Can a Fuzzy Rule Look for a Needle in a Haystack?

Akira Imada

Brest State Technical University
Belarus

Our Interest is

a Network Intrusion Detecion System

in which

we need a set of TEST-DATA

to train and test the system with.

⇓

This talk is a consideration on such a test-data.

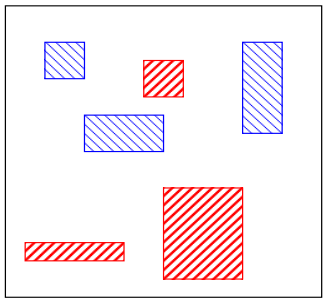
So many artificial data-samples have been proposed so far.

⇓

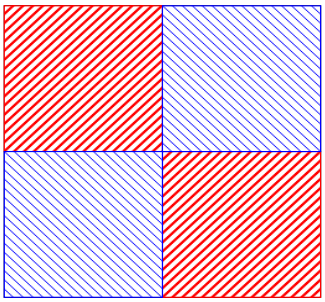
Let's categorize them

□ Fictitious 2-D pictures of test-sample

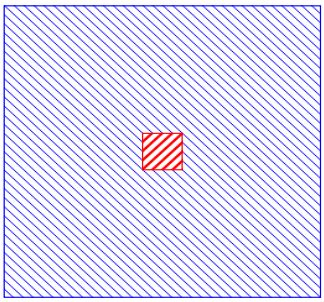
Do data cover the whole universe?



Do we train the system with both normal and abnormal?



What if the size of abnormal known is tiny?



□ Four concerns about so-far proposed test-sample

- Given data do not cover the whole universe
  - ⋆ E.g., Fisher's IRIS Flower, KDD-cup 1999/2003, $\cdots$

    $\Rightarrow$ We could miss crucial abnormal in no-defined area.

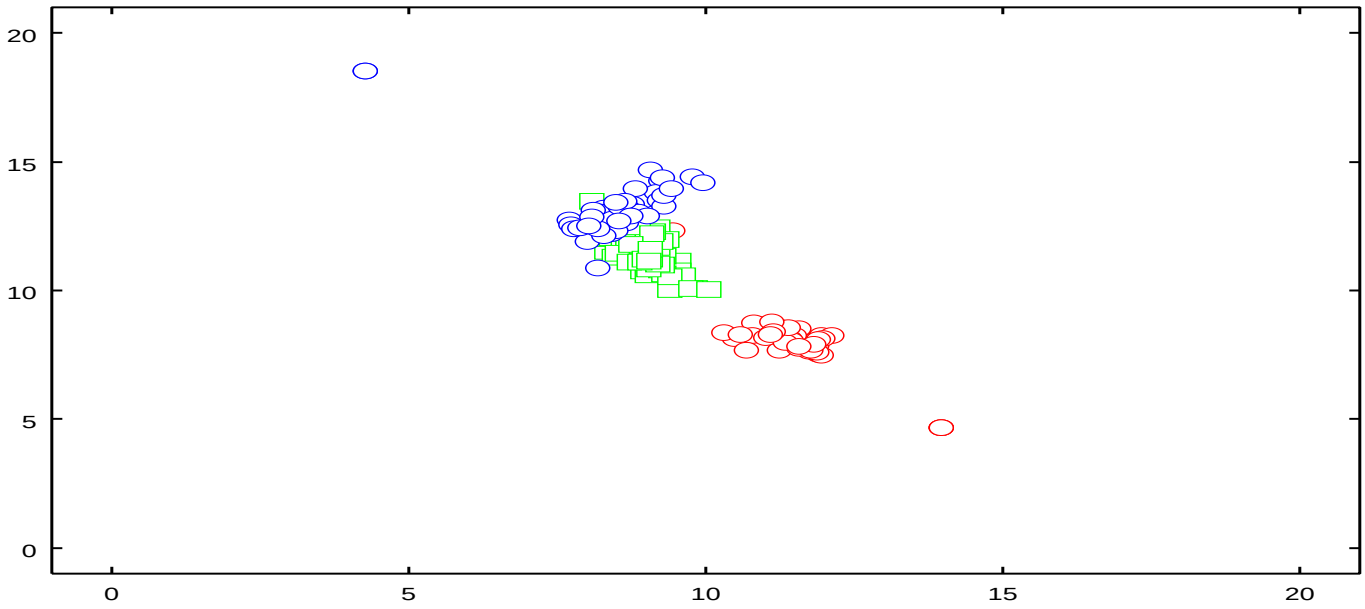
- Any search point is a possible candidate of transaction.
  - ⋆ E.g., Ayara et al.

