
May 2016

3rd International Conference on Cryptography, Cyber-Security and Information Warfare (3rd CryCybIW), Hellenic Military Academy 26th – 27th 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)

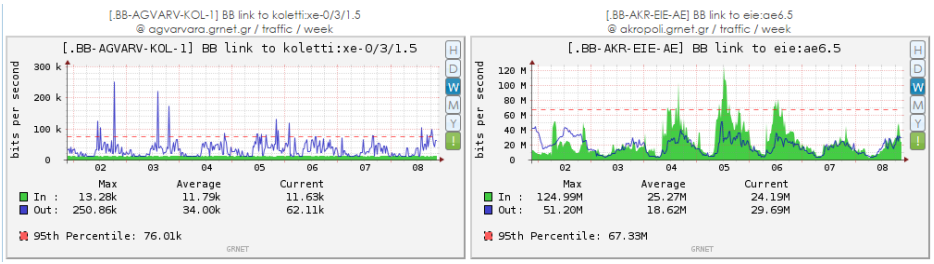


3rd International Conference on Cryptography, Cyber-Security and Information Warfare (3rd CryCybIW), Hellenic Military Academy 26th – 27th May 2016.

Network Monitoring (GRNET)

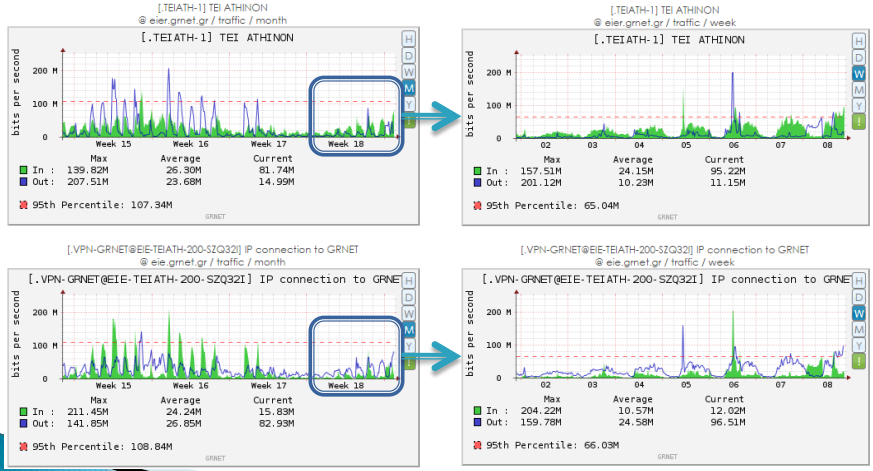
GRNET Backbone Links

- https://mon.grnet.gr/rg/search/Backbone%20links
- GRNET Graphs__ Search Page.html



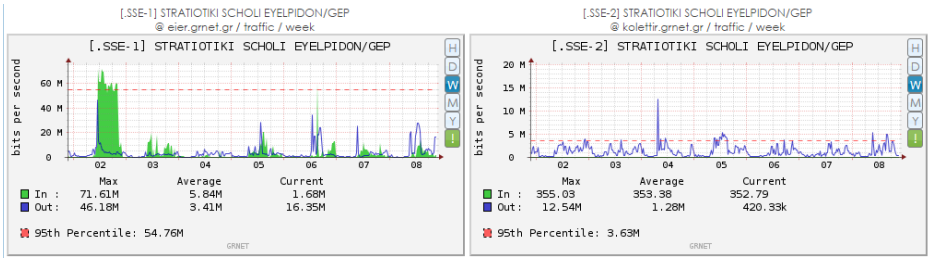
Network Monitoring (TEI-A)

TEI of Athens Backbone Link (Monthly & Weekly)



Network Monitoring (SSE)

