Università degli Studi di Milano
Dipartimento di Tecnologie dell'Informazione

Artificial Immune Systems and Applications for Computer Security

Antonia Azzini and Stefania Marrara

Artificial Immune System (AIS)

Computational systems inspired by theoretical immunology.

Development and application domains follow the soft computing paradigms of Artificial Neural Networks (ANNs), Evolutionary Algorithms (EAs) and Fuzzy Systems (FS).

Applied in a wide variety of areas:

- Pattern recognition and classification (Carter - 2000, Timmis – 2002,…)
- Optimization (Fukuda – 1998, De Castro – 2000,…)
- Data analysis (Timmis – 2001, Von Zuben – 2000,…)
-Computer Security (Bentley – 1999, Forrest – 2000,…)
-…

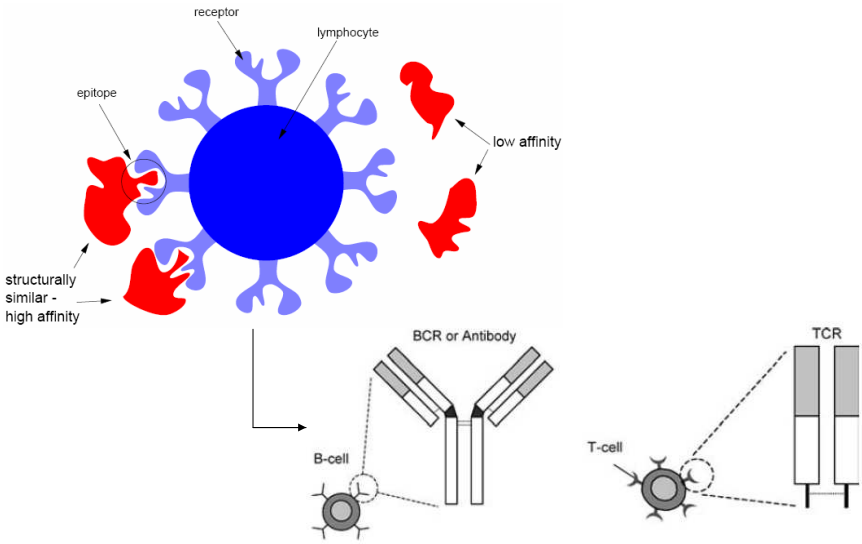
Immune System

- Purpose:
  - protect the body from the threats posed by pathogens
  - minimize harm to the body and ensures its continued functioning.
- Aspects that the IS faces:
  - identification or *detection* of pathogens (self/nonself),
  - efficient *elimination* of those pathogens
  - Efficient recognition of self antigens, molecules of the own body.

Innate vs Adaptative

- Innate Immune System
  - From birth
  - Not specialized
- Adaptative Immune system
  - Specific response to pathogenes
  - The adaptive immune system also provides memory capabilities to the immune system.

Cell Representation

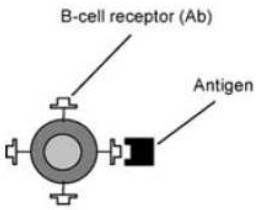


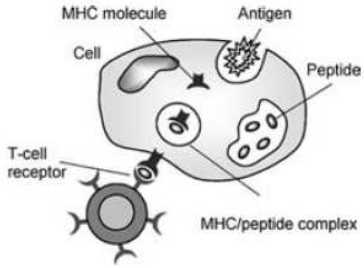
IS: Basic Concepts

- Cells and molecules interact to detect and eliminate infectious agents (pathogens).
- Surfaces of immune system cells are covered with receptors, some chemically bind to pathogens and some bind to other immune system cells or molecules to enable the complex system of signaling that mediates the immune response.
- IS cells circulate around the body (blood and lymphsystems) forming a dynamic system of distributed detection and response.
- No centralized control and little, if any, hierarchical organization.
- IS is robust to failure of individual components and attacks on the IS itself.
- Problem of detecting pathogens is for "self" and "nonself" (elements of the body, and pathogens).