- Train with both normal and abnormal sample.

  $\Rightarrow$ What if huge normal sample vs. few abnormal sample?

- Can we train the sytem only by NORMAL data?

□ A visualization of IRIS data



Our Goal is

to search for only a few ABNORMAL (no-self) pattern

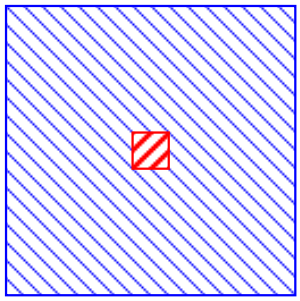
hidden in

an enormous amount of NORMAL (self) patterns

by

training using only NORMAL patterns

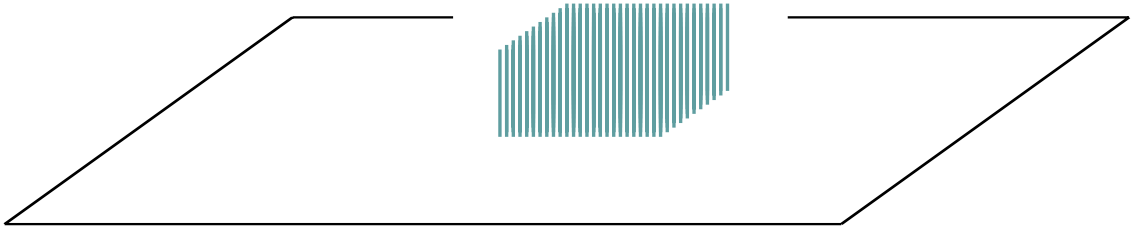
□ A tiny-flat-island-in-a-huge-lake



- Island $\Rightarrow x_i \in [-a, a]$ $(a \leq 1)$
- Lake $\Rightarrow x_i \in [-1, 1]$ $\quad (i = 1, \cdots, n)$.

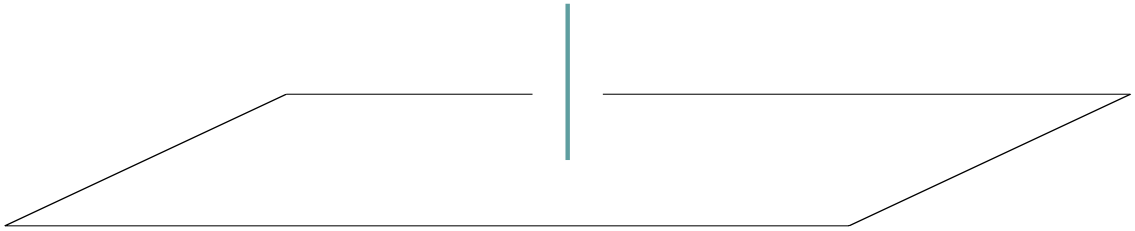
— We can control the complexity by changing the size.

