CRACS
CENTER FOR RESEARCH IN ADVANCED COMPUTING SYSTEMS
INESCPORTO LA

On applying Tunable Activation Threshold (TAT) hypothesis to Network Intrusions and Spam detection

Mário J. Antunes[1], Luis A. Santos[2], Manuel E. Correia[3]

[1] PhD Student in Computer Science at University of Porto (FC-DCC); CRACS Associate PhD Student (mantunes@dcc.fc.up.pt)
[2] MSc Student in Bioinformatics at University of Porto (FC-DCC); CRACS Associate MSc Student (labrisio@dcc.fc.up.pt);
[3] Assistant Professor at University of Porto ((FC-DCC)); CRACS Effective Member (mcc@dcc.fc.up.pt)

Introduction

A Network Intrusion Detection System (NIDS) is an application that analyses the traffic in a computer network in search for evidence of an ongoing attack or intrusion.

Over the last years, email has become an important means of communication, with consequent increase in the amount of spam delivered. Since emails are very personal, each individual's correspondence has its own traits thus creating a possible basis for differentiating normal emails from unwanted ones.

Scope

Most commercially available NIDS are knowledge-based systems that search for known attack signatures, and thus do not cope with attack innovation. Anomaly-based detection systems that search for outliers of normal network activity are a better alternative but currently produce a high level of false alarms.

The natural selection during the evolution of the vertebrate IS solve the problem of creating a system capable of monitoring a normally changing environment and the capacity to detect intrusions. This system is thus capable of distinguish “normal” body components from similar “abnormal” chemical structures present in micro-organisms. It also learns and memorises the first encounter with these intruders using this knowledge to better fight them in secondary encounters. Even more relevant for the designing of an anomaly detection system is the fact that IS learns the body composition during embryo life and adapts to physiological changes as the individual matures and ages. So, the IS has been an appealing inspiration to the deployment of Artificial Immune Systems for anomaly detection.

The state of the art in the development of NIDS based on the IS is divided into two main classes: classical Burnet's negative selection and Matzinger's Danger Theory.

In this research we decided to explore the appropriateness of applying Grossman and Paul's Tunable Activation Threshold hypothesis to build an architecture for an adaptive anomaly detector.

Aims

1. to investigate whether TAT possesses adequate adaptive characteristics to make it suitable to non-biological environments, like a computer network.
2. to use the results obtained to a better understanding of the scope of the TAT hypothesis itself.

The model

The mathematical model for TAT in T-Cells:

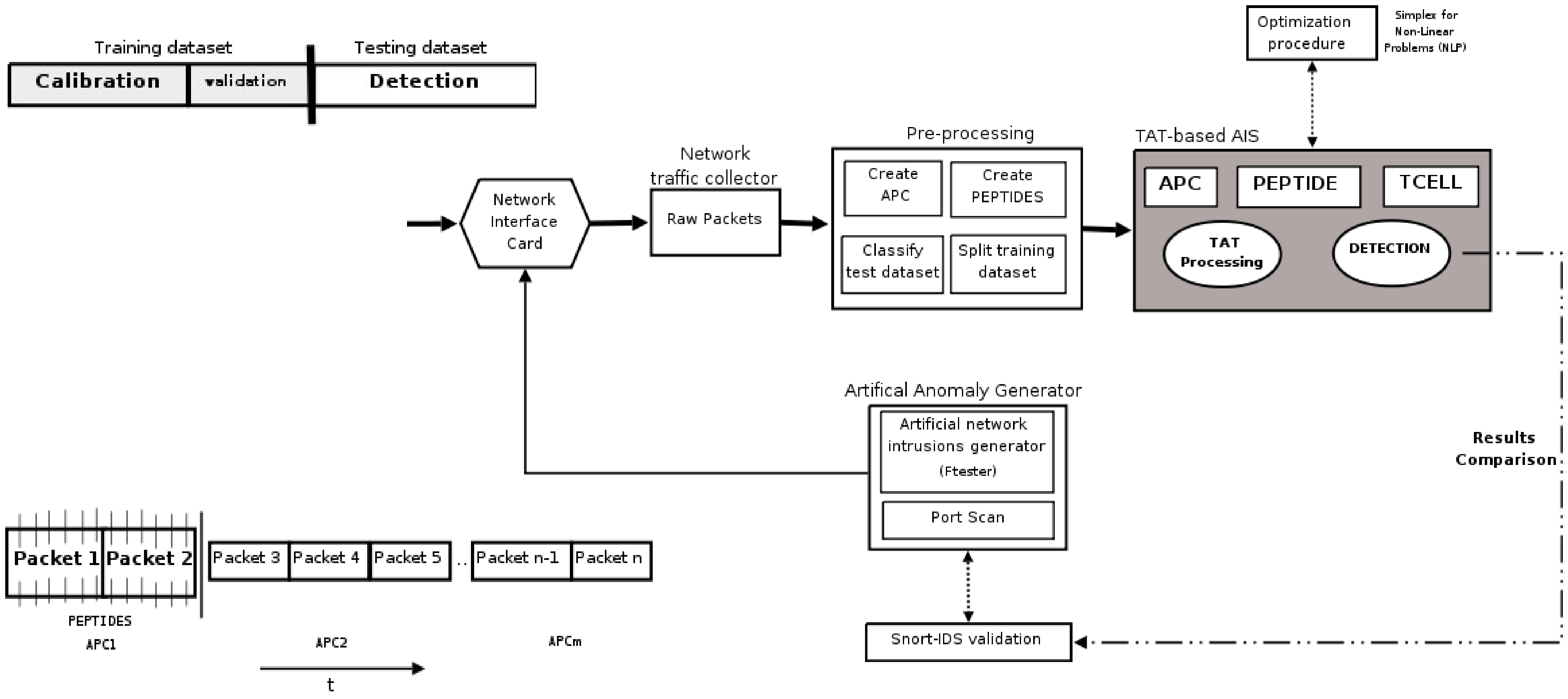
1. T-cell activation is controlled by two enzymes: Kinase (**K**) and Phosphatase (**P**)
2. Antigenic signal (**S**) leads to a linear increase of **K** and **P** until a plateau is reached
3. For the same **S**, **K** increases faster than **P**. If the signal persists, **P** reaches a higher plateau
4. In the absence of **S**, **K** returns to basal level faster that **P**