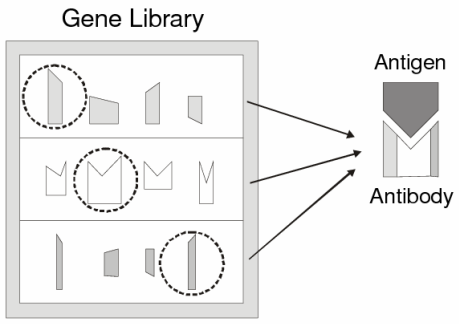
Pattern Recognition

• Recognition in the immune system is based on shape complementarity.
• Basically occurs at molecular level.
• “Shapes” of B and T cell surfaces have to be matched by the shapes of Antigens.
• Major Histocompatibility complex (MHC): antigens presented by molecules expressed in complex mode.





Gene Expression Process



Antibody Generation: the gene segments of different gene libraries are randomly selected and concatenated in a random order.

Immune Network Theory

- The hypotesis is that the immune system mantains an idiotypic network of interconnected B cells for antigen recognition.
- These cells both stimulate and suppress each other in certain ways that lead to the stabilization of the network.
- Two B cells are connected if the affinities they share exceed a certain threshold
- The strenght of the connection is directly proportional to the affinity they share.

Clonal Selection

The whole process of:

- Antigen recognition
- Cell proliferation (mitosis)
- Differentiation into memory cells

Affinity Maturation:

- Degree of binding of the cell receptor with the antigen.
- Inversely proportional with mutation: the higher the affinity a cell receptor has with an antigen, the lower the mutation rate and vice-versa.
- Directly proportional with proliferation: the higher the affinity the higher the number of offspring generated and vice-versa.

Negative Selection

- Works by learning the set of self strings in a training phase and classifying new data as normal or anomalous during a test phase.
- It consists of multiple negative detectors are analogous to limphocytes in the immune system.
- Detection is modeled as partial matching between s and the string representing d.
- Negative detectors match non-self strings, and not self strings.

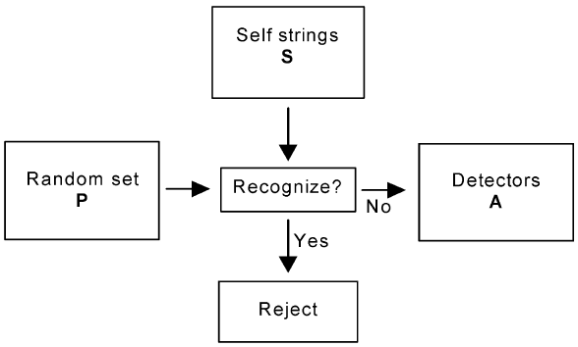
Negative Selection Algorithm (1)

- Distributed, by placing different detectors on different computers.
- Different randomly-generated detectors on different computers confer diversity, because different computers will be able to detect different intrusions.
- Robust: the loss of some detectors on a single computer will not result in a complete absence of protection.
- If the self set is representative of empirical normal behaviour, then policy is implicitly specified.
- Flexible: protection and computational requirements depend on the number of detectors, the number of detectors can be automatically increased.
- Localized detection no communication is required, the system is scalable (anomaly and signature-based detection).

Negative Selection Algorithm (2)

In training phase:

- candidate detectors are randomly generated and compared to all self strings.
- If a candidate detector matches any self strings it is deleted and replaced by a new random detector.
- The process is repeated.



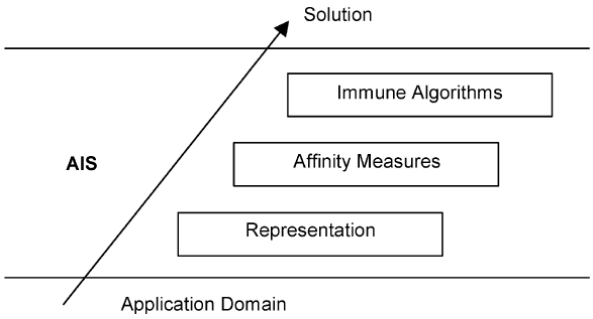
Positive Selection

- The T cell receptor (TCR) is similar to that of the B cell,except that it is not secreted as antibody and does not bind directly to antigens.
- Rather it binds to peptides (small fragments of protein broken down from the pathogen) presented in a complex with a specialised self molecule called the Major Histocompatibility Complex (MHC).
- MHC is a specialised complex involved in regulating the T cell response in the immune system