□ From a fitness landscape point of view



□ A Needle in a Haystack

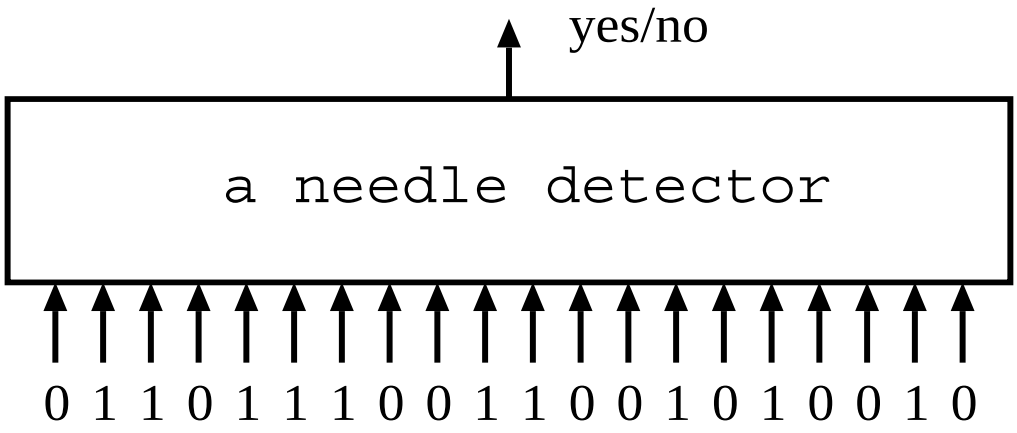
A schematic skecth on fictitious 2D-space



The original Hinton & Nowlan's Needle:

- A-needle ⇒ Only one configuration of 20 bits of binary string.
- Haystack ⇒ $2^{20} - 1$ search points.

□ **What can we do to look for the needle?**

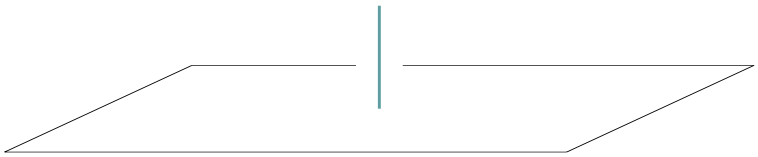


□ How difficult?

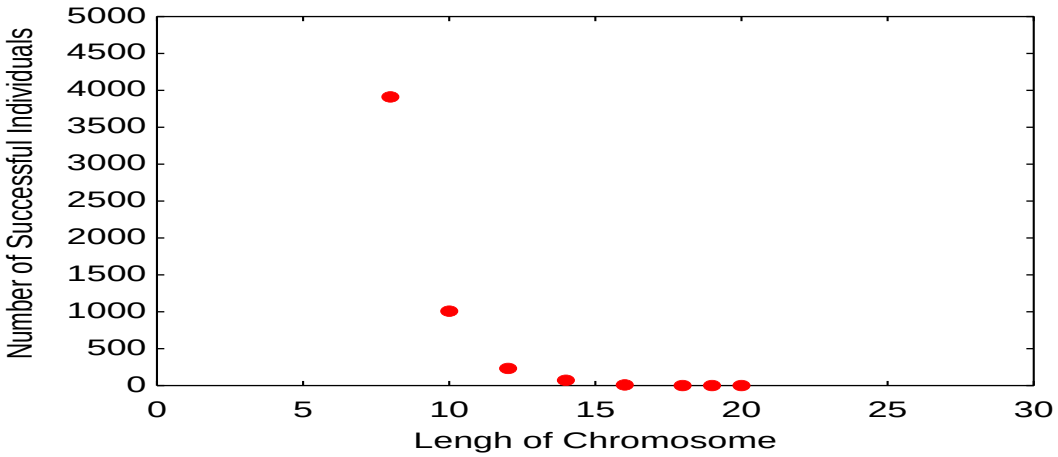
- Random Search

$$2^{20} = 1,048,576$$

- Lifetime Learning – Baldwin Effect (Hinton & Nowlan 1995?)



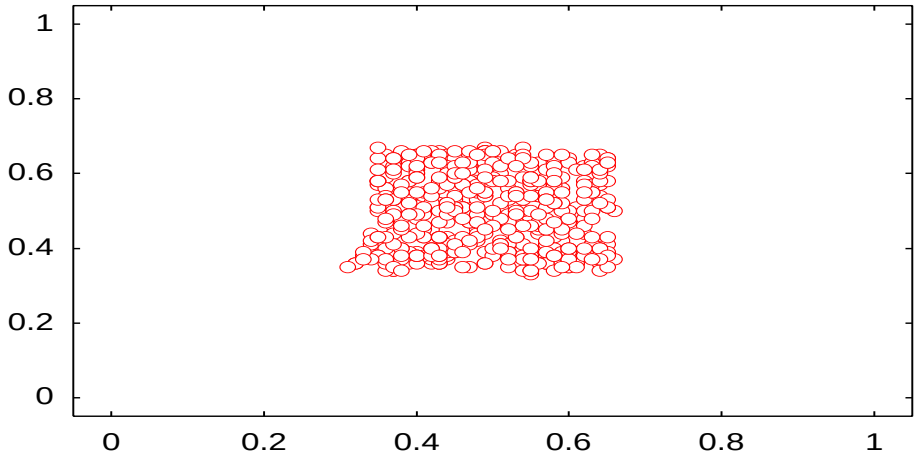
□ Random Search



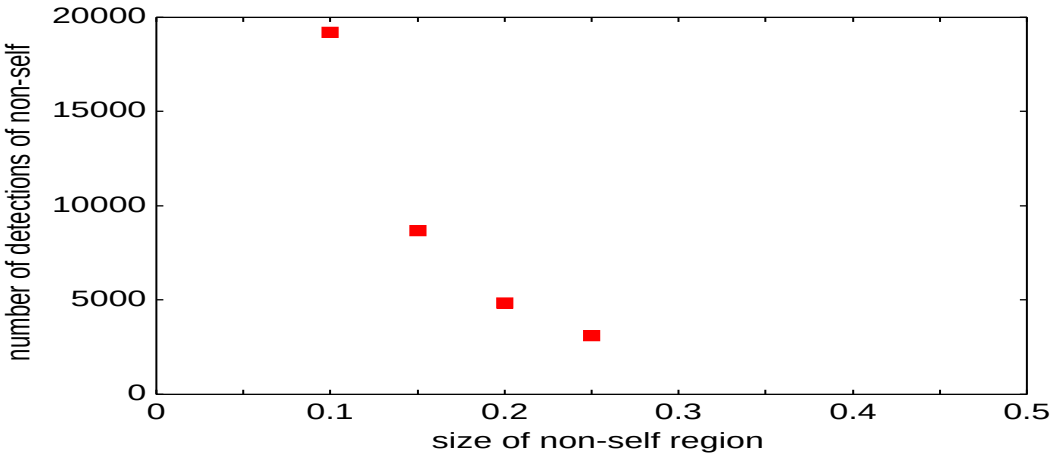
□ How can we approach it?

- Artificial Immune System
- Evolutionary Computation
- Fuzzy Rule
- Data-mining Technique
- etc

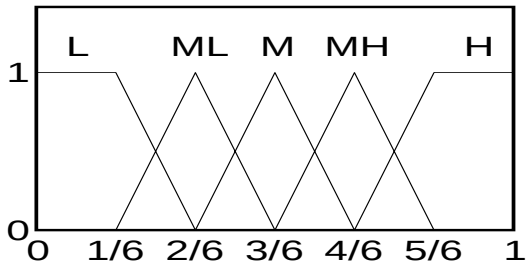
An immune approach — Sphere Detectors



□ What if top area shrinks to zero?