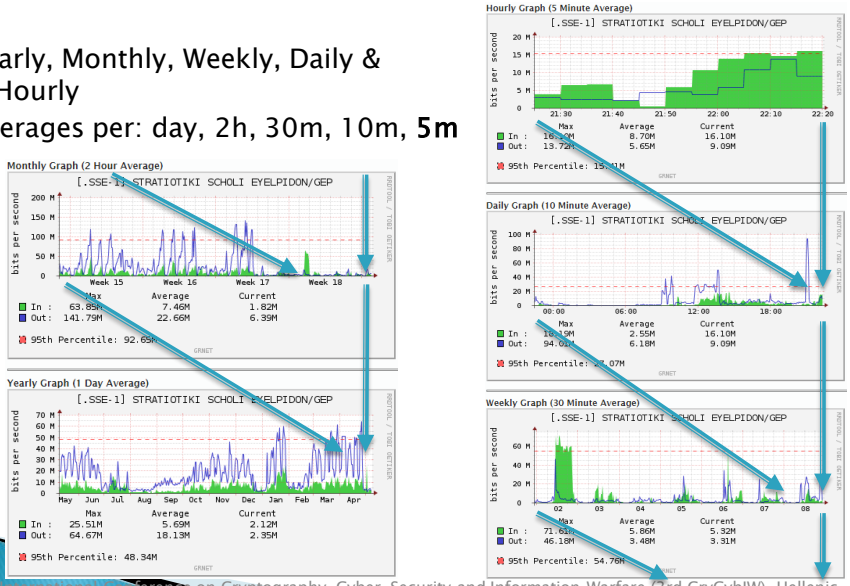
Hellenic Army Academy (ΣΣΕ/SSE) to GRNET Backbone Link (weekly traffic May 2-8 2016)



Network Monitoring (Sampling)

Yearly, Monthly, Weekly, Daily & Hourly

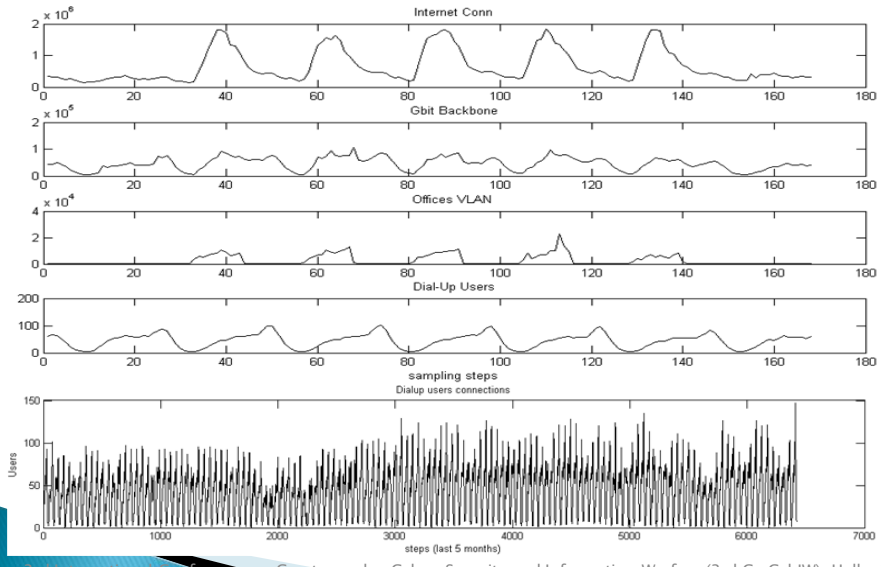
Averages per: day, 2h, 30m, 10m, **5m**



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



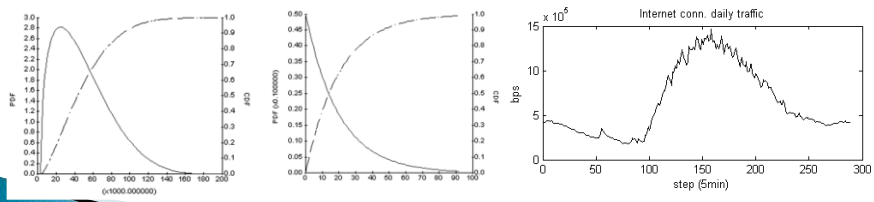
3rd International Conference on Cryptography, Cyber-Security and Information Warfare (3rd CryCybIW), Hellenic Military Academy 26th - 27th May 2016.

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

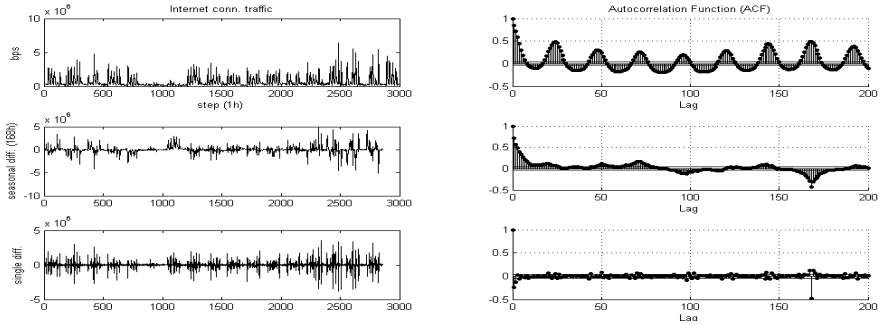
Modeling Bandwidth **Utilization** via:

- ARMA, S-ARIMA
- State-Space
- Other (lookup tables, NNs, etc.)