Positive Selection

- The widely held view of the reason behind this difference between the MHC of individuals is that this ensures the immune systems of all individuals do not react in the same way to pathogens.
- Positive selection is an area in immunology where there are contrasting views. This arises around the ability of positive and negative selection to work together to both *retain* cells that recognise the self-MHC:peptide complex, while also *removing* cells that recognise any self peptides

Artificial Immune Systems



Representation: to create abstract models of immune organs, cells and molecules

Affinity Measures: to quantify the interactions of these elements

Immune Algorithms: govern the dynamics of the AIS

Principles of AIS

- Robustness: consequence of the fact that IS is diverse, distributed, dynamic and error tolerant.
- Adaptability: can learn to recognize and respond to new infections and retain a memory of them.
- Autonomy: no outside control required.
- Anomaly detection: ability to detect novel pathogens to which it has not been previously exposed.
- Diversity, generality: unique IS for each individual in a population
- Distributed protection: millions of distributed components that interact locally to provide protection.

Detection System

- Detection Event: when the number of receptors bound exceeds some threshold, the lymphocyte is activated.
- A detection event occurs in the IS when chemical bonds are established between receptors on the surface of an immune cell, and epitopes, which are locations on the surface of a pathogen or protein fragment (a peptide).
- A lymphocyte will only be activated by pathogens if its receptors have sufficiently high affinities for particular epitope structures on the pathogens, and if the pathogens exist in sufficient numbers in the locality of the lymphocyte.

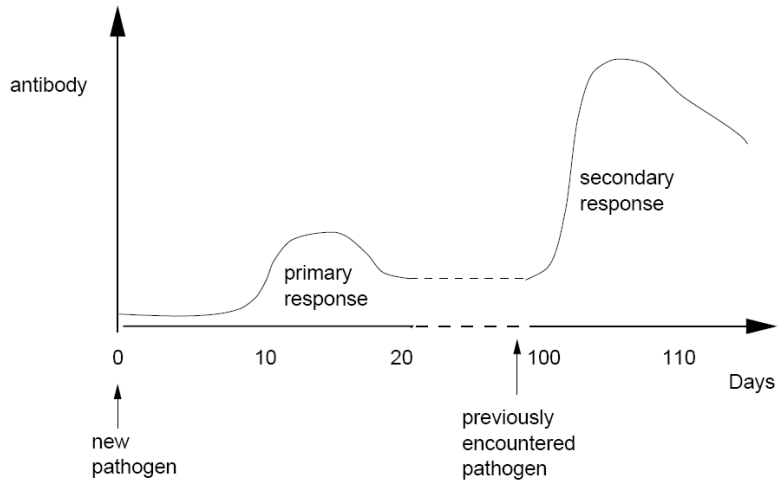
Immunology for Computer Scientist

- Recognition: chemical bonds established between specific receptors and epitopes.
- Receptor Diversity, to ensure that at least some lymphocytes can bind to any given pathogens, dynamic protection, with a continual turnover of lyimphocytes.
- Adaptation: B-cells, learn foreign proteins and remember them (memory of IS) for speeding up future responses. Affinity maturation enables B-cells to adapt to specific pathogens.
- Tolerance: responsability of another class of lymphocytes, Th-cells, measure of auto-immune response to a self-attack from the IS.

Learning and Memory: critical aspects

- Problem: limited lifetime of B-cells
- Some Solutions in the literature:
  - Adapted B-cells (memory cells) live up to the lifetime of the organisms [MacKay, 1993].
  - B-cells constantly restimulated [Gray, 1992].
- Consequences:
  - Primary response
  - Secondary response

Primary and Secondary Responses



Computer Security

Computer security system should protect computers from intrusions. Aspects to computer security:

- Confidentiality, authorized access to confidential data.
- Integrity, data protected from maliciuous or accidental corruption.
- Availability of data to the authorized users.
- Accountability, sufficient information for perpatrators identification.
- Correctness, minimization of fals alarms from incorrect classification.

