Review

- More on Hebbian Learning
- Heteroassociative Architecture
- Backpropagation

Review – Backpropagation

- Backpropagation is the most well know and widely used neural network system
- It is a multi-layered, feedfoward, perceptron-like structure
- Uses the backpropagation rule (or generalized delta rule) for training

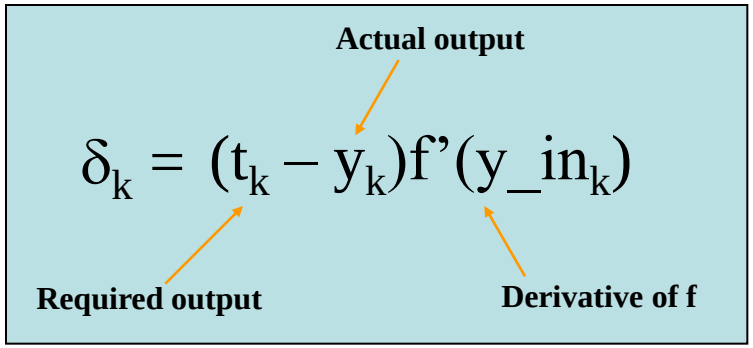
OUTLINE

- Backpropagation Training
- Applications
  - –IDS
  - –Eyes

Backpropagation Training

Training Algorithm 1

- **Step 0: Initialize the weights to small random values**
- **Step 1: Feed the training sample through the network and determine the final output**
- **Step 2: Compute the error for each output unit, for unit k it is:**



Training Algorithm 2

- Step 3: Calculate the weight correction term for each output unit, for unit k it is:

$$\Delta w_{jk} = \alpha \delta_k z_j$$

Hidden layer signal

A small constant

Training Algorithm 3

- Step 4: Propagate the delta terms (errors) back through the weights of the hidden units where the delta input for the j^{th} hidden unit is:

$$\delta\_in_j = \sum_{k=1}^{m} \delta_k w_{jk}$$

The delta term for the j^{th} hidden unit is:

$$\delta_j = \delta\_in_j f'(z\_in_j)$$

Training Algorithm 4

- Step 5: Calculate the weight correction term for the hidden units:

$$\Delta w_{ij} = \alpha \delta_j x_i$$

- Step 6: Update the weights:

$$w_{jk}(new) = w_{jk}(old) + \Delta w_{jk}$$

- Step 7: Test for stopping (maximum cylces, small changes, etc)

Options

- There are a number of options in the design of a backprop system
  - Initial weights – best to set the initial weights (and all other free parameters) to random numbers inside a small range of values (say –0.5 to 0.5)
  - Number of cycles – tend to be quite large for backprop systems
  - Number of neurons in the hidden layer – as few as possible