A Fuzzy approach



$$\Downarrow$$

$$(MMMMMM\cdots M)$$

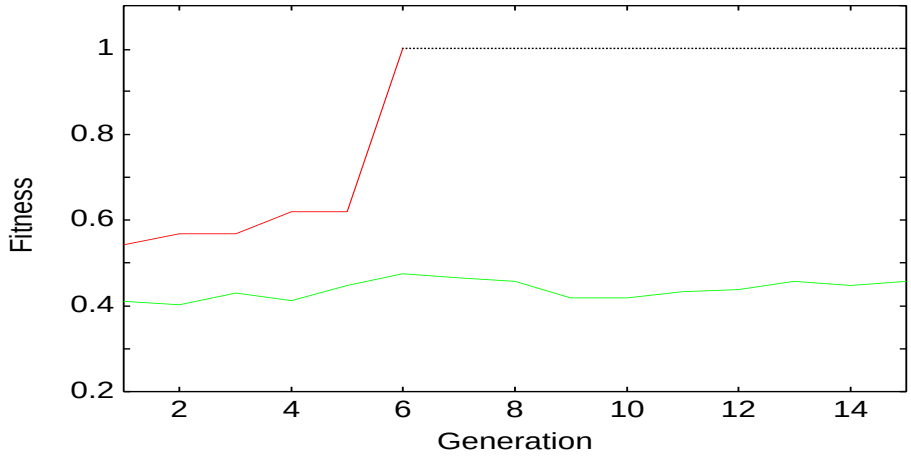
$$\Downarrow$$

IF $\{x_1$ is Middle$\}, \cdots,$ and $\{x_{20}$ is Middle$\}$ THEN no-self.

□ Island in the 6-D lake

Fairly large island ($x_i \in [0.25, 0.75]$)
vs.
Small island ($x_i \in [0.45, 0.55]$)