Computer Security (2)

- Important issue: ability to determine difference between normal-harmful activity.
- Anomalies examples:
  - Network Intrusion: attacks on a system coming through the network with computer communications via standard protocols.
  - Traffic volume anomalies: generated from:
    - DoS attacks (intentionally created by attackers)
    - flash crowds (unintentionally caused by a larger numer of normal users)
- Consequences: dramatic increase in servers' load, packet loss and congestion, degrading network operation, impacting QoS of the user.
- Solution -> timely detect intrusions from the onset.

Network traffic anomalies: Anomaly Detection

- Relies on building models from network data.
- Discovers variations form the model in the observed data.
- Problem of:
  - density level detection.
  - Aggregation in time and in space (short and long scales).
  - Different levels of protocol stack:
    - IP packet level,
    - transport level,
    - application level.
- Traffic volume anomaly examples:
  - Network operation anomaly
  - Flash crowd anomaly
  - Network abuse anomaly

Network Intrusion Detection (1)

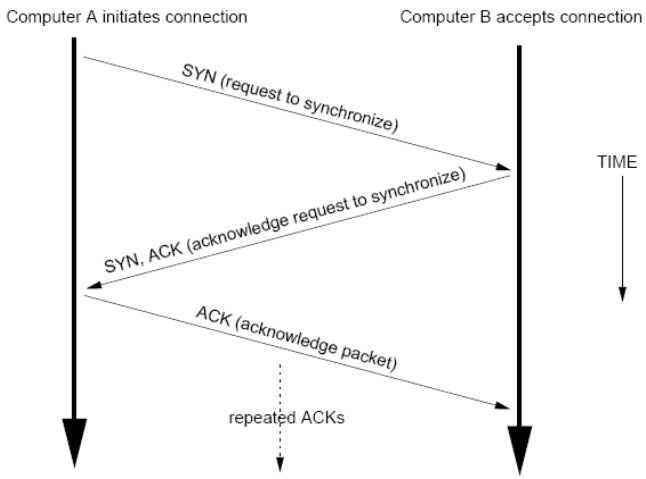
- In monitoring network traffic all attacks on a system must come through the network.
- Computers communicate via standard protocols
- Protocols monitor allows the ID system to be independent from the local operating system.

Attacks can be divided into:

- Host-targeted attacks: exploit holes in programs running as servers
- Network-targeted attacks: exploit weaknesses in network protocols.

Systems fail to achieve: adaptability - flexibility

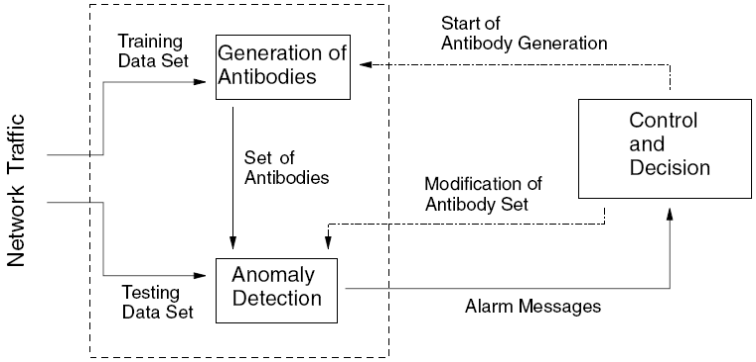
Network Intrusion Detection (2)



The Three-way TCP Handshake for a reliable communication.

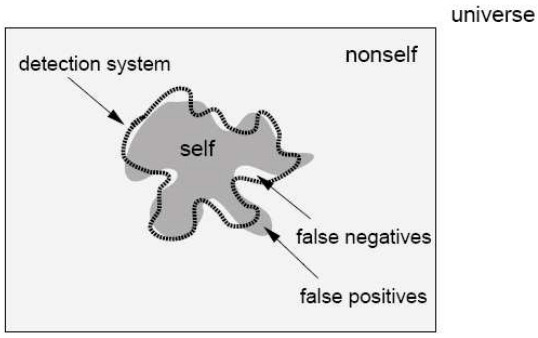
Anomaly Detection System

General Architecture of anomaly detection system.



