Security and Trustworthiness in Cloud Computing

Bruno L. Dalmazo, João P. Vilela, Marília Curado

{dalmazo, jpvilela, marilia}@dei.uc.pt

CISUC, Department of Informatics Engineering, University of Coimbra

UNIVERSIDADE DE COIMBRA

encontro CIÊNCIA '17

ENCONTRO COM A CIÊNCIA E TECNOLOGIA EM PORTUGAL

Centro de Congressos de Lisboa

3 a 5 Julho

ciencia2017PT

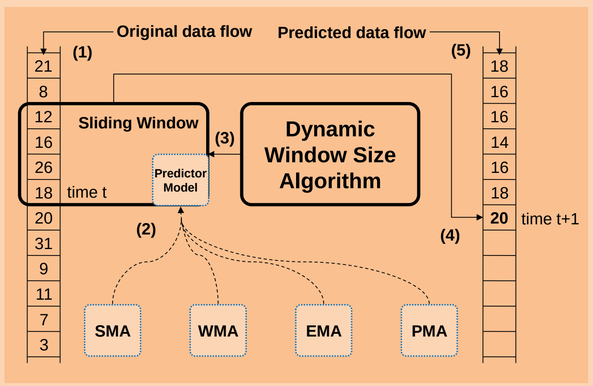
Poisson Moving Average is based on a statistical model where observations are weighted with a Poisson distribution inside a sliding window

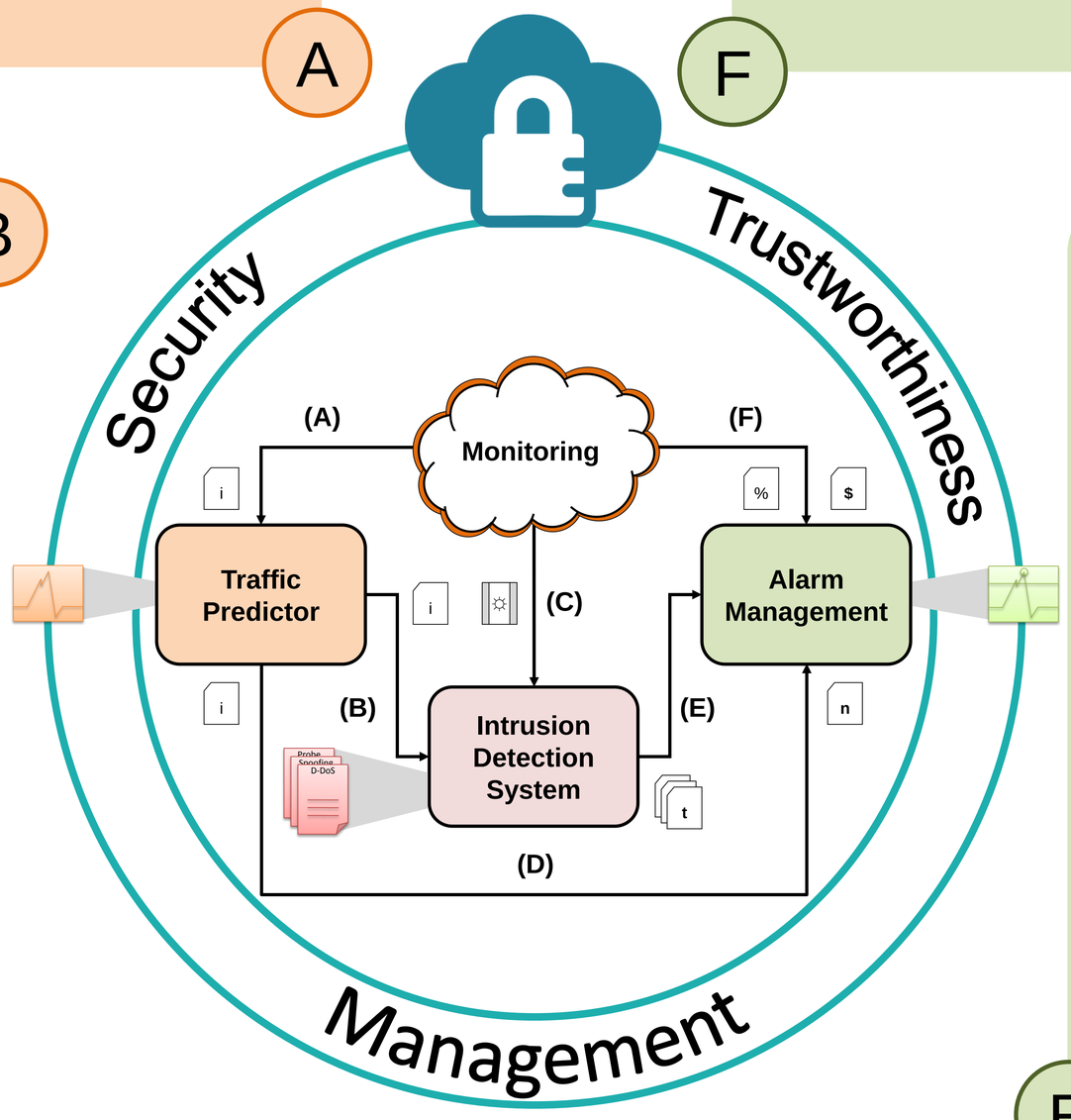
$$P[N(t) = k] = \frac{e^{-\lambda t}(\lambda t)^k}{k!}$$