Model Identification via:

- MMPA Multi-model Partitioning algorithms

ARMA, S-ARIMA Models



$$\varphi(B)\nabla^1\nabla^1_{48}X_k = \theta(B)\Theta(B^{48})u_k$$

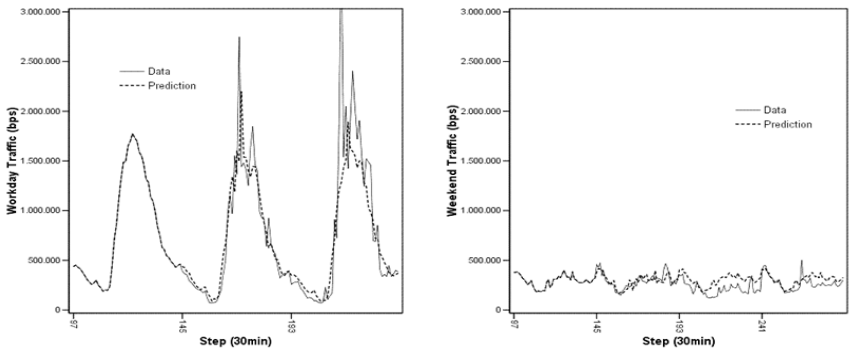
$$(1-\varphi_1 B)(1-B)(1-B^{48})X_k = (1-\theta_1 B)(1-\Theta_1 B^{48})u_k \quad \Rightarrow$$

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

The autoregressive (AR) and moving average (MA) parameters of the model are: $\phi_1 = 0.413027$, $\theta_1 = 0.942437$, $\Theta_1 = 0.959323$

ARMA, S-ARIMA Models

ARMA models predictions for workday & weekend



State-Space Models

- ARMA models transferred to state-space

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

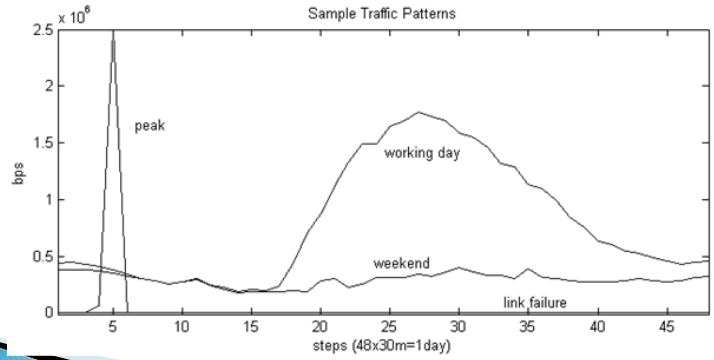
$$x_{k+1} = \begin{bmatrix} -a_1 & I & \cdots & 0 & 0 \\ -a_2 & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \cdots & I & 0 \\ -a_{n-1} & 0 & \cdots & 0 & I \\ -a_n & 0 & \cdots & 0 & 0 \end{bmatrix} x_k + \begin{bmatrix} b_1 - a_1 b_0 \\ b_2 - a_2 b_0 \\ \vdots \\ \vdots \\ \vdots \end{bmatrix}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

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

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

Set (bank) of Models

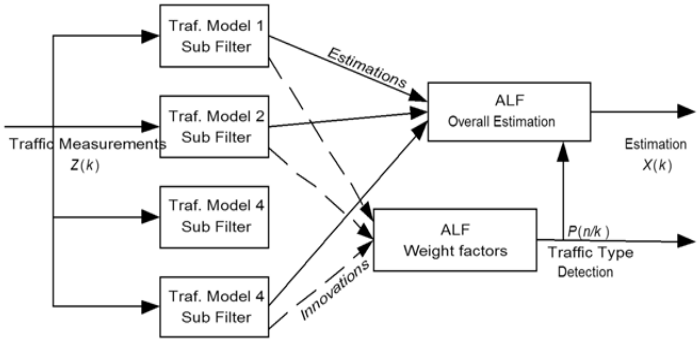
A Collection of models describing typical utilization patterns creates the "model Bank", e.g.:



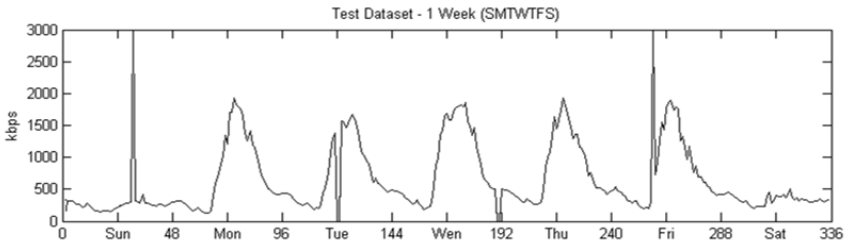
3rd International Conference on Cryptography, Cyber-Security and Information Warfare (3rd CryCybIW), Hellenic Military Academy 26th – 27th May 2016.