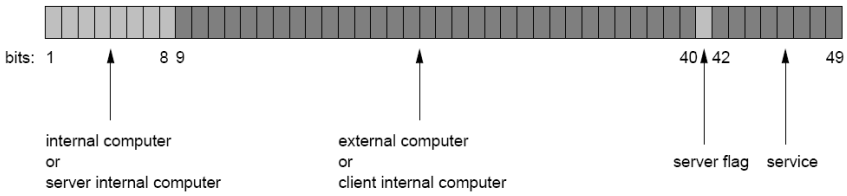
AIS approaches for network security presented in the literature

ARTIS for LISYS: Immuno-Inspired Distributed Detection System – Forrest et al.

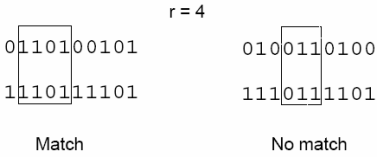


Architecture of AIS

Base representation of a TCP/IP SYN packet.

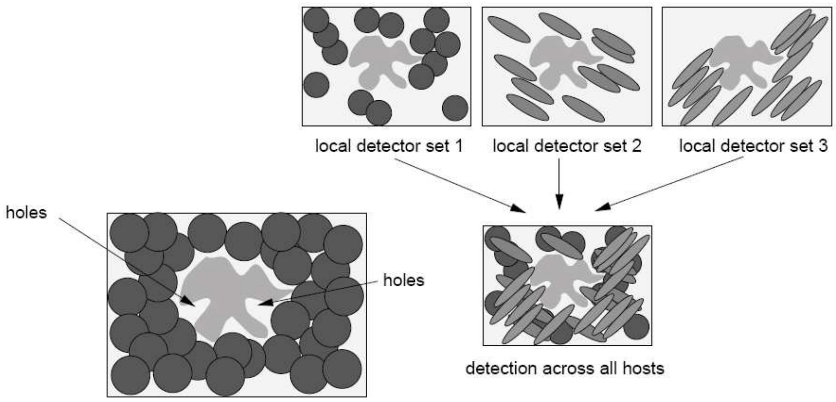


Matching Rule:
r-contiguous bits



Holes and Multiple Representations

Holes: derived from patterns in the nonself set that cannot be covered by valid negative detectors of a given specificity.



different representation for each local detection system.

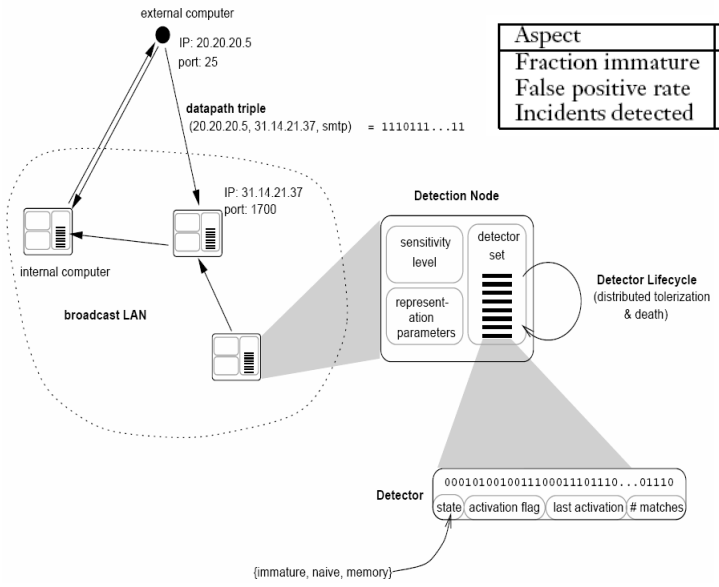
Extensions of Basic Model (1)

GOALS	MECHANISM
• Elimination of Autoreactive Detectors	• Costimulation
• Adaptation to changing self-sets	• Distributed Tolerization
• Signature-based detection	• Dynamic Detectors
	• Memory Detectors

Extensions of Basic Model (2)

- Costimulation in the eliminating autoreactive lymphocytes.
- Distributed tolerization Each detector is created with a randomly-generated bit string (analogous to a receptor) and remains immature for a time period T called the tolerization period.
- Dynamic Detectors Each detector has a probability pdeath of dying once it has matured. When it dies, it is replaced by a new randomly-generated, immature detector.
- Memory Detectors The IS "remembers" the structures of known pathogens to facilitate future responses.

