Intrusion Detection using Artificial Intelligence

Juan J. Flores

Universidad Michoacana

Morelia, Mexico

juanf@umich.mx

Contents

- Introduction
- Classification
- ANNs – SOMs
- ANNs – Multilayer Perceptrons
- Fuzzy Inference
- Hidden Markov Models (*HMMs*)
- Evolutionary Computation
- Agent-Based
- Conclusions

Introduction

- security mechanisms of a system are designed so as to *detect/prevent* unauthorized access to system resources and data
  - Virus, denial of service, exploits, etc.
- Attempted or Ongoing attacks
- Data:
  - *Confidentiality*
  - *Integrity*
  - *Availability*

Introduction

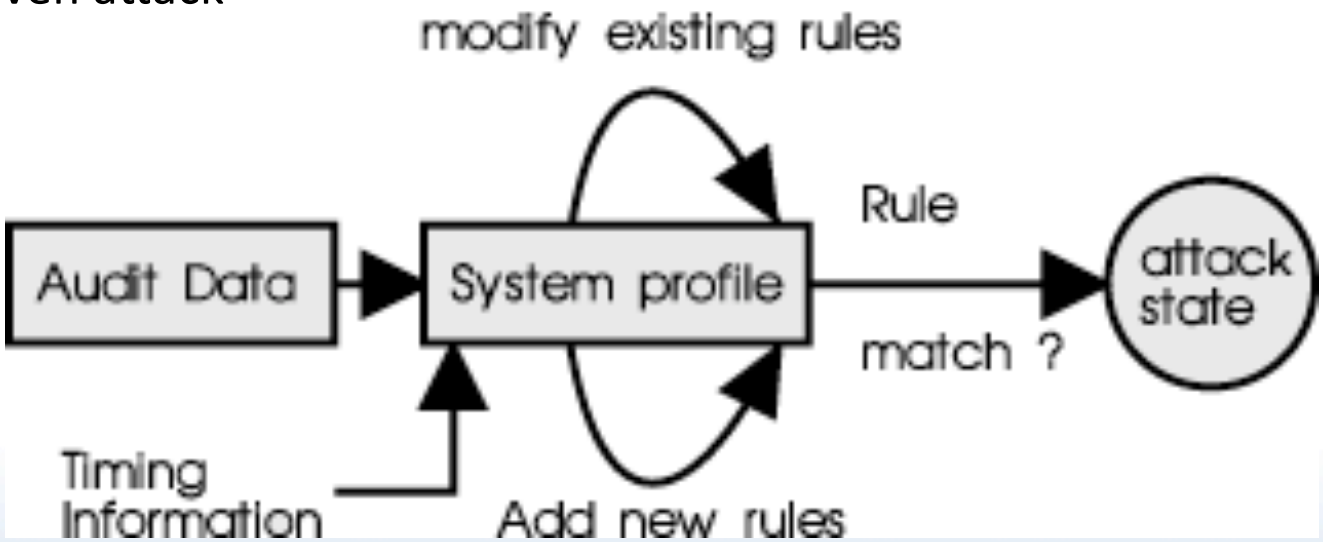
- increased connectivity
- more systems are subject to attack by intruders
- exploit flaws
  - operating system
  - application programs
- OS -> *audit data*
- *100 Mb/day*
- *Manual analysis unfeasible*

Introduction

- ID categories
  - Misuse vs. Anomaly
  - Network vs. Host
  - Passive vs. Reactive
- Protocol Anomaly
- Traffic Anomaly

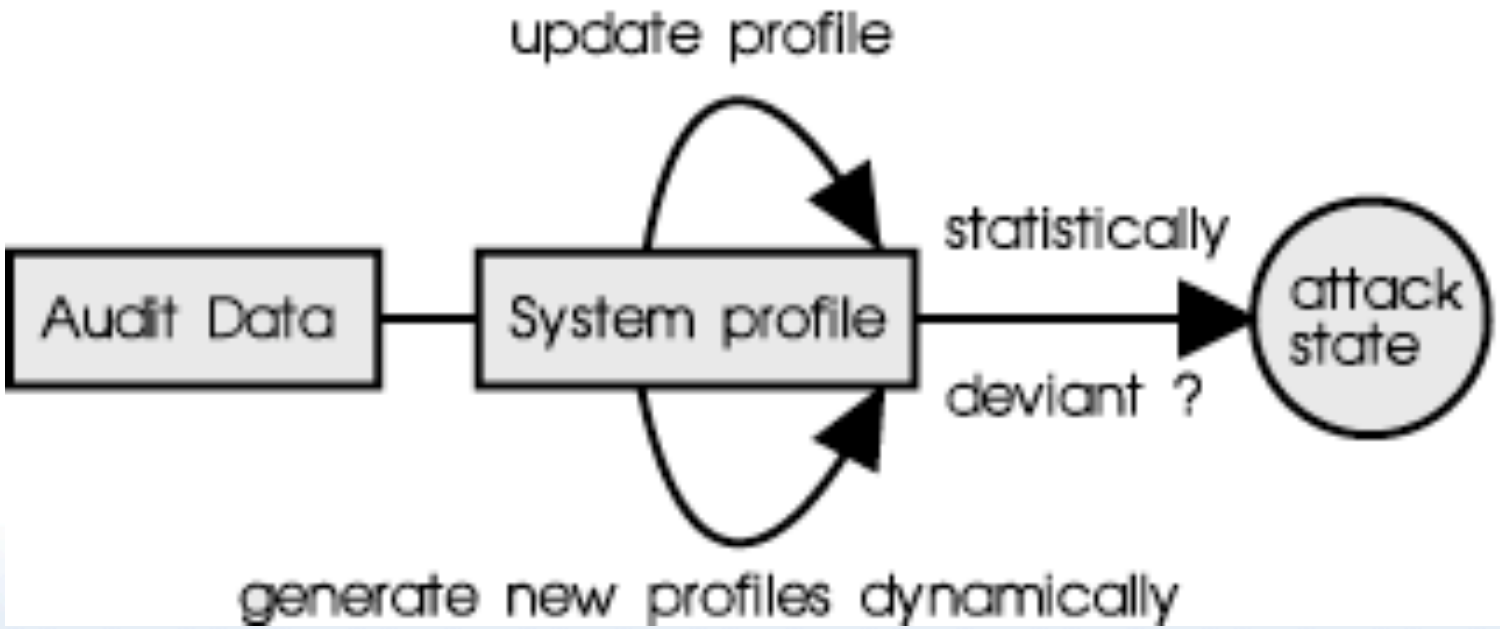
Introduction

- **Misuse Detection**
  - Attacks: pattern or signature
  - Models based on malicious users
  - Can detect many or all *known* attack patterns
  - Of little use for unknown attack methods
  - How to write a signature that encompasses *all* possible variations of a given attack



Introduction

- **Anomaly Detection**
  - Models based on normal (activity profile) users
  - All intrusive activities are necessarily anomalous
  - States deviating significantly from normal are considered as intrusion attempts