A

B

DyWiSA is a **Dynamic Window Size Algorithm** focused on providing a standardized approach for evaluating the best candidate predictor models for cloud environments





F

Step 1

IDS output: O_0 O_1 O_2 O_3 O_4 ... O_n

Alarm database: A_0 A_1 A_2 A_3 A_4 ... A_n

Individual similarity approach for each feature

Step 2

F_0 F_1 F_2 F_3 F_4 ... F_n

Clustering relevant features

Step 3

Features O_n — Features A_n

Similarity approach for groups of alarms

$$Sim_{ED} = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2}$$

$$Sim_{TM} = \frac{\sum_{i=1}^{n} x_i y_i}{\sum_{i=1}^{n} {x_i}^2 + \sum_{i=1}^{n} {y_i}^2 - \sum_{i=1}^{n} x_i y_i}$$

E

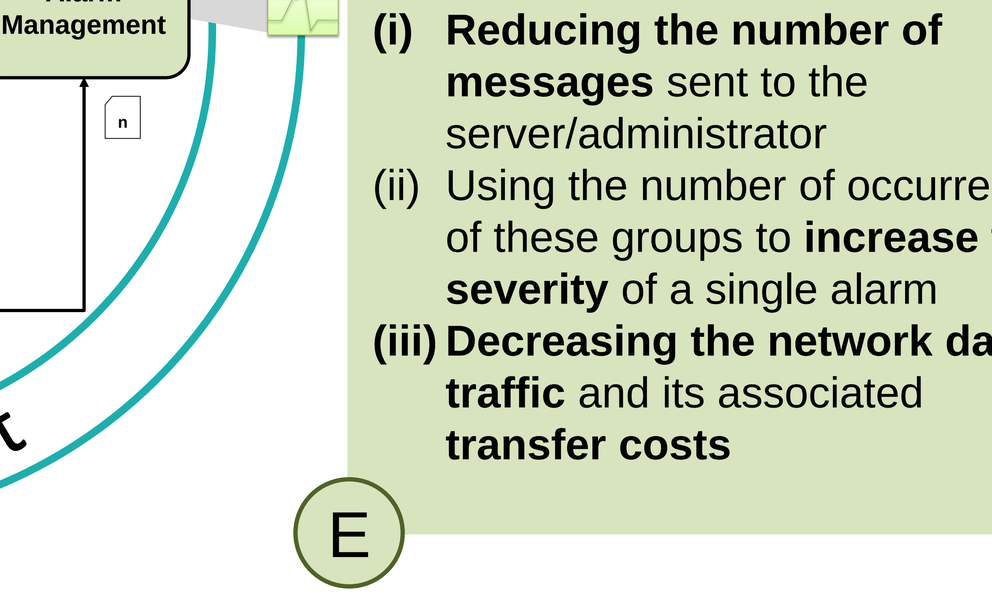
(i) **Reducing the number of messages** sent to the server/administrator

(ii) Using the number of occurrence of these groups to **increase the severity** of a single alarm

(iii) Decreasing the network data traffic and its associated **transfer costs**

C

D



Anomaly Detection Mechanism

References

[1] Dalmazo B. *et al*. **Performance Analysis of Network Traffic Predictors in the Cloud**. Journal of Network and Systems Management. Springer, 2017.

[2] Dalmazo B. *et al*. **Online traffic prediction in the cloud**. International Journal of Network Management. John Wiley & Sons, 2016.

[3] Dalmazo B. *et al*. **Expedite Feature Extraction for Enhanced Cloud Anomaly Detection**. IEEE/IFIP NOMS Workshop on Security for Emerging Distributed Network Technologies, 2016.