$\Downarrow$



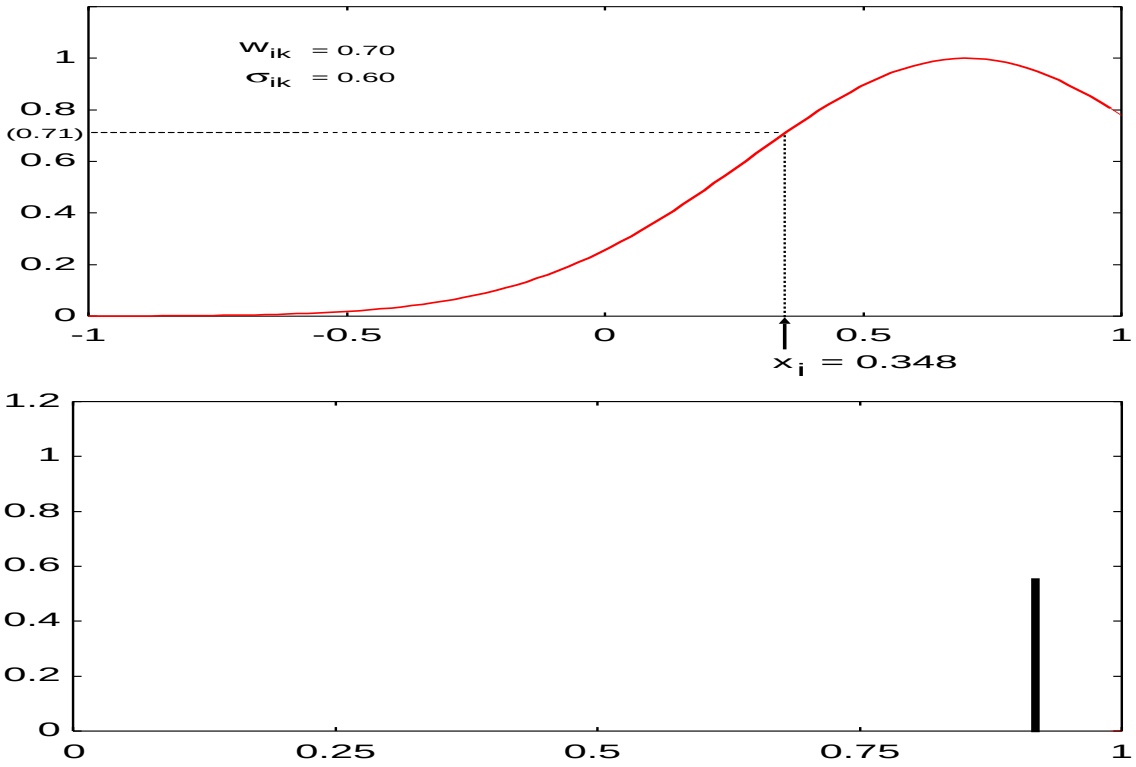
□ A curse of dimension

For the island $x_i \in [0.45,0.55]$ in the 20-D lake

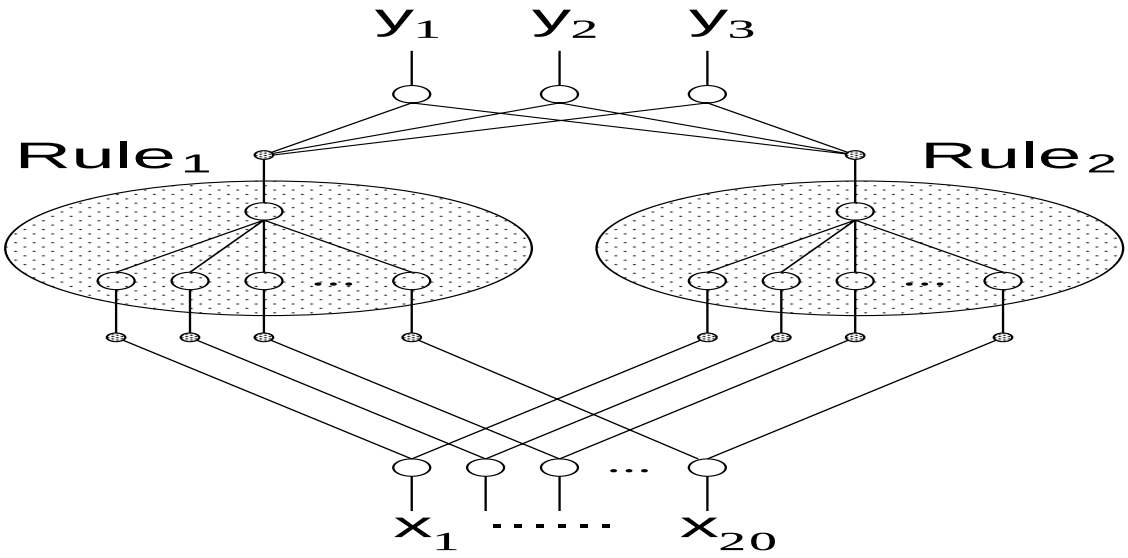
$$\Downarrow$$

$$(0\ 1\ 3\ 4\ 0\ 4\ 4\ 1\ 4\ 4\ 1\ 1\ 4\ 1\ 4\ 3\ 0\ 0\ 0\ 2)$$

Shape/Location adaptive membersip function



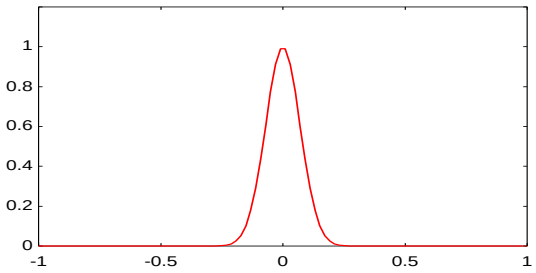
A Fuzzy Neural Network Approach



A result of an evolution

$$M$$

$$\Downarrow$$



□ Conclusion

We usually don't know many ABNORMAL samples while we have fuge NORMAL samples.

If we know what(where) is ABNORMAL in advance its really easy to be detected.

⇓

Training should be only by using NORMAL samples!

⇓

a-needle or tiny-island as testdata for net work intrusion detection"

- **This is somewhat old but still UNKNOWN and worth while tackle again.**