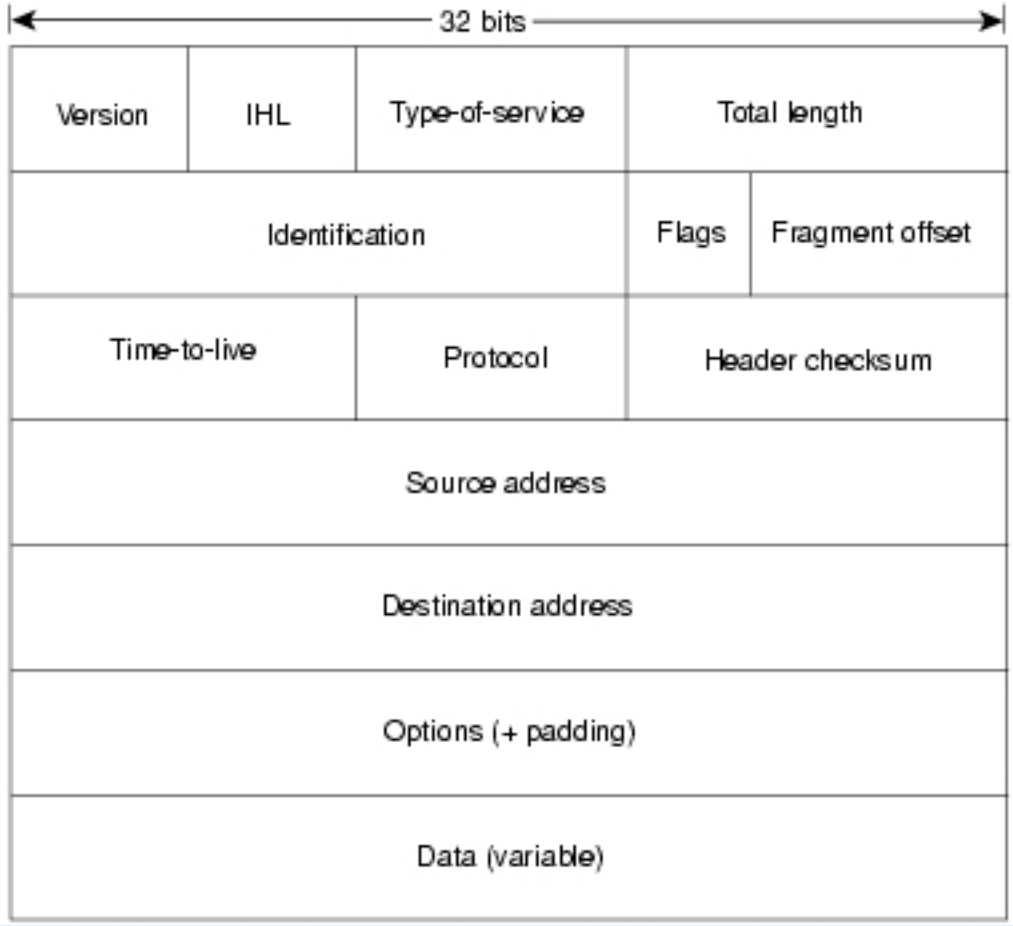


Introduction

- **Anomaly Detection Approaches**
  - Statistics
  - Artificial Intelligence
    - **ANNs – SOMs**
    - **ANNs – Multilayer Perceptrons**
    - **Fuzzy Inference**
    - **Hidden Markov Models (*HMMs*)**
    - **Evolutionary Computation**
    - **Agent-Based**
  - Hybrid

Introduction

- **What to measure?**
  - Networking IP packets
  - Ethereal
  - tcpdump
  - PCAP (libpcap)



Introduction

- What to measure?

Network Connection Features	Traffic Features
Duration of connections	Count (# conn. to host past 2 secs)
Protocol (TCP, UDP, etc.)	Serror (% conn. w/SYN errors)
Service (hhtp, ssh, sftp, telnet, ftp, etc.)	Rerror (% conn. w/REJ errors)
Flags	Same_srv (% conn. to same service)
Source bytes	Diff_srv (% conn. to different service)
Destination bytes	Srv_count (#conn. same serv.past 2 secs)
	Srv_serror
	Srv_rerror
	Srv_diff_host

- Convert features to numbers (count, %, avg, etc.)

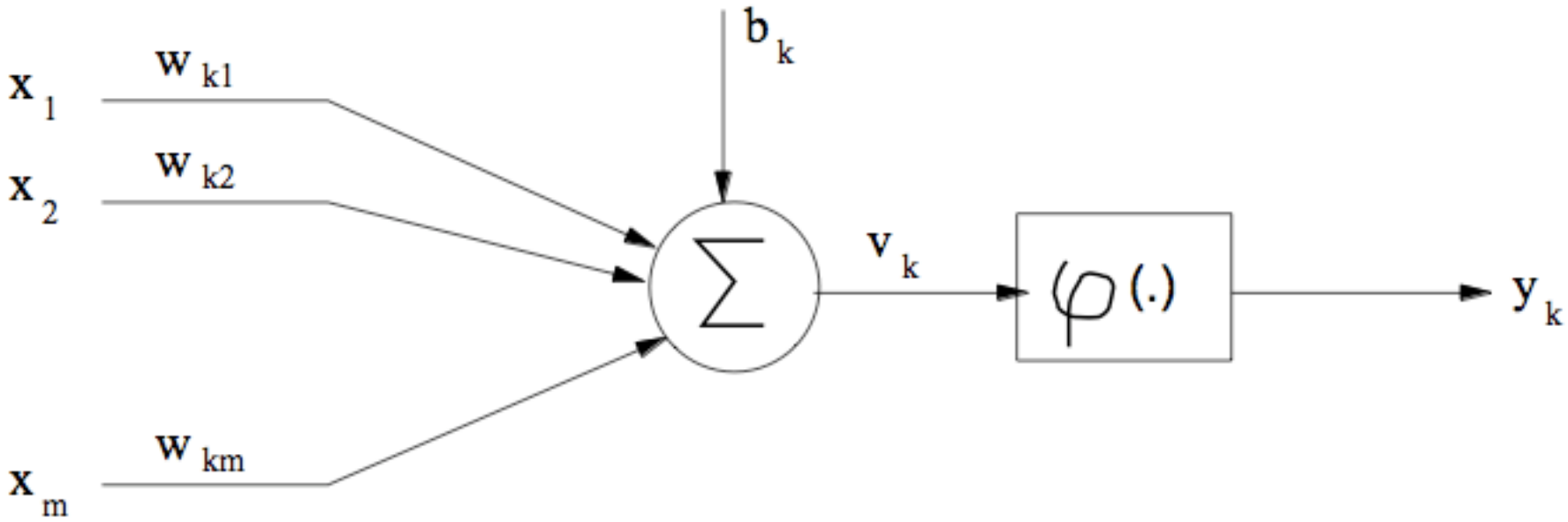
Classification

- Given a set of features the IDS determines if the observed behavior is normal, or what kind of a set of attacks is occurring.

- The ID problem is then a classification problem.

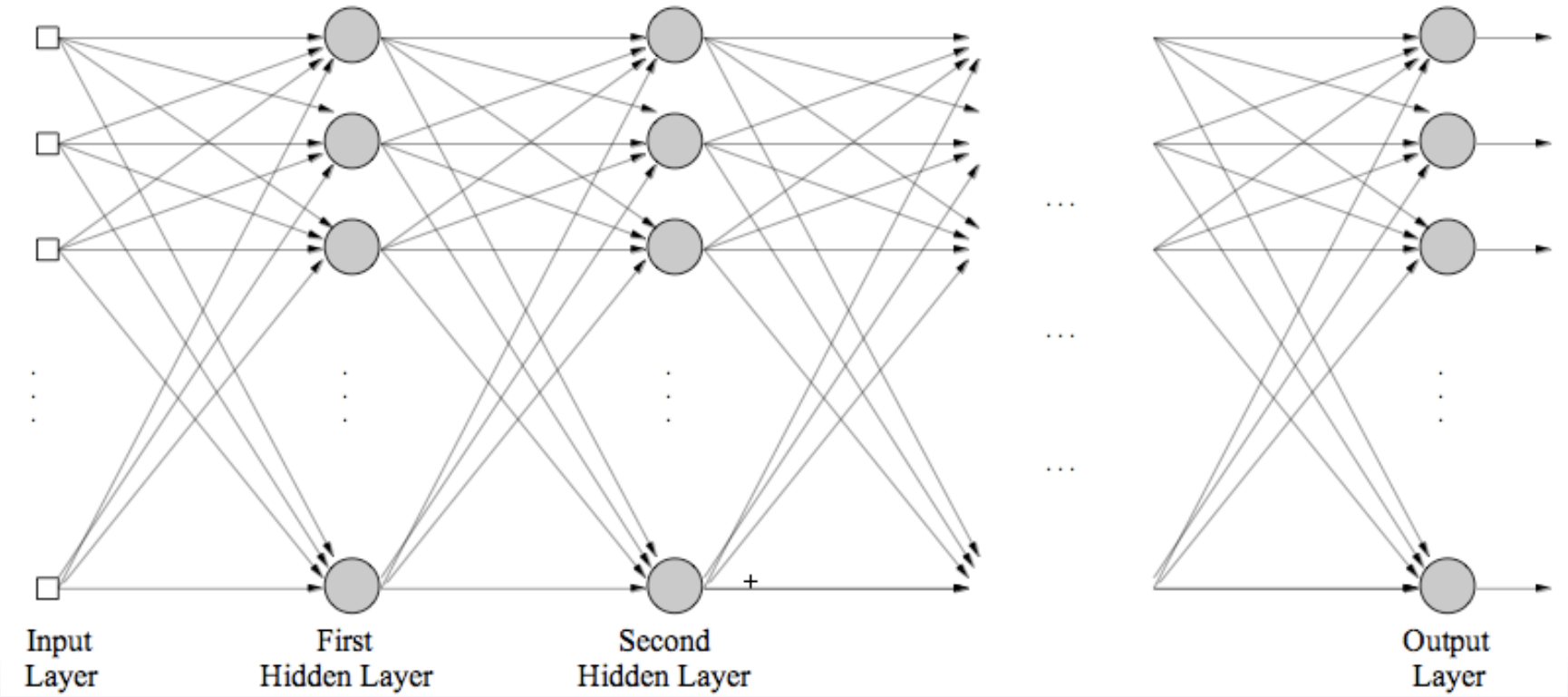
Artificial Neural Networks

- Neural Processing Unit - Neuron



Artificial Neural Networks

- Feed Forward Architecture



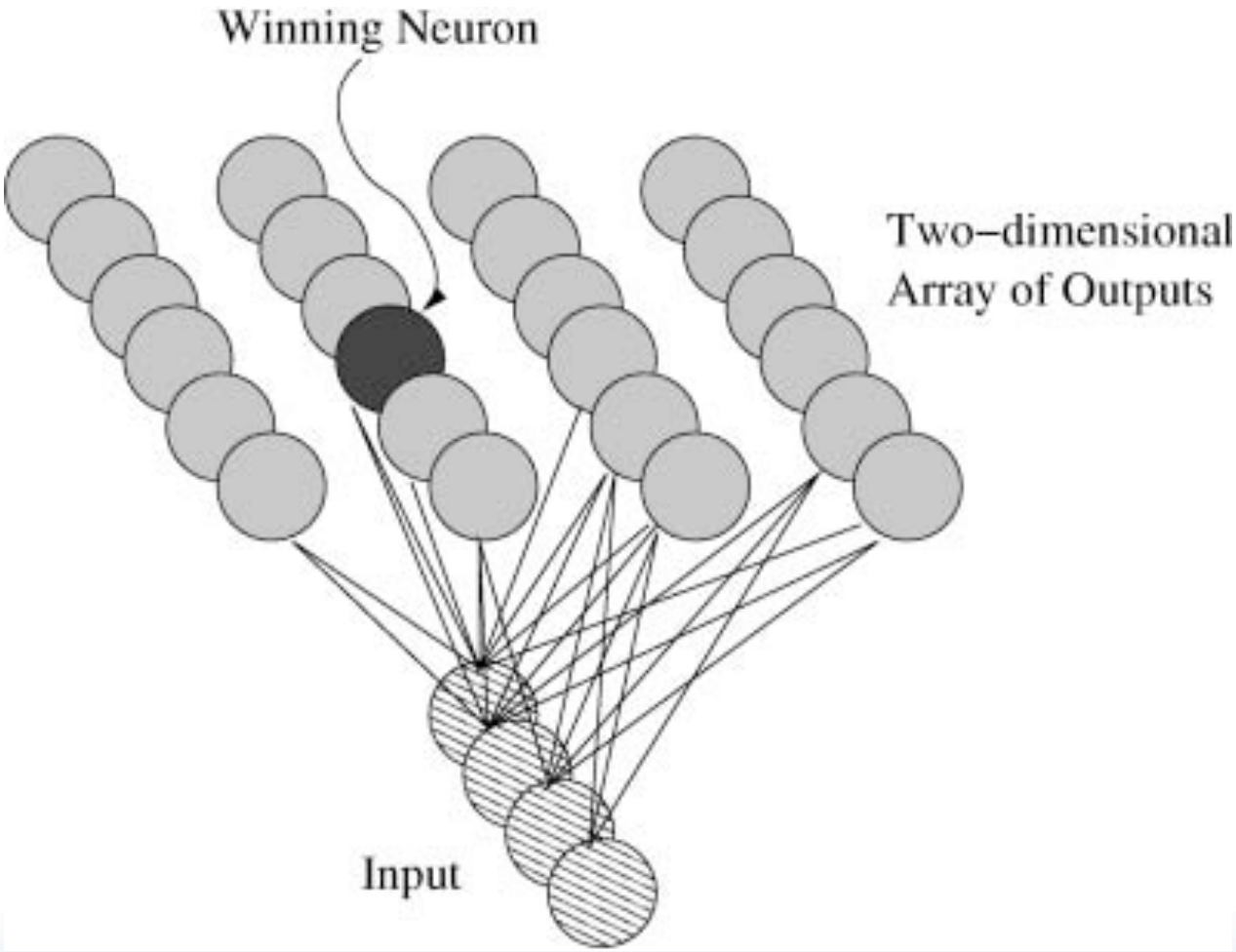
Artificial Neural Networks

- Training/Validation Sets
- Normal/Abnormal - examples of several classes of attacks
- Back Propagation Training

ANN Self-Organizing Maps

- SOMs are based on competitive learning.
- Kohonen's architecture is most common.
- Map an input signal of arbitrary dimensions to a 1- or 2-D output.
- Unsupervised learning.
- Input layer receives set of features.

ANN Self-Organizing Maps



ANN Self-Organizing Maps

- Given a pattern $\mathbf{x} = [x_1, x_2, \ldots, x_m]^T$
- Neuron j has weights

$$\mathbf{w}_j = [w_{j1}, w_{j2}, \ldots, w_{jm}]^T, j = 1, 2, \ldots, l$$

- Winning neuron $i(\mathbf{x}) = \min_j \|\mathbf{x} - \mathbf{w}_j\|$
- Learning rule

$$\mathbf{w}_j(n+1) = \mathbf{w}_j(n) + \eta(n) h_{j,\, i(x)}(n) (\mathbf{x} - \mathbf{w}_j(n))$$

ANN Self-Organizing Maps

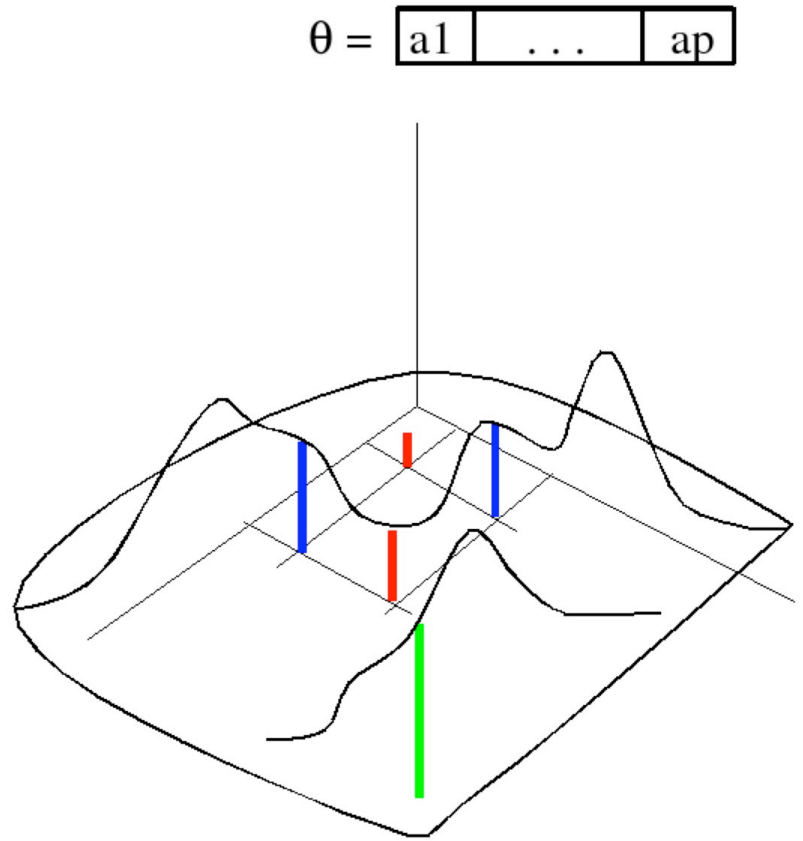
- SOMs are not classifiers
- Clusters normal and abnormal traffic data.
- Sets of normal data records activate certain neurons.
- All other neurons indicate suspicious activity.

ANN Self-Organizing Maps

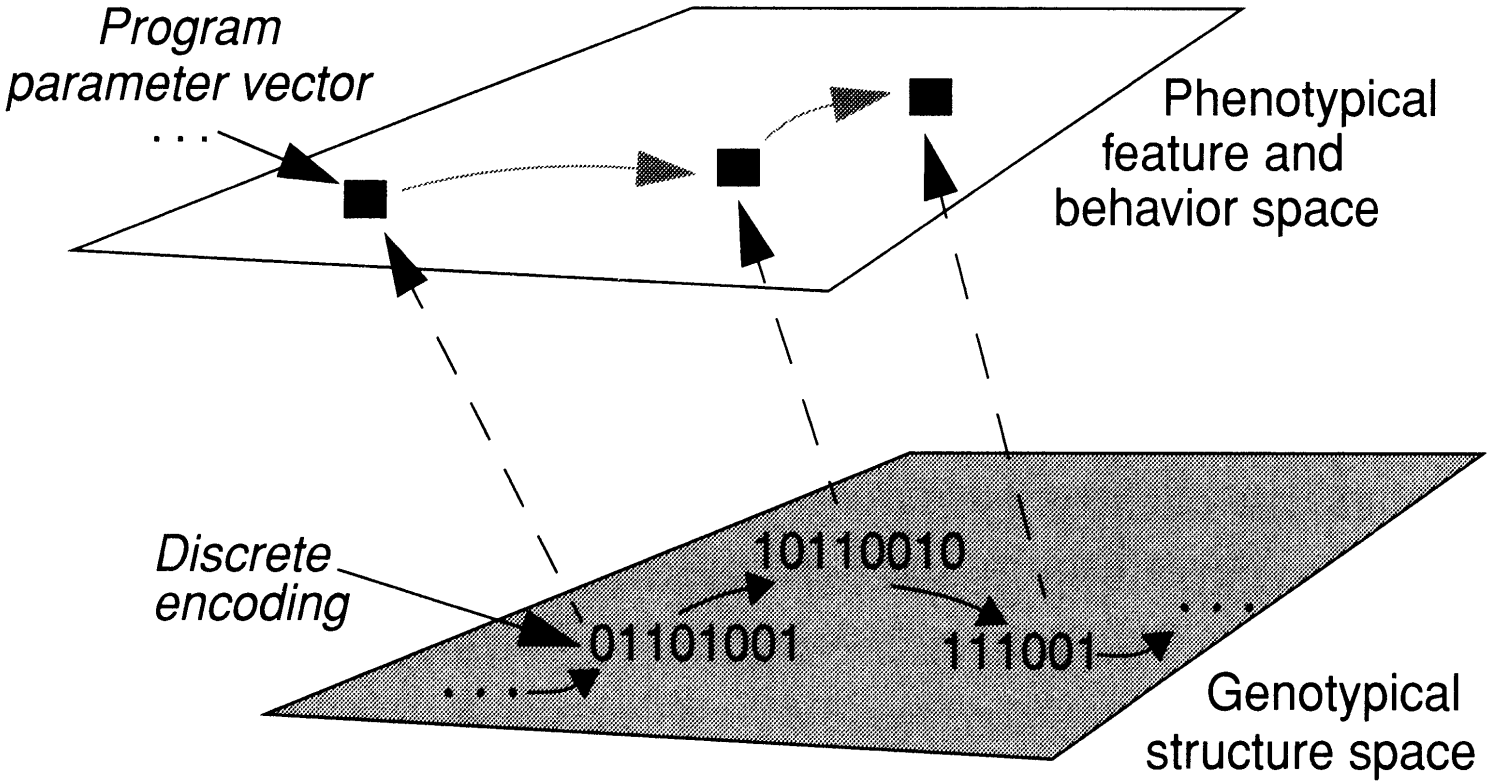
	1	2	3	4	5	6	7	8	9	10
1										
2		16								
3										
4										
5						54			8490	
6	1700				4					
7										
8										
9								8		
10			1511				1900			

Algoritmos Genéticos

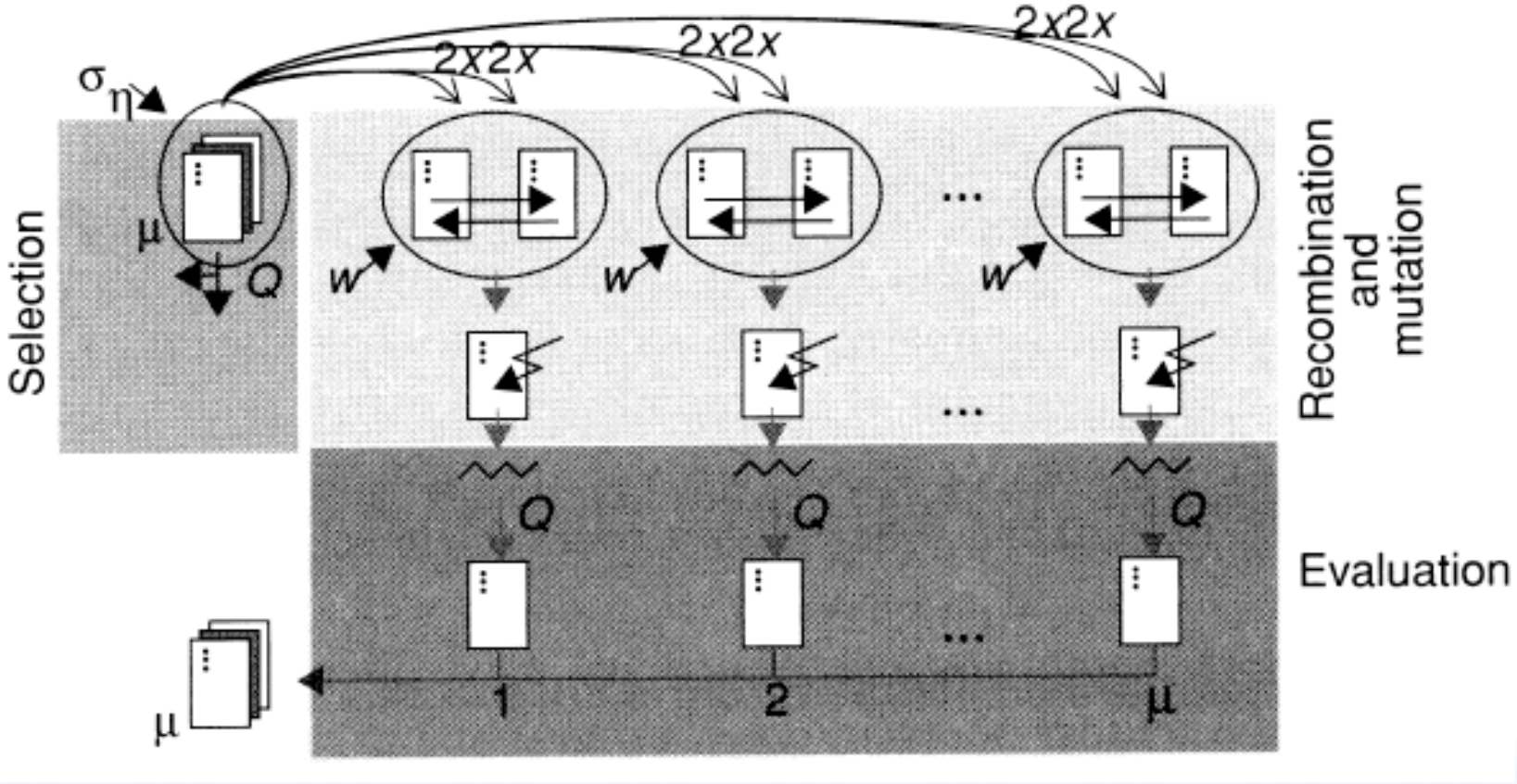
- Original
- Cruza
- Mutación



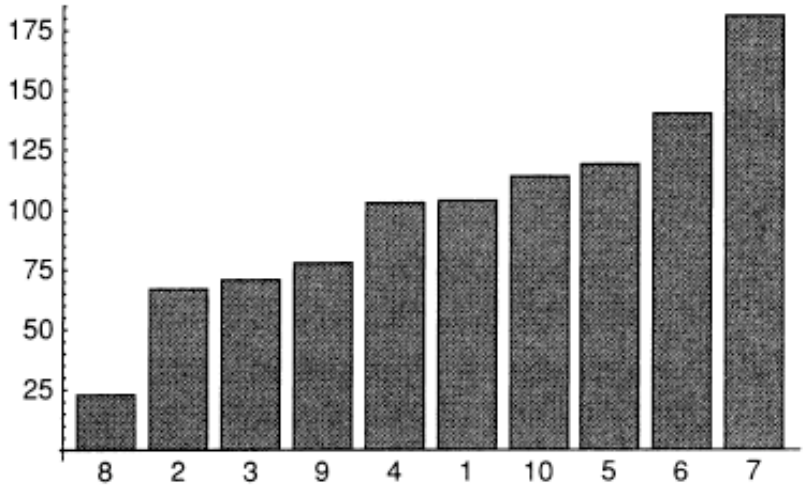
Fenotipo y Genotipo



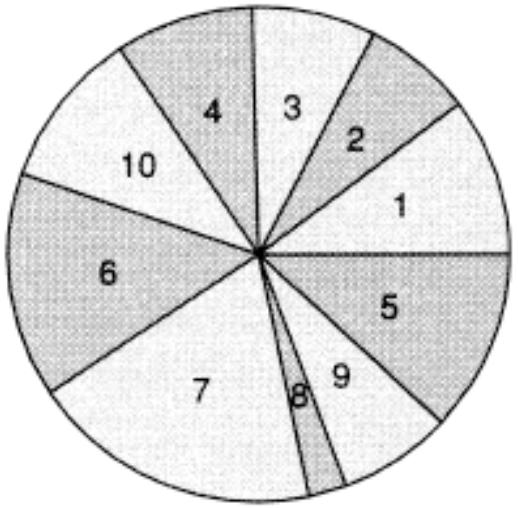
Esquemas de Evolución



Selección por Aptitud

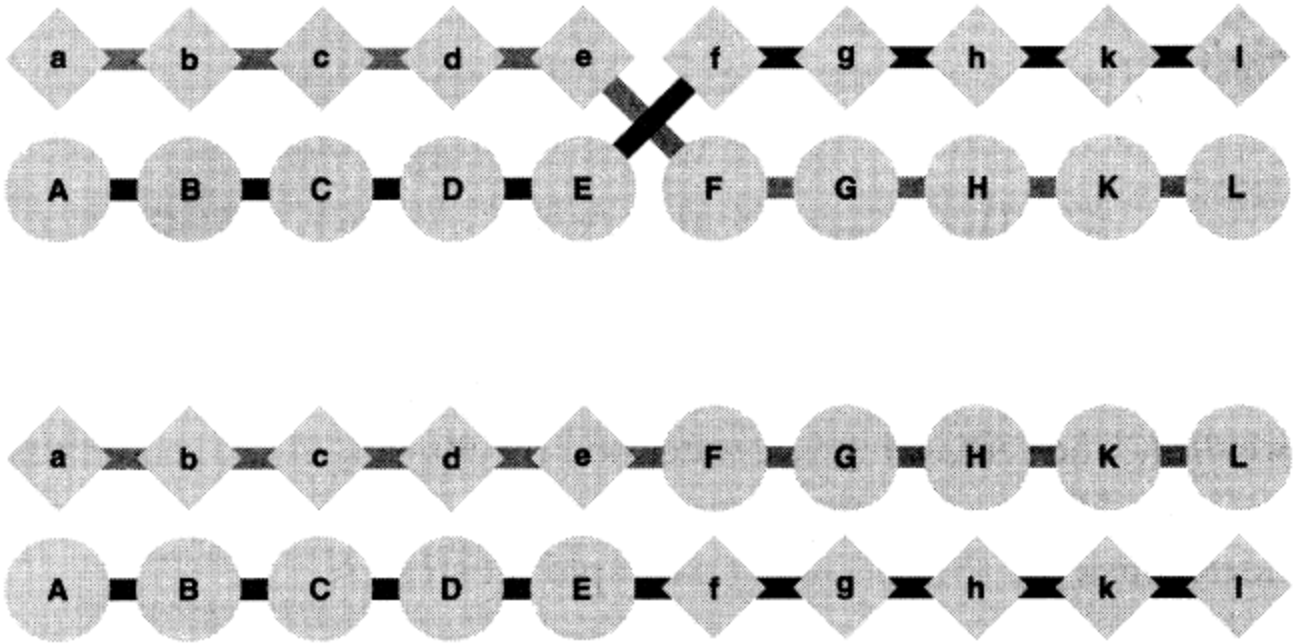


Aptitud



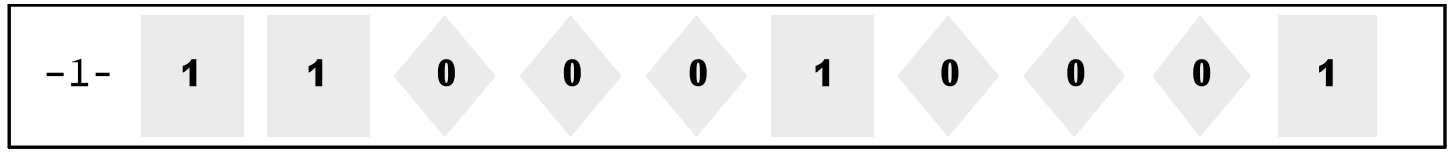
Probabilidad

Cruza

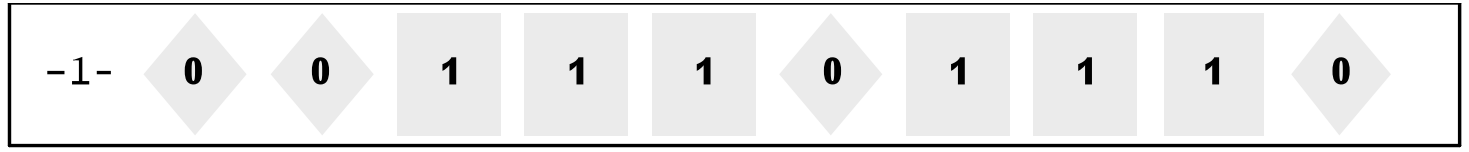


Mutación

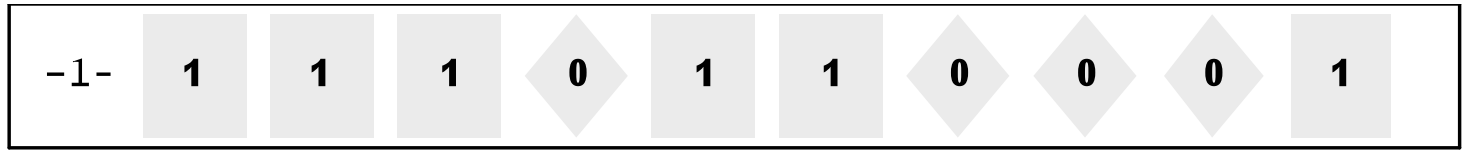
- Original

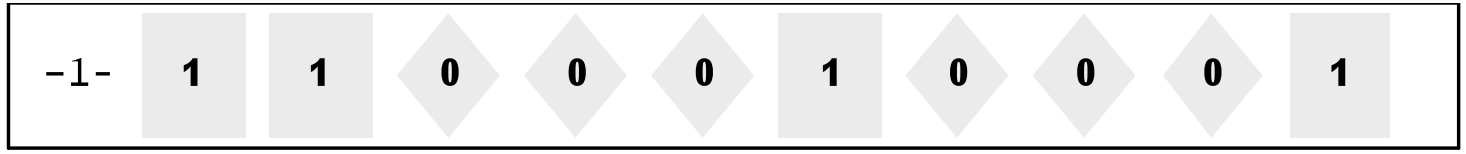


-



- mutación con probabilidad = 0.1

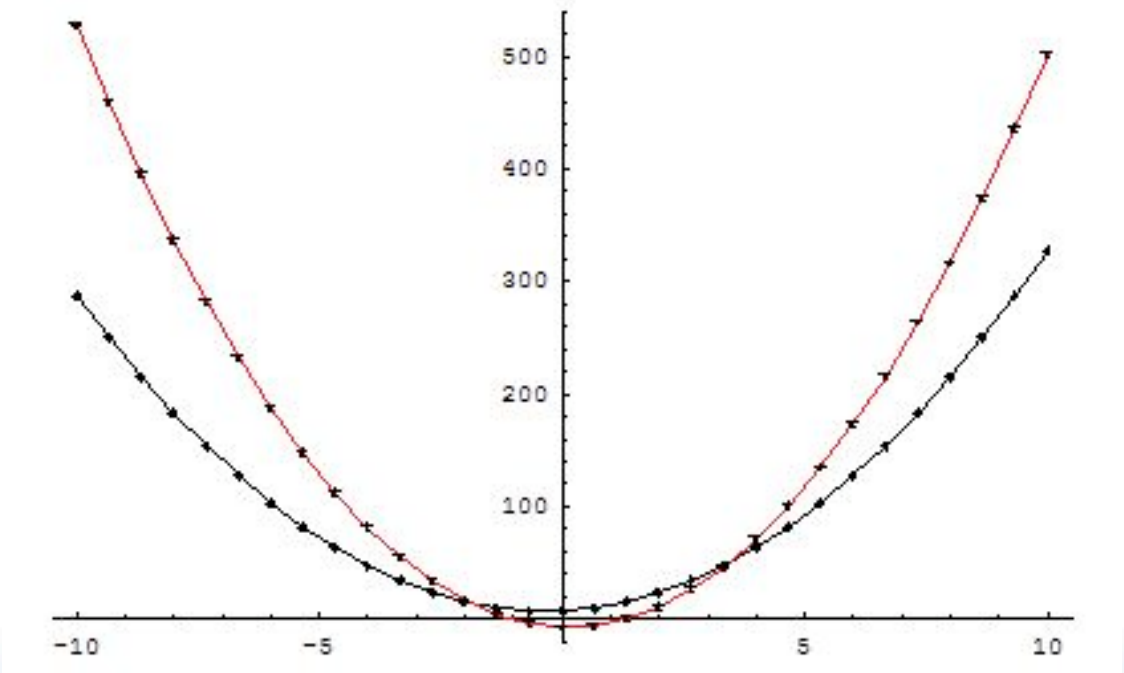




Ejemplo - Parábolas

$$y = ax^2 + bx + c$$

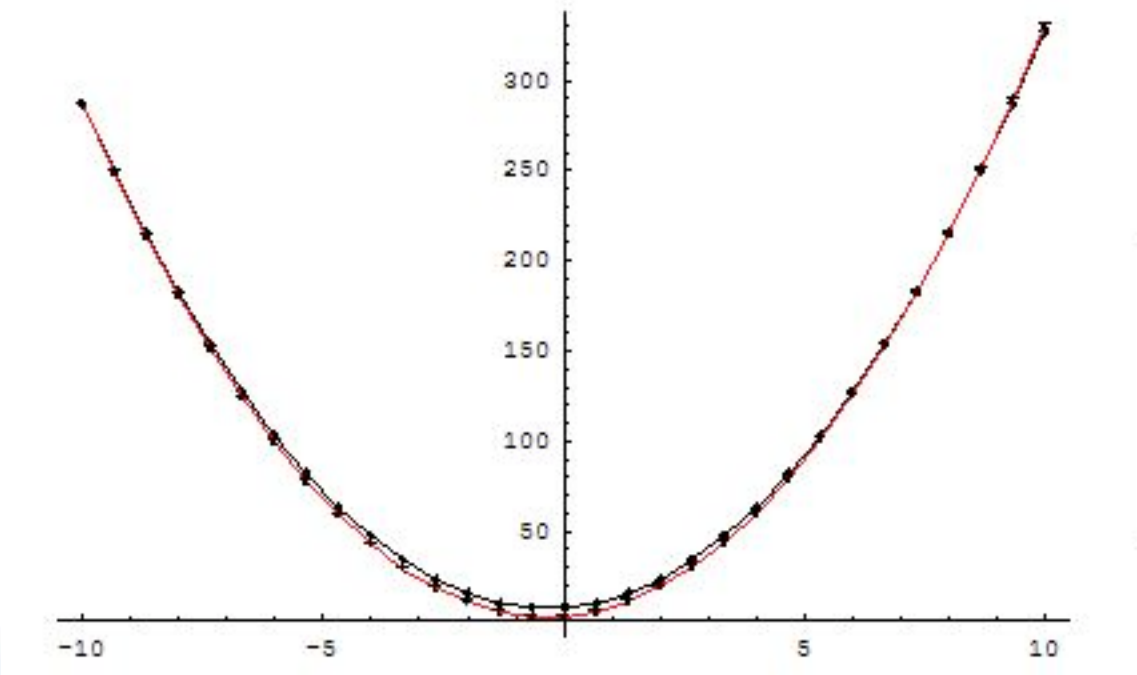
$a \quad b \quad c$



Ejemplo - Parábolas

$$y = ax^2 + bx + c$$

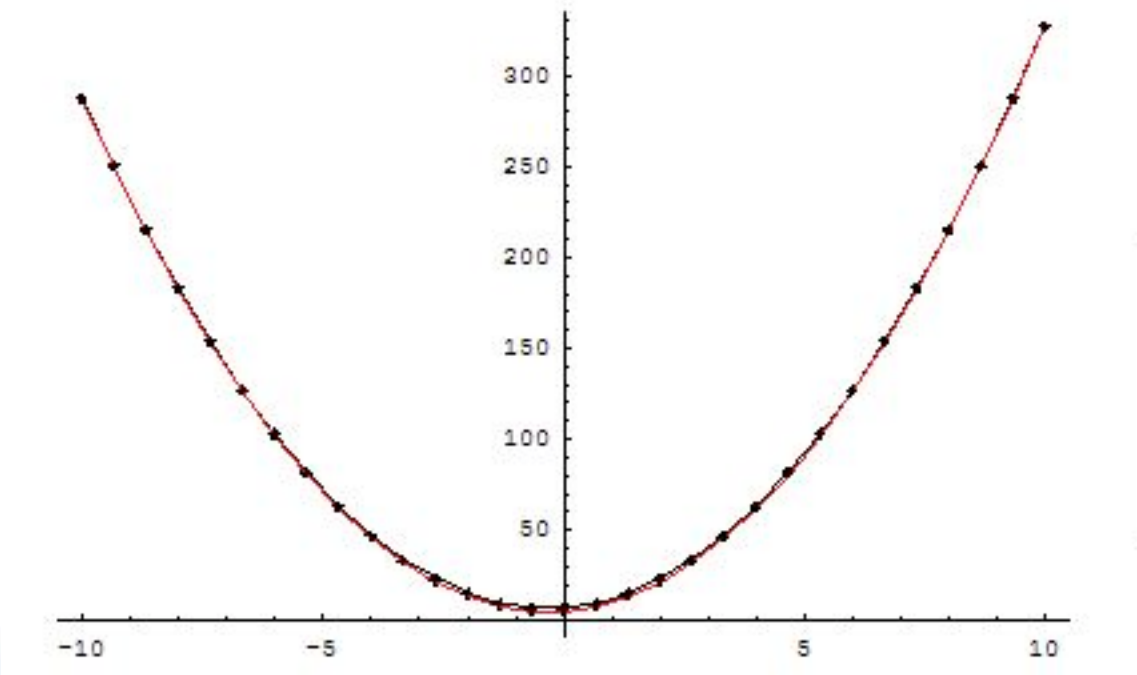
$a \quad b \quad c$



Ejemplo - Parábolas

$$y = ax^2 + bx + c$$

$a \quad b \quad c$



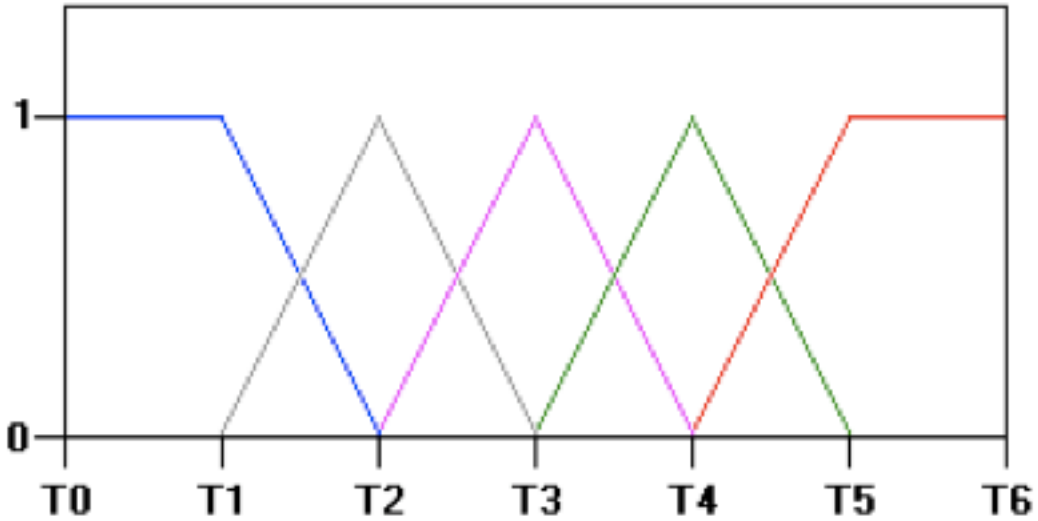
Fuzzy Systems

- Uncertainty in ID
  - ANNs
  - Fuzzy Classifiers
  - HMMs
  - Among others

Fuzzy Systems

- Fuzzy Linguistic Terms
- Fuzzy Rules
- Inference Mechanism
- Defuzzyfication

Fuzzy Systems

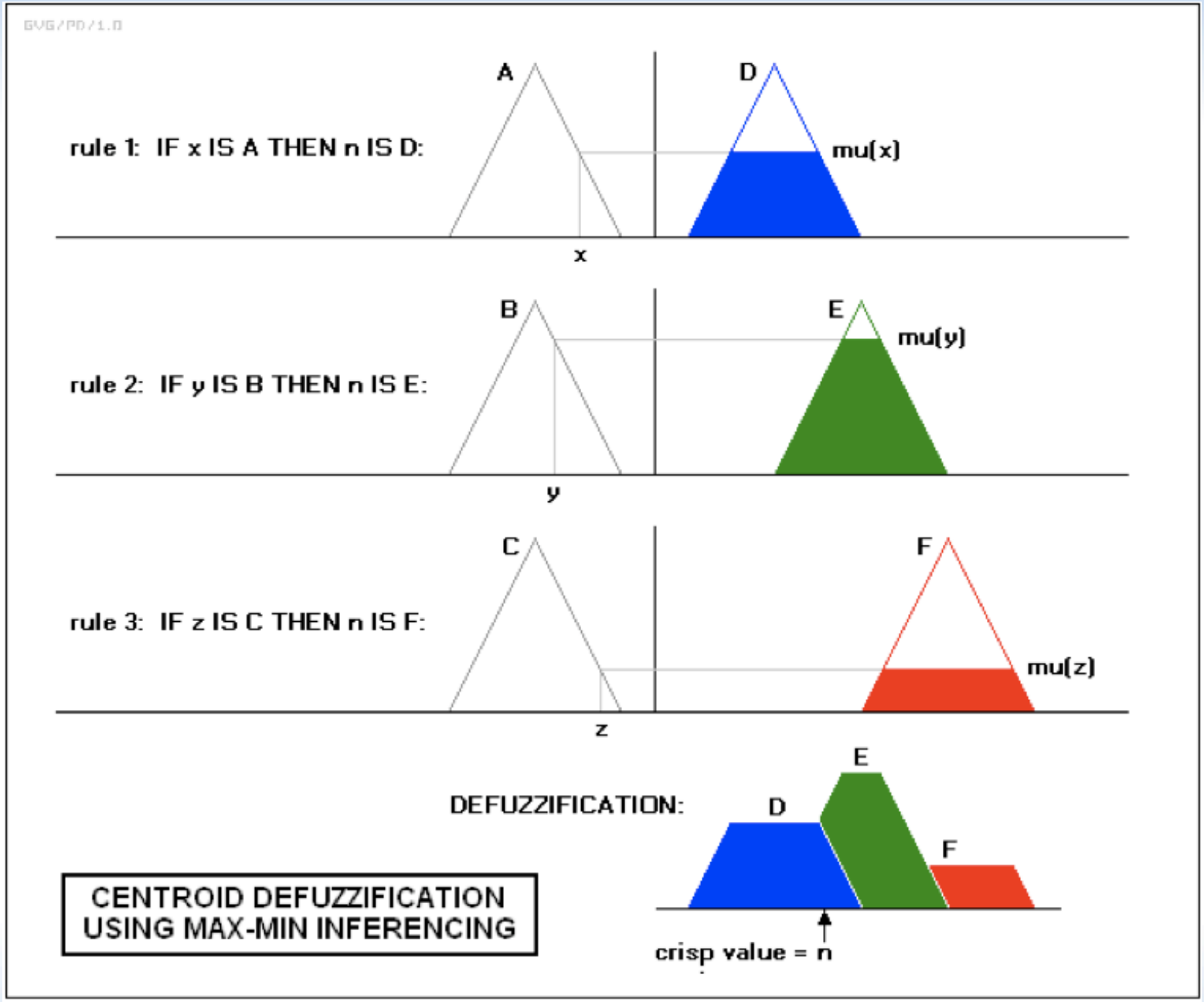


If src_bytes is low and

num_access_files is high

then attack_type is PAS

Fuzzy Systems



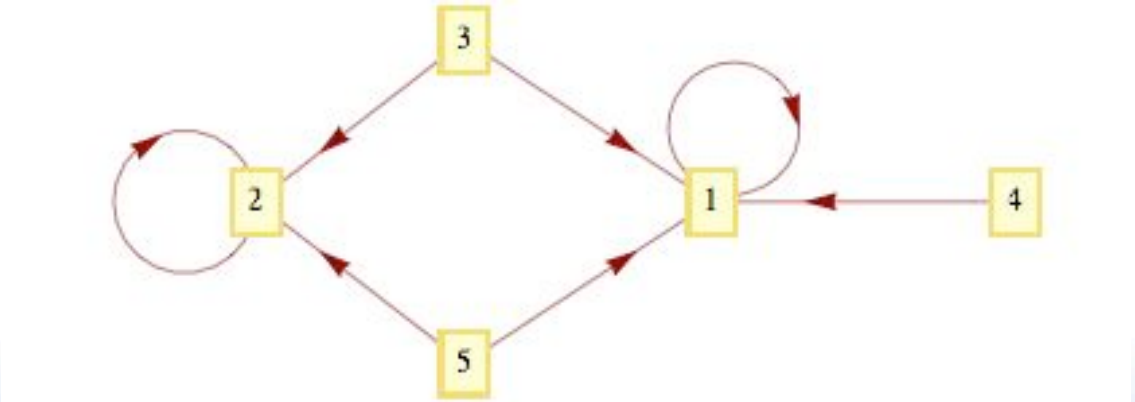
Fuzzy Systems

- Fuzzy version of expert Systems
- Rules
  - provided by expert
  - automatically learned (mined)
- Rule learning, GA, GP, etc.
- Given the set of rules, use GA to tune parameters

Hiden Markov Models

- An HMM is formed by a finite number of states connected by transitions.

- HMMs can generate an observation sequence depending on its transitions, and initial probabilities.



Genetic Algorithms (GAs)

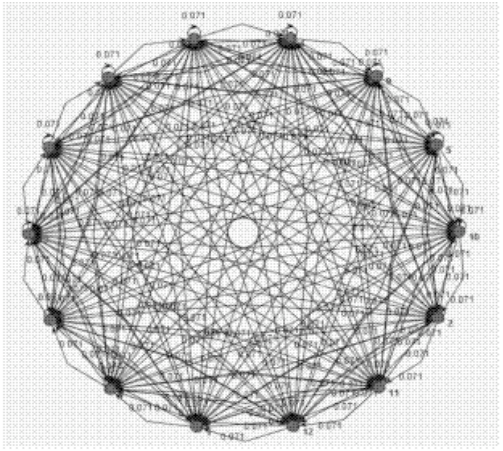
- Genetic Algorithms is a global search technique, that can be used to optimize the HMM parameters.

Framework For Evolving HMMs

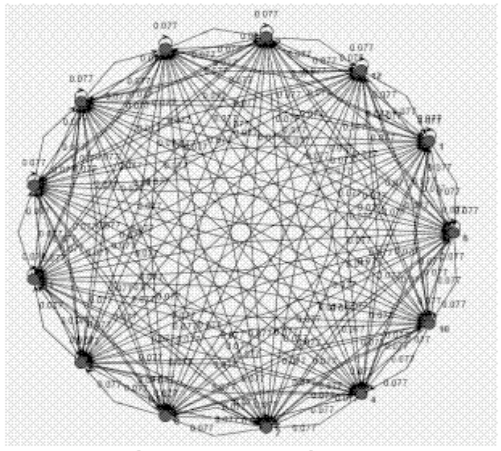
- We start with a random population of Chromosomes

SIZE	TRANSITIONS	PARAMETERS	Pi

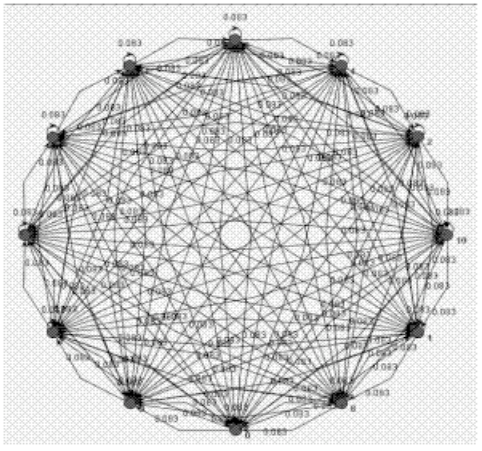
Evolving HMMs



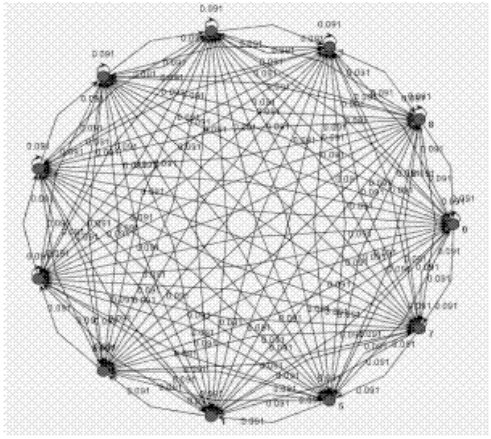
a) Generation 1



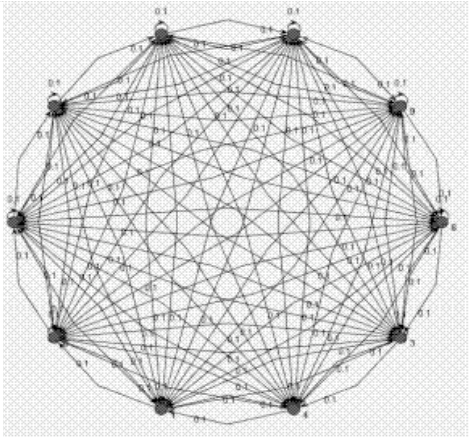
b) Generation 5



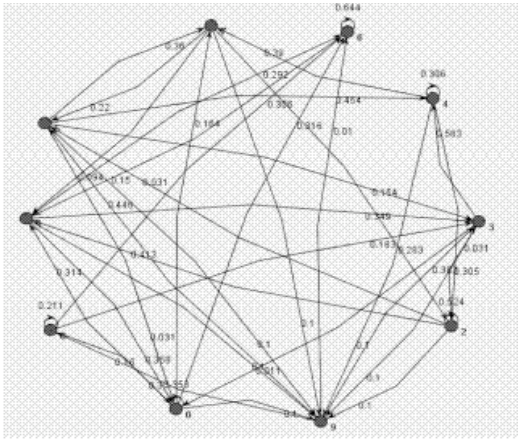
c) Generation 10



d) Generation 11



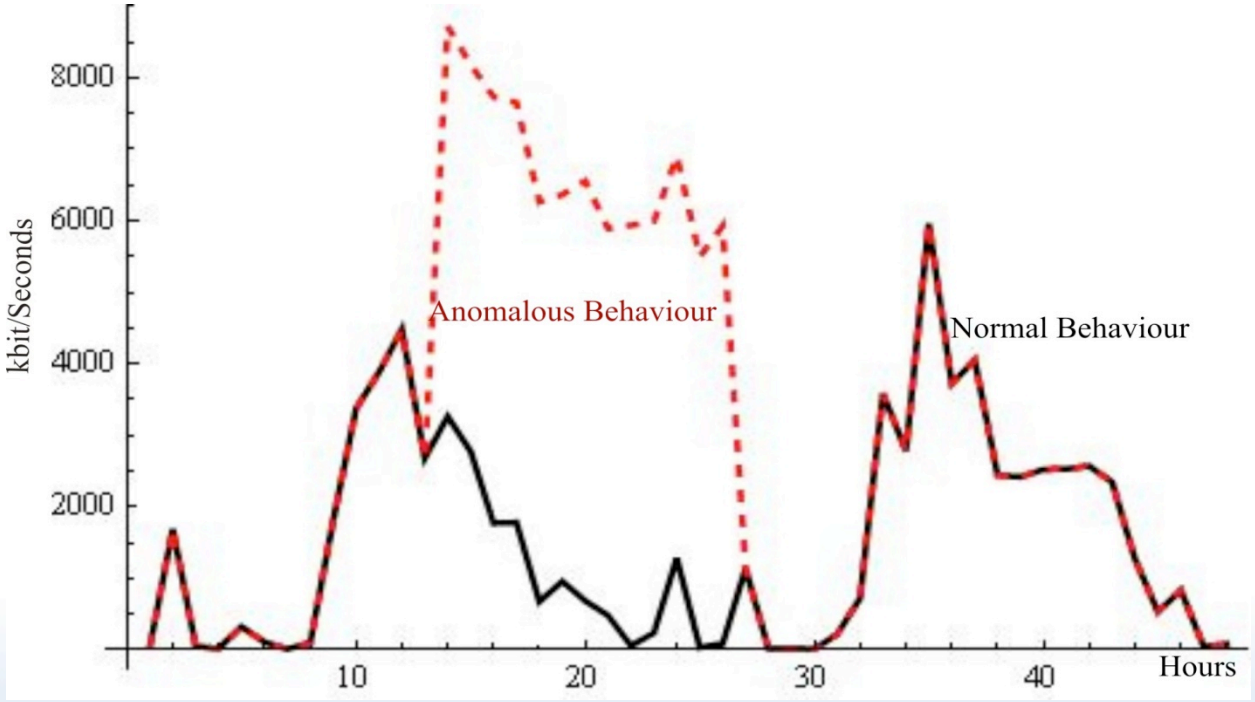
e) Generation 85



f) HMM evolved

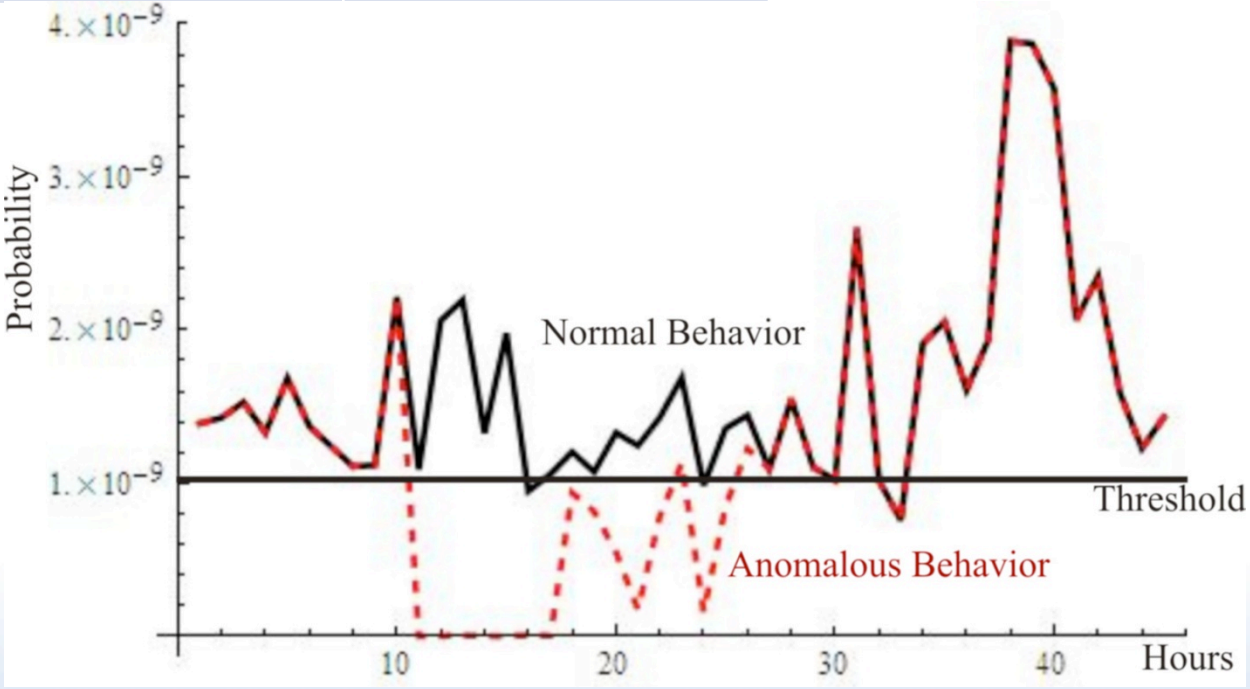
Results

- GAs evolved HMMs based on the observation sequence given by the network bandwith used at the UM.



Results…

Window Size	%		
	Hits	False Positives	False Negatives
3	89	7	4
4	*93*	*2*	*5*
5	89	4	7
6	84	5	11



Probability Graphic of Window Size 4

Agent-Based IDSs

- Each agent is an ID processor
  - Snort
- Platform for mobile agents
  - Morpheus
  - Jade
- Distributed sensors
- tcpdump
- Typically send alerts to a central processor
- Central processor integrates data
- More information → better discrimination

CONCLUSION

- IDS are not even close to our wishes.
- Work on hybridization of AI techniques
- Work on representation and reasoning schemes
- Work on hybridization Misuse-Anomaly Detection

FIN

¡GRACIAS!

juanf@umich.mx