Architecture of LISYS and results



Aspect	Result
Fraction immature	0.23±0.01
False positive rate	1.76±0.20
Incidents detected	7 out of 7

Immune Technique to Detect Anomalies in Network Traffic (Gonzalez, Dasgupta 2002)

- AIS technique extending two-class into a multiple class approach.
- Non-self space is further classified in multiple sub-classes to determine the abnormality level.
- Genetic algorithm for rules evolution to cover the abnormal space.
- Detectors are represented by hypercubes that satisfy rules.
- Satisfactory rule: not include positive samples and cover a large area.

R^1: If $Cond_1$ then **non_self**

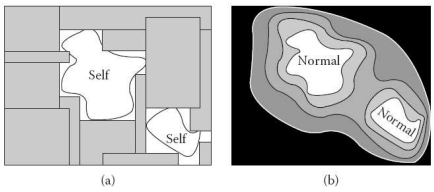
$\vdots$ $\vdots$ $\vdots$

R^m: If $Cond_m$ then **non_self**

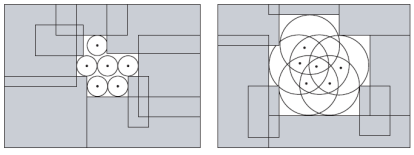
$Cond_i = x_1 \in [low_1^i, high_1^i]$ and ... and $x_n \in [low_n^i, high_n^i]$

- $(x_1, ..., x_n)$ is a feature vector
- $[low_i^j, high_i^j]$ specifies the lower and upper values for the feature x_i in the condition part of the rule R^j.

The Proposed Approach



(a) Self and non-self division of the Descriptor space.
(b) Approximation of the non-self space by interval rules.



Set of normal samples represented as points in a 2D space.
(a) Rectangular rules cover the non-self space using a small value of *v*.
(b) Rectangular rules cover the non-self space using a large value of *v*.
(c) Level of deviation defined by each *v*, where level 1 corresponds to Non-self cover in (a) and level 2 Corresponds to non-self cover in (b).

Anomaly detection in TCP/IP networks (Bouvry et al. 2007)

- Use only TCP SYN packets as representatives of TCP communication.
- Antibodies and antigens represented by binary arrays correspondig to headers of packets.
- Euclidean or Hamming distances measure similarities between antibodies and antigens.
- Antibodies generation with:
  - Positive characterization: legal traffic is used to create detectors
  - Random characterization: detectors are randomly created
  - Negative characterization: detectors are generated with antibodies not belonging to the legal traffic.

Results

- The cost of running the system highly depends on a method of generation of antibodies.
- Positive characterization is the faster, weakest for time of detection: it is much larger than Negative.
- Random characterization requires more computational costs, but best for detection time: it provides the smallest number of detectors.
- Negative characterization is the most expensive.
- The choice of method for detector generation is matter of compromise between requested speed and available memory.

Negative Selection and Niching by AIS for Network ID (Bentley et al. 1999)

Problems to solve:

• new antibodies randomly generated are inefficient to detect antigens

•. Excessive computational time caused by random-generation approach

Niching of the IS: evolution of antibodies towards the existing 'antigen' patterns to exclude ineffectual detectors.

Modified Negative Selection: algorithm with niching that replaces the random generation of pre-detectors with their evolution towards 'non-self'.

Modified Negative Selection Algorithm

FIRST PHASE: the modified negative selection algorithm builds self profiles, that are encoded in an appropriate data representation.

SECOND PHASE:

For each self profile and its corresponding detector set:

- D detector patterns are randomly generated with fitness =0
- N detector patterns are randomly selected from D detectors
- A single self pattern is randomly selected from the self profile
- Update fitness value of detectors
- Select fittest P_b% detectors as parents and apply genetic operators (crossover, mutation) to generate new detectors
- Delete the worst P_w% detectors

Create new detector population by including the selected parents and the offspring generated.

THIRD PHASE: detector patterns in each detector set are compared to the pattern in each corresponding new self profile. Alarm signal is generated if they are similar beyond a predefined threshold.

Data Profiling

- TCP packets are considered for anomaly detection
- For each TCP connection are extracted:
  - Connection identifier: initiator address, initiator port, receiver address, receiver port
  - Known port vulnerabilities
  - 3way Handshaking
  - Traffic intensity

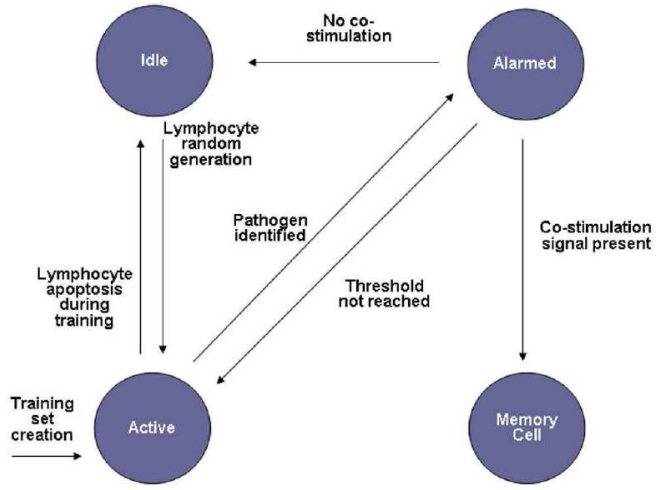
Detector Phenotype = (Number of Packet =[10,26], Duration =[0.3,0.85], Termination = “half closed”, … etc)

Self Phenotype = (Number of Packet = 35, Duration = 0.37, Termination = “normal”, …etc)

AIS for NIDS (Gabrielli et al. 2006)

- Affinity between a lymphocyte and a traffic substring is substituted by a binary match between the two strings with *true* if the two strings are equal or *false* otherwise.
- Random generation is implemented as a batch procedure executed to replace dead lymphocytes in order to have the same number of active lymphocytes as at the end of the training phase.
- For each lymphocyte four possible states of life are considered
  - Idle
  - Active
  - Alerted
  - Memory cell
- Co-stimulation: the flow back from the HTTP system is used to the client to represent the confirmation signal.

Lymphocyte state model



Conclusions and Future Work

- AIS constitute a successfull computational intelligence paradigm inspired by IS to solve problems in different domain areas.
- Evolutionary algorithm and artificial neural networks to improve pattern classification and network security.
- The choice of method for detector generation is matter of compromise between requested speed and available memory.
- Current research is directed to find more effective methods of generating detectors (Promising alternative for searching rule detectors is applying coevolutionary algorithms).
- real-time self-adaptiveness

In the Literature…

- J. Kim, P. J. Bentley, U. Aickelin, J. Greensmith, G. Tedesco, and J. Twycross (2007). Immune system approaches to intrusion detection - a review. Natural Computing.
- V. Cutello, G. Nicosia, M. Pavone, J. Timmis (2007) " An Immune Algorithm for Protein Structure Prediction on Lattice Models", IEEE Transactions on Evolutionary Computation.
- F. Esponda, H. Jia, S. Forrest, and P. Helman (2006) , "Protecting Data Privacy through Hard-to-Reverse Negative Databases," Proceedings of the Information Security Conference
- S. Garrett (2005) "How Do We Evaluate Artificial Immune Systems?" Evolutionary Computation.
- F. Gonzalez (2003). A study of artificial immune systems applied to anomaly detection. Technical report.
- H. Inoue and S. Forrest (2002) **"**Anomaly Intrusion Detection in Dynamic Execution Environments.", *New Security Paradigms Workshops.*
- L. DeCastro and J. Timmis (2001) "Artificial Immune Systems: A New Computational Intelligence Approach"
- …