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)

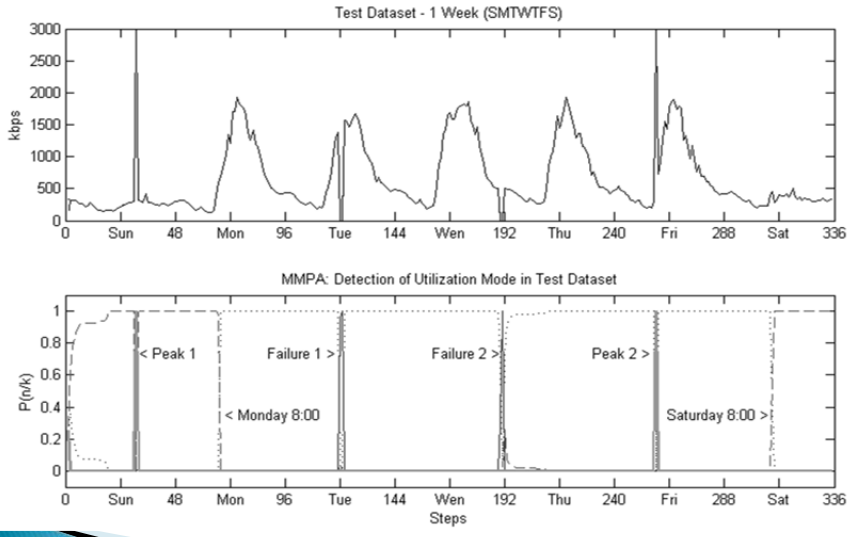


Test Dataset



Utilization Data of a typical week (Sun - Sat) enriched with failure & abuse (peak) events

Test Results



Conclusions

- 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

3rd International Conference on Cryptography, Cyber-Security and Information Warfare (3rd CryCybIW), Hellenic Military Academy 26th - 27th May 2016.

Selected References

[26] P.KuanHoong, I.K.T.Tan, C.YikKeong, "BitTorrent Network Traffic Forecasting With ARIMA" (IJCNC, 2012) Vol.4, No.4

[27] J. Kaur, S.Agrawal and B.S.Sohi, "Internet Traffic Classification for Educational Institutions Using Machine Learning", I.J. Intelligent Systems and Applications, 2012, 8, 37-45.

[8] Shu Y., Yu M., Liu J. and Yang O.W.W. (2003), "Wireless Traffic Modeling and Prediction Using Seasonal ARIMA Models", IEEE Intl. Conference on Communication May 2003, ICC'03 vol. 3.

[9] Marina Thottan and Chuanyi Ji, (2003), "Anomaly Detection in IP Networks", IEEE Transactions on Signal Processing, Vol. 51, No. 8, August 2003, pp. 2191-2204.

MRTG-RRDtool

[24] Oetiker Tobias, (2005), Multi Router Traffic Grapher (MRTG) tool, Software Package & Manuals, http://oss.oetiker.ch/mrtg/ Last visit: Mar 2016.

[25] Oetiker Tobias, (2016), Round Robin Database Tool (RRDtool), Software Package & Manuals, http://oss.oetiker.ch/rrdtool/ Last visit: Mar 2016.

TEI of Athens Case

[5] Moussas V.C., "Network Traffic Flow Prediction using Multi-Model Partitioning Algorithms", in Proceedings of the 2nd SCCE International Conference "From Scientific Computing to Computational Engineering", D. T. Tsahalis (editor), Athens, 5-8 July, 2006

[10] Moussas V.C., Daglis M., Kolega E., "Network Traffic Modeling and Prediction using Multiplicative Seasonal ARIMA Models", Proceedings of the 1st International Conference on Experiments/Process/System Modeling/Simulation/Optimization, Athens, 6-9 July, 2005.

[11] Moussas V.C., Pappas Sp. St., "Adaptive Network Anomaly Detection Using Bandwidth Utilization Data", Proceedings of the 1st International Conference on Experiments/Process/System Modeling/Simulation/Optimization, Athens, 6-9 July, 2005.

MMPA Algorithm

[20] Lainiotis D.G., "Partitioning: A Unifying Framework for Adaptive Systems, I: Estimation", Proc. IEEE, Vol. 64, pp. 1126-1142, 1976.