T-cell response: **K should be higher than P**

Under these conditions:

1. T-cells that receive **continuous** or sufficiently frequent signals become **unresponsive**
2. T-cells that **rarely** see their antigen, remain **sensitive**

A NIDS architecture

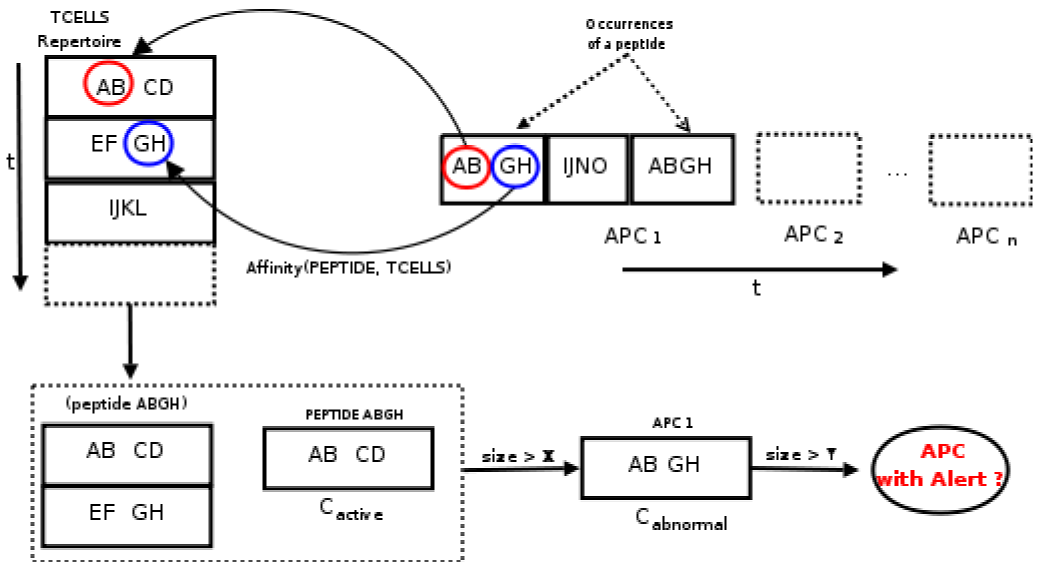


Preliminary results on intrusion detection

Run	K0	P0	S0	Kmax	Pmax	ϕK	ϕP	$Affinity$ %	C_{active} %	$C_{abnormal}$ %
1	80.0	90.6424	8	10.0	11.3303	18	12.545	24.29	53.42	42.35
2	80.0	107.904	8	10.0	13.488	18	9.877	41.56	53.61	28.48

Run	Phase	APCs	$PEPTIDEs$	$TCELLs$	Attacks		True Positives		False Positives	
					Qty	APCs	Qty	APC	Qty	%
1	Training Testing	916 107	4,244,899 251,472	63 93	1 4	2 8	1 4	1 7	5 6	0.5 5.6
2	Training Testing	726 225	6,387,471 419,560	77 63	1 2	2 22	1 2	1 6	8 16	1.1 7.1

The Algorithm



Conclusions

1. This first attempt reveals that TAT has interesting characteristics when applied to anomaly detection.
2. The detection process takes advantage of the “committees” decisions.
3. Preliminary tests have shown that detection success is intimately related with T-Cell generating repertoire quality.

Acknowledgements

1. To Doutor Jorge Carneiro and the Group of Theoretical Immunology from Instituto Gulbenkian da Ciência (IGC), for helping us better understanding the theoretical immunological issues involved.
2. To the undergraduate students from ESTG-Leiria, Miguel Saraiva, Filipe Mendes, Patrícia Silva, Pedro Gomes and Elson Dias for the contributions on the development of the TAT simulator.