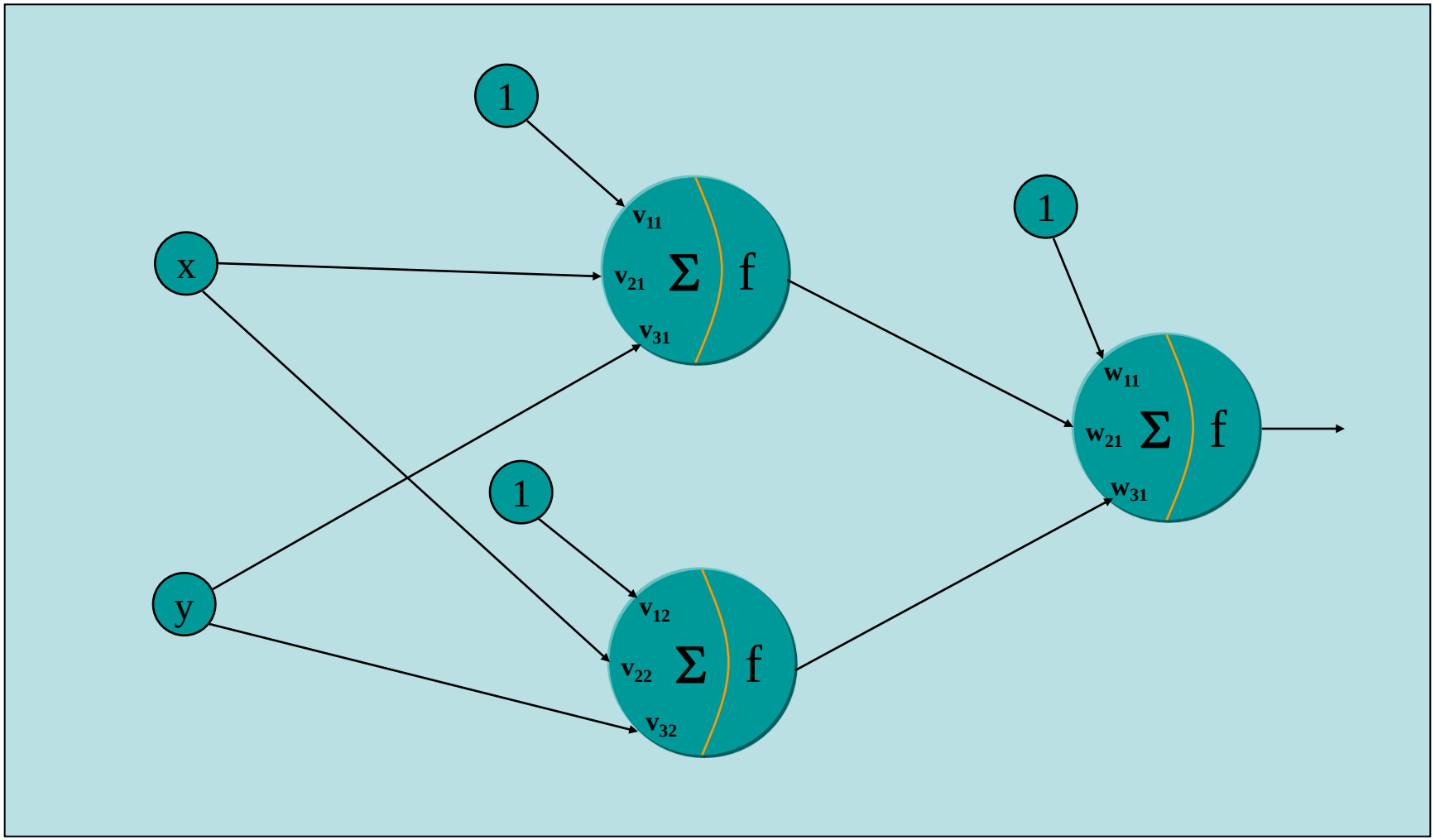
Example

- The XOR function could not be solved by a single layer perceptron network

- The function is:

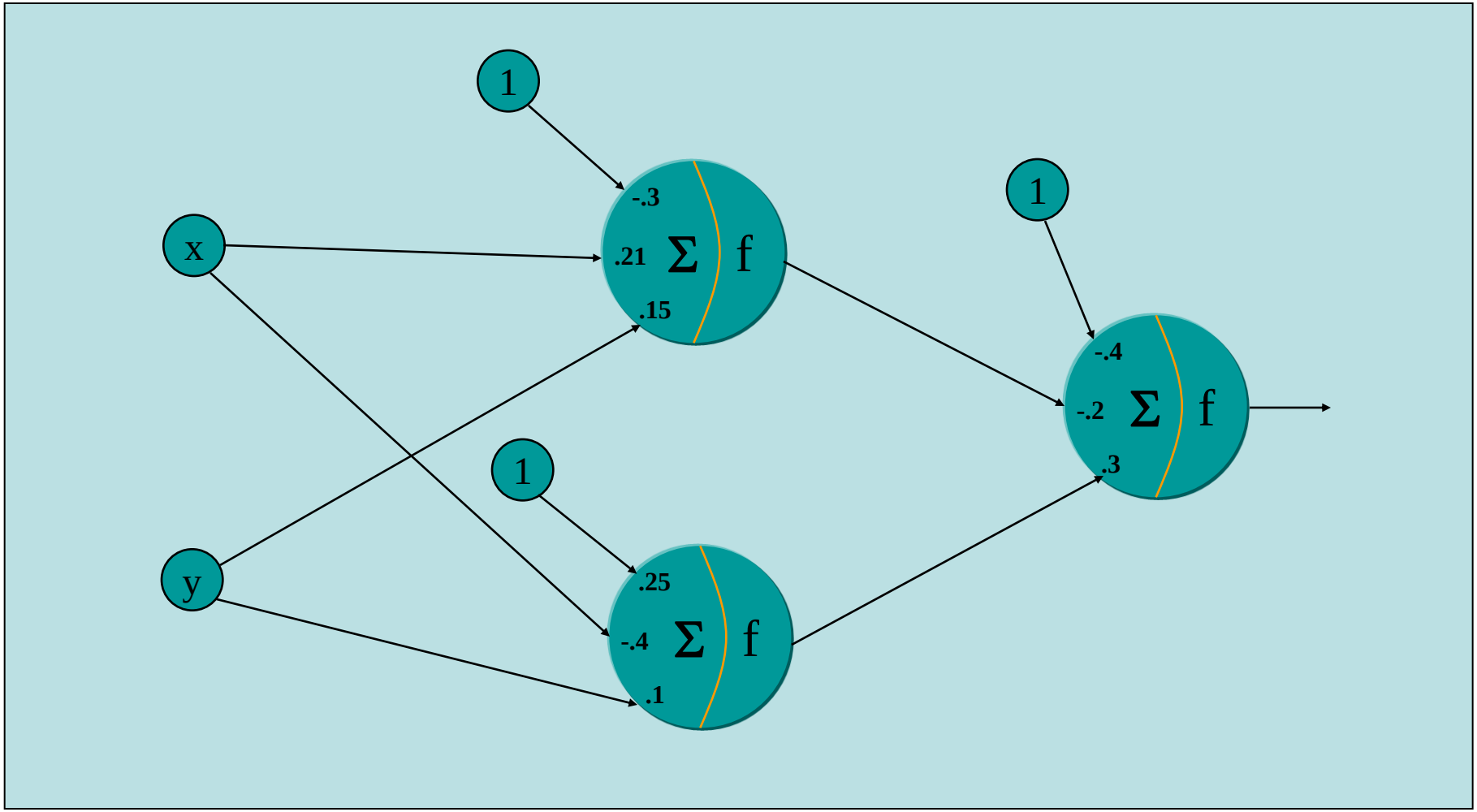
X	Y	F
0	0	0
0	1	1
1	0	1
1	1	0

XOR Architecture

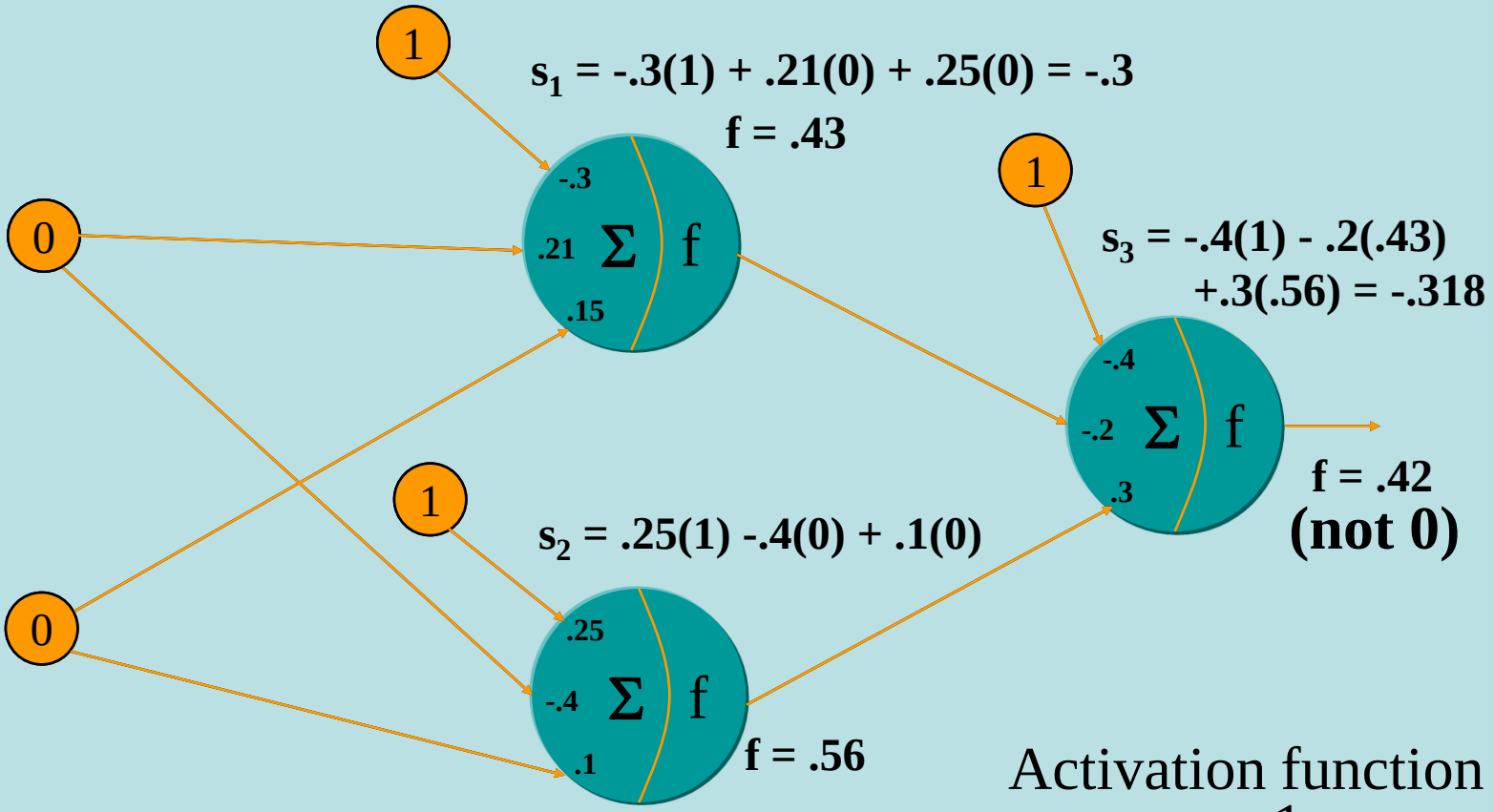


Initial Weights

- Randomly assign small weight values:



Feedfoward – 1st Pass

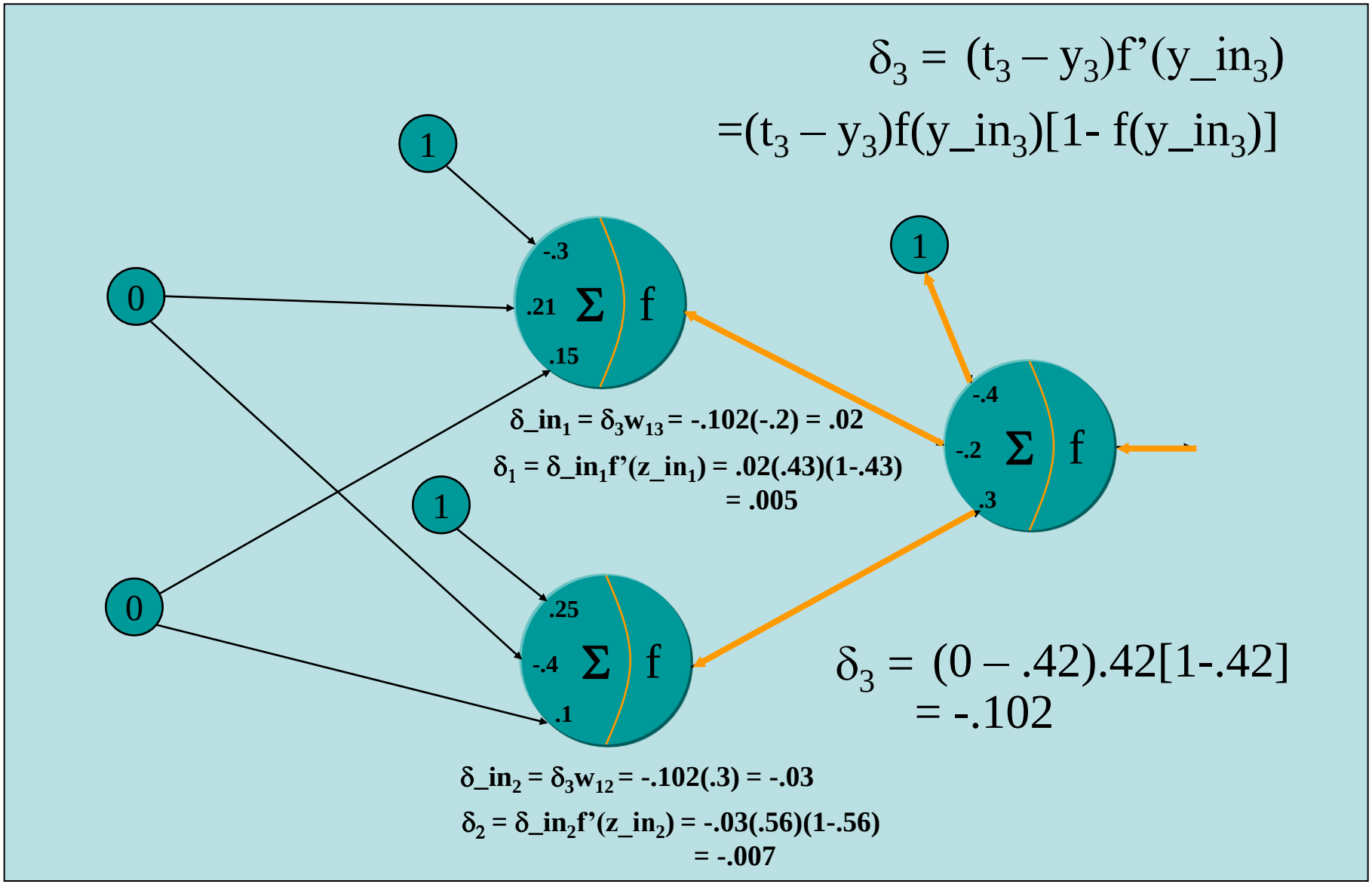


Training Case: (0 0 0)

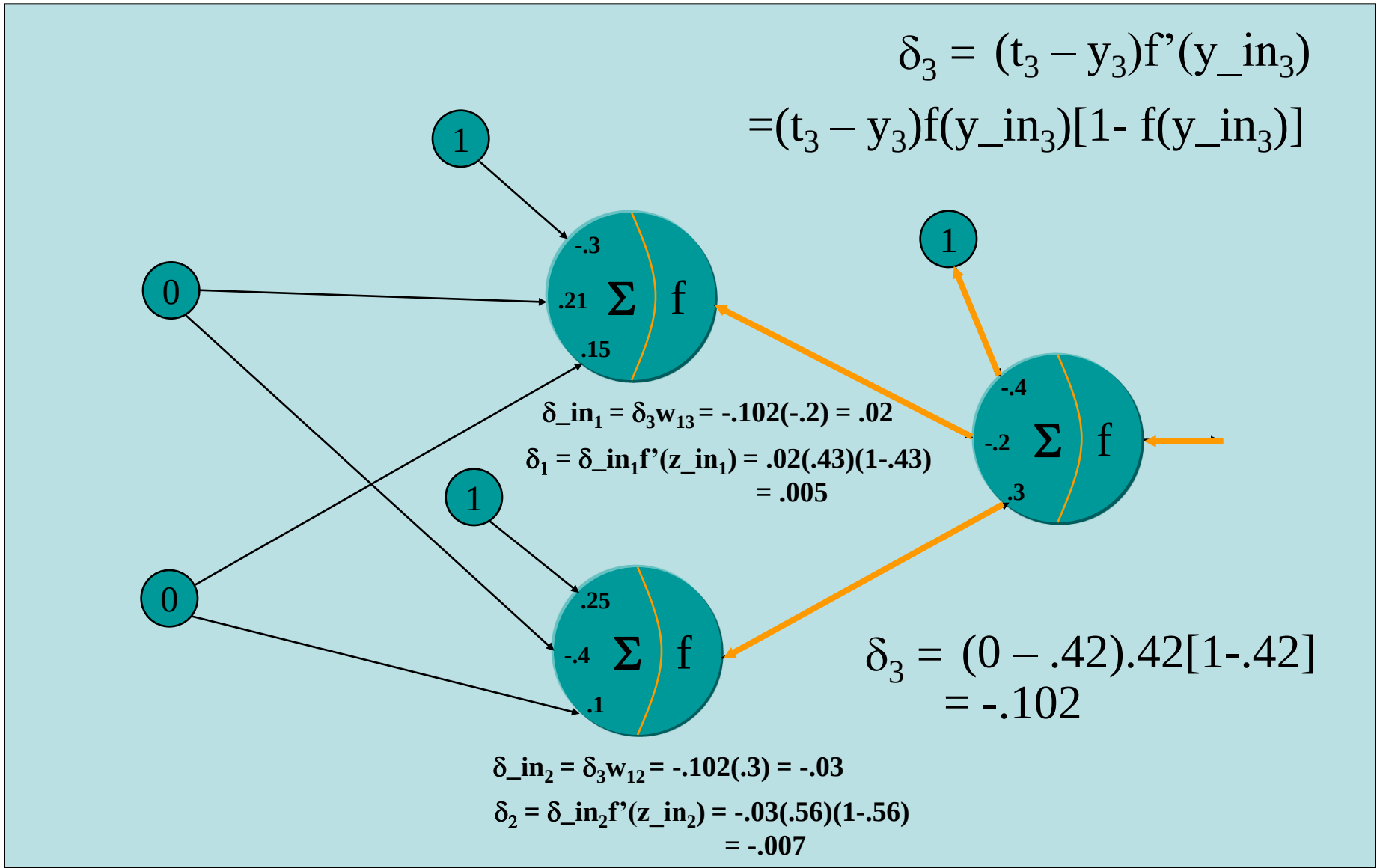
Activation function f:

$$y_j = \frac{1}{1 + e^{s_j}}$$

Backpropagate

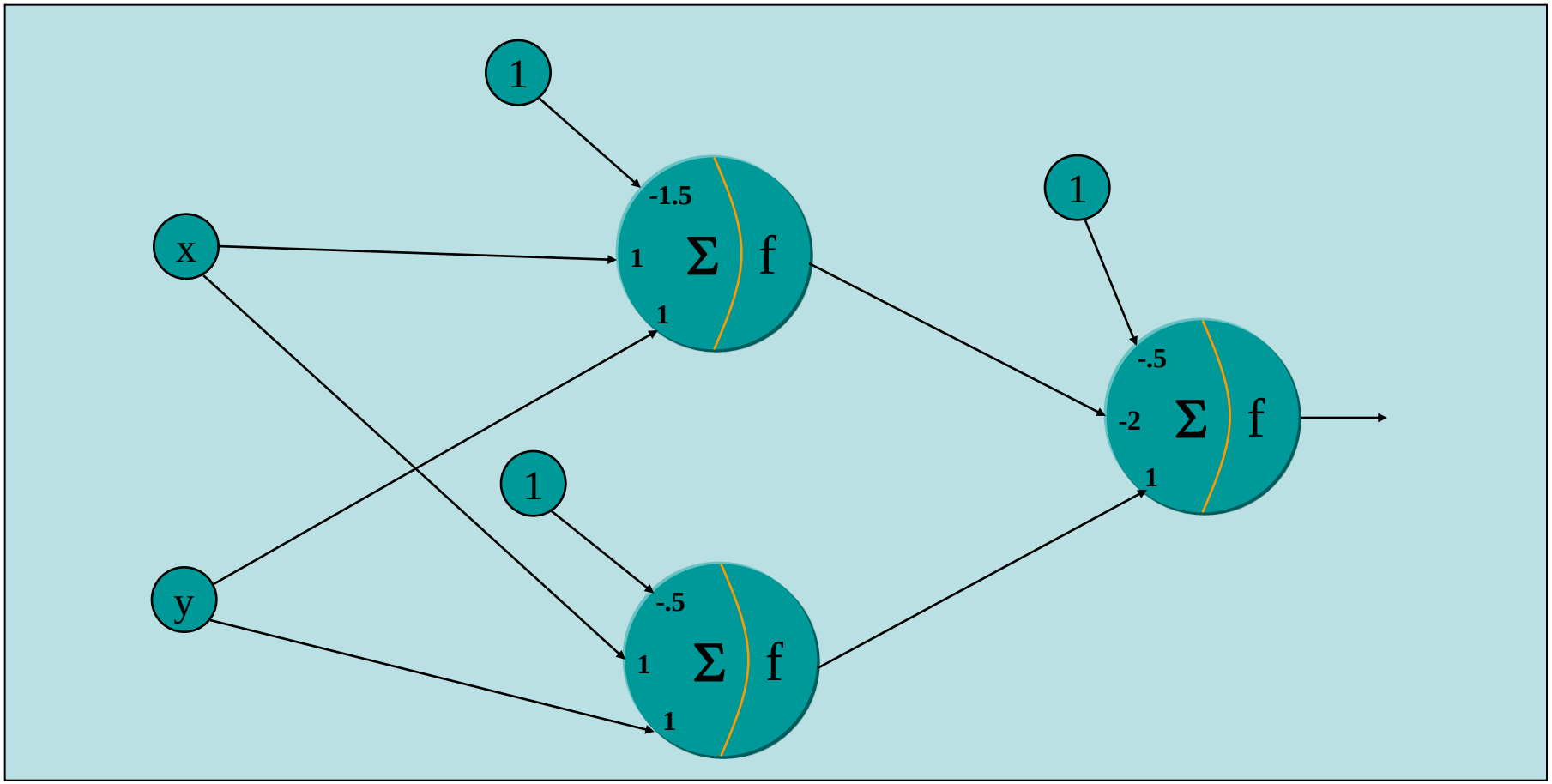


Update the Weights – First Pass



Final Result

- After about 500 iterations:



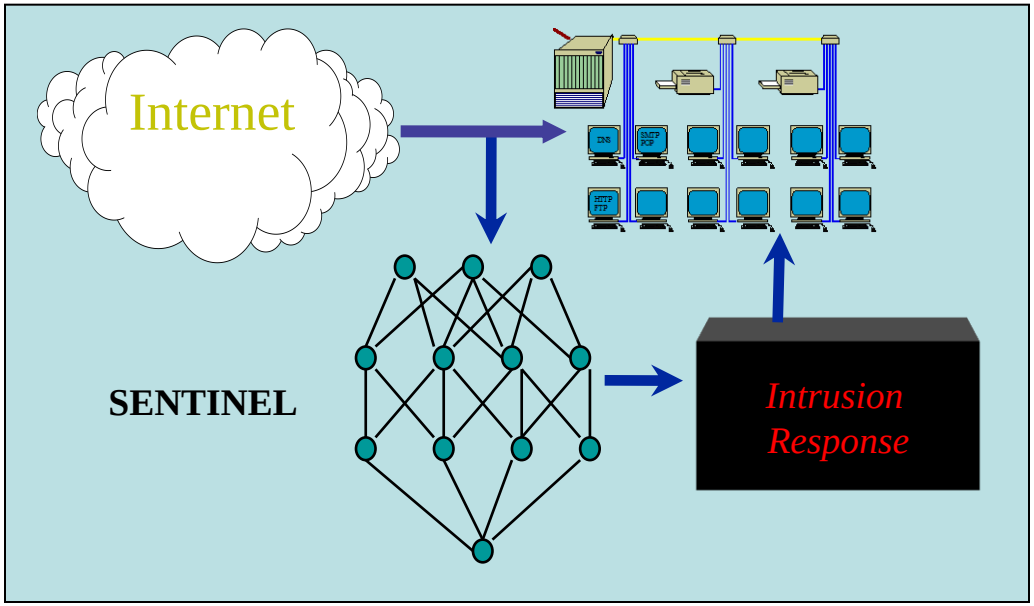
Applications
Intrusion Detection Systems

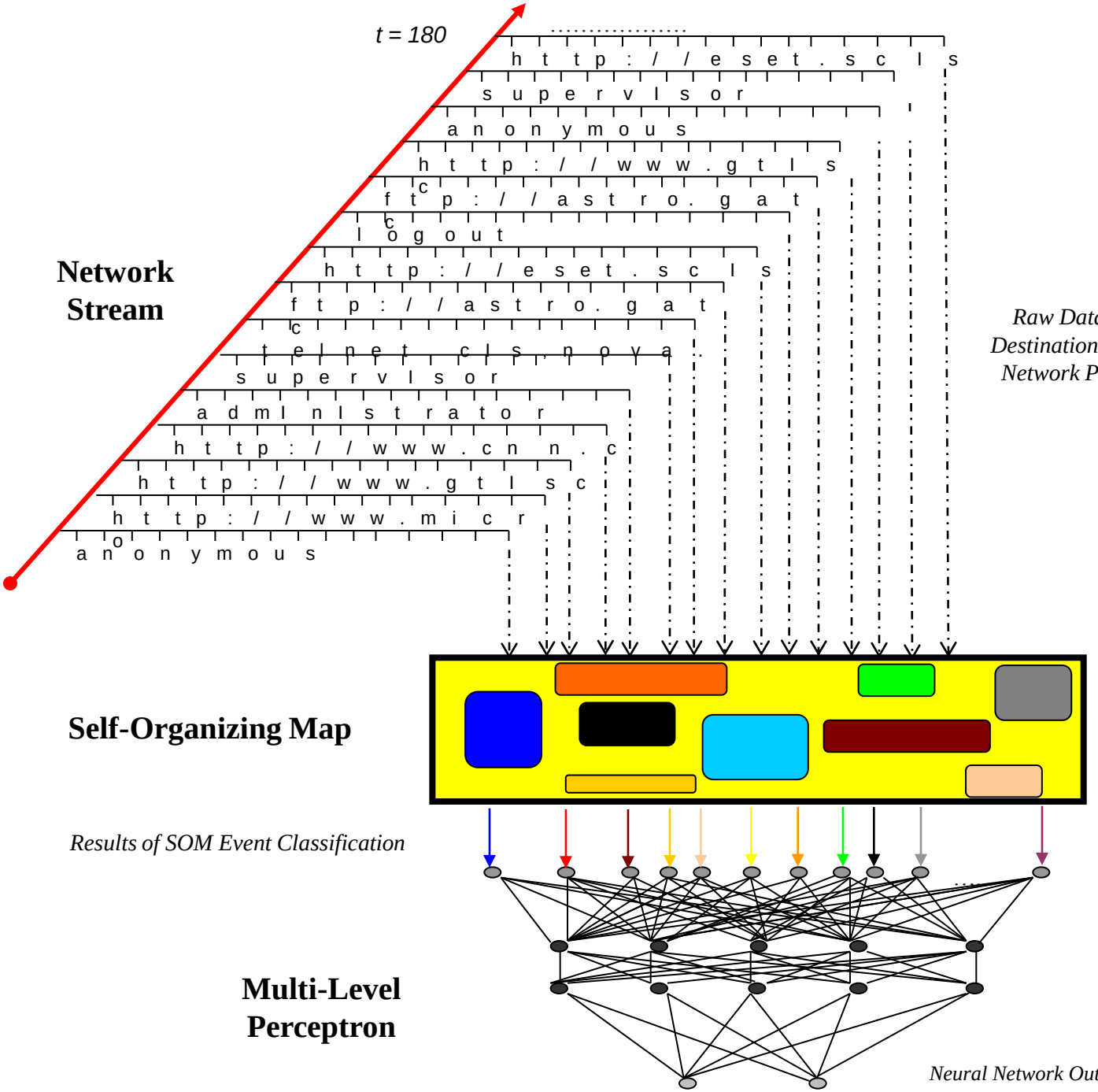
- **Anomaly Detection** - The identification of unauthorized system usage by discovering statistical variances from established norm, (e.g., profiles of authorized users). Primarily used for detecting internal intrusions.

- **Misuse Detection** - The detection of external attacks (“hackers”, etc.). Traditionally addressed by matching current activities to established attacks patterns.

Sentinel

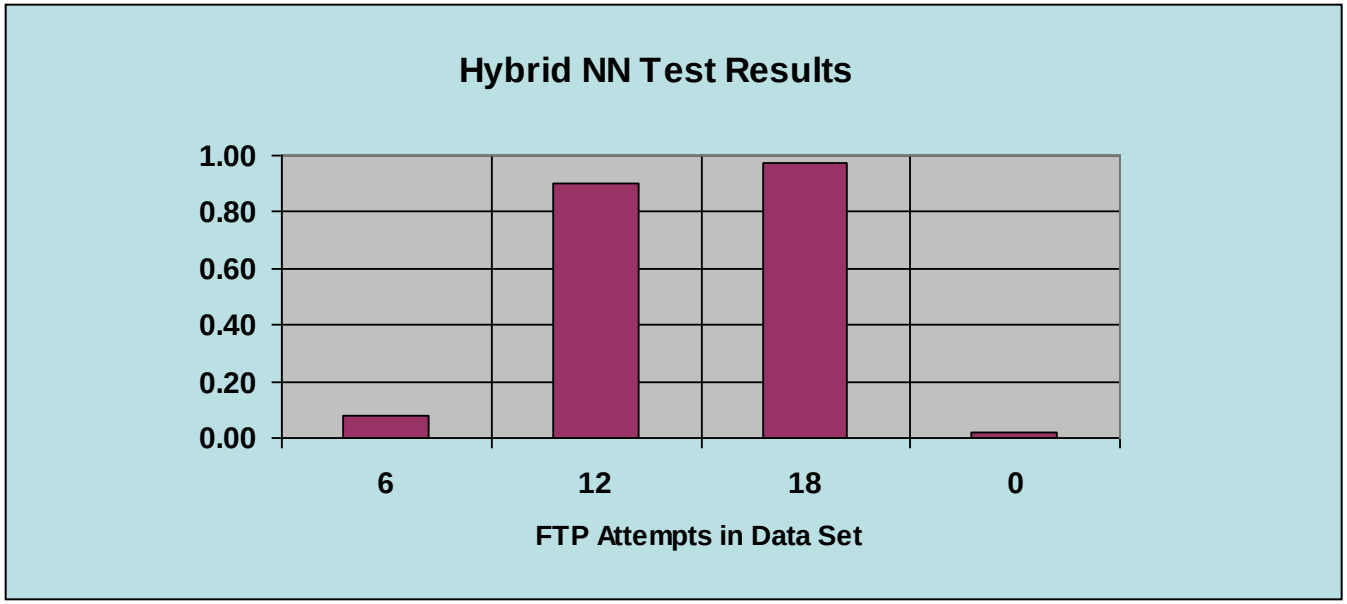
- GOAL: Initial design and development of a neural network-based misuse detection system which explores the use of this technology in the identification of instances of external attacks on a computer network.




t = 180
http://eset.scls
supervisor
anonymous
http://www.gtls
ftp://astro.gat
c
logout
c
http://eset.scls
ftp://astro.gat
c
telnet cls.noya.
supervisor
administrator
http://www.cnn.c
http://www.gtls c
http://www.micr
o
anonymous
Network Stream
Raw Data and Destination Port of Network Packets
Self-Organizing Map
Results of SOM Event Classification
Multi-Level Perceptron
Neural Network Output

Results

- Tested with data sets containing 6, 12, 18, and 0 “attacks” in each 180 event data set
- Successfully detected >= 12 “attacks” in test cases
- Failed to “alert” in lower number of “attacks” (per design)

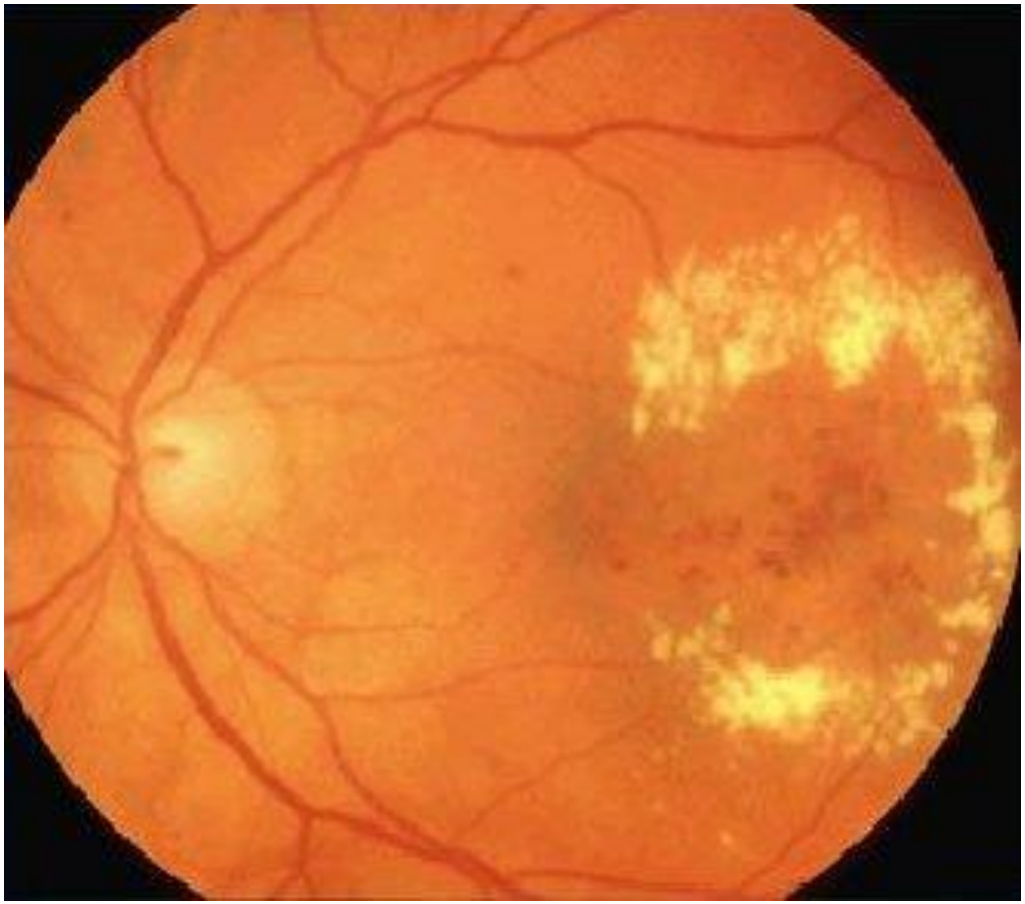


An automatic screening system for Diabetic Retinopathy

- Visual Features:
  - Nerve: Circular yellow and bright area from which vessels emerge
  - Macula: Dark elliptic red area
  - Microaneurysms: Small scattered red and dark spots (in the order of 10x10 pixels in our database of images)
  - Haemorrhages: Larger red blots
  - Cotton spots (exