User Authentication With Neural Networks

Nicola Capuano[1], Marco Marsella[1], Sergio Miranda[1], Saverio Salerno[1,2]

[1] CRMPA – Centro di Ricerca in Matematica Pura ed Applicata c/o DIIMA – University of Salerno, Italy

[2] DIIMA – Dipartimento di Ingegneria dell'Informazione e Matematica Applicata University of Salerno, Italy

e-mail: niccap@crmpa.unisa.it, marmar@crmpa.unisa.it, miranda@crmpa.unisa.it, salerno@ponza.dia.unisa.it.

USER AUTHENTICATION METHODS

1) **Knowledge-based methods** (password, passphrases)

2) **Artifacts** (keys, magnetic cards, etc.)

3) **Biometrics** (fingerprints, voice patterns, signatures, typing styles, etc.)

OUR APPROACH

Knowledge Based

+

Biometrics

Steps:

1) Password verification
2) Typing style recognition

TYPING STYPLE RECOGNITION

Step 1 - Hold and latency times calculation

Press	Release	Time	Hold	Latency
N		0		
	N	109	109	
I		216		107
C		292		-47
	I	339	123	
O		409		-55
	C	464	172	
	O	535	126	
L		561		26
	L	660	99	
A		769		109
	A	851	82	

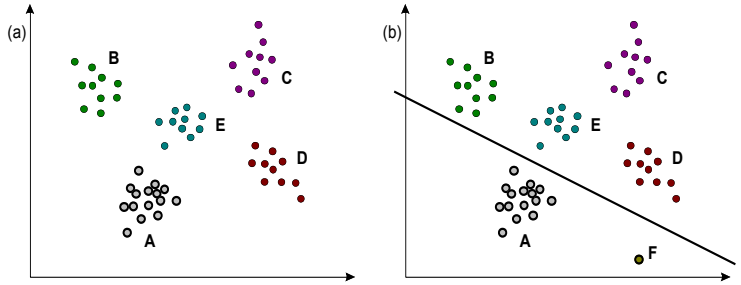
Step 2 - Neural Net interrogation

1st APPROACH: STANDARD MLP

Drawbacks:

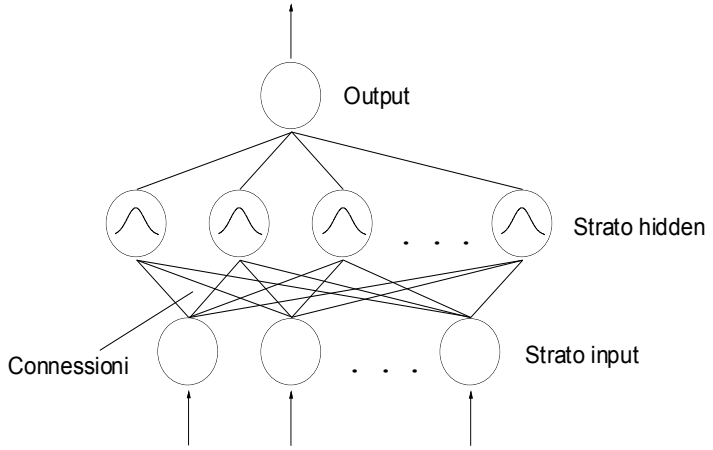
1) Correct and wrong patterns must be provided during the training phase (loss of security)

2) Training set cannot be representative of the universe



OUR NEURAL NET

Structure:



Hidden Layer Activation Function:

$$y_j = \exp\left\{-\frac{\|x - v_j\|^2}{2\sigma^2}\right\}$$

Output Layer Activation Function:

$$z = \max_j y_j$$

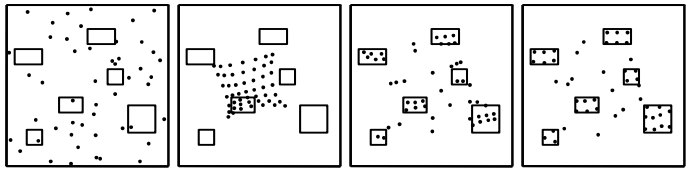
NEURAL-GAS TRAINING

Traditional SOM Adaptation Step:

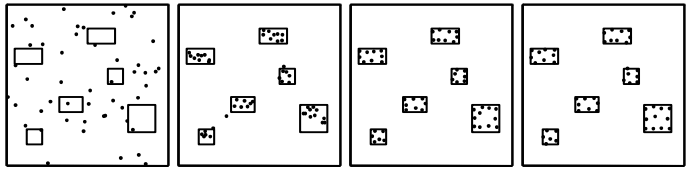
$$w_{ij}^{(t+1)} = w_{ij}^{(t)} + \varepsilon^{(t)} \cdot h_{\sigma^{(t)}}\left(d\left(j,k\right)\right) \cdot \left(x_i^{(t)} - w_{ij}^{(t)}\right)$$

Neural-Gas Adaptation Step:

$$w_{ij}^{(t+1)} = w_{ij}^{(t)} + \varepsilon^{(t)} \cdot h_{\sigma^{(t)}}\left(rank\left(j\right)\right) \cdot \left(x_i^{(t)} - w_{ij}^{(t)}\right)$$



SOM status after 0, 10, 25 e 50 epochs.

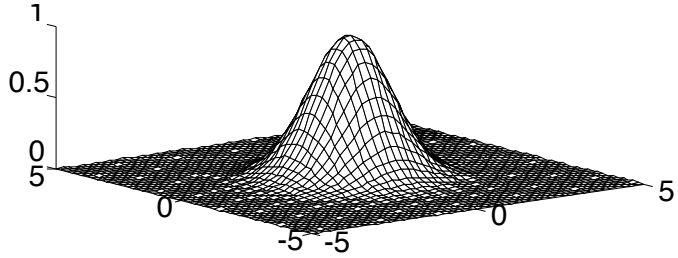


Neural-Gas status after 0, 10, 25 e 50 epochs.

A LAST QUESTION

Hidden layer activation function:

$$y_j = \exp\left\{-\frac{\left\|x - v_j\right\|^2}{2\sigma^2}\right\}$$



Modified Hidden layer activation function:

$$y_j = \exp\left\{-\sum_i \frac{\left(x_i - v_{ij}\right)^2}{2\sigma_{ij}^2}\right\}.$$

Where:

$$\sigma_{ij} = \sigma + mv_{ij}$$

EXPERIMENTAL RESULTS

User	Authentication	Intrusions
1	98 %	5 %
2	99 %	0 %
3	100 %	1 %
4	100 %	2 %
5	78 %	5 %
6	100 %	12 %
7	93 %	0 %
8	89 %	15 %
9	95 %	3 %
10	97 %	0 %

Parameters:

$N = 5, M = 15, \sigma = 0.6, m = 20, \varepsilon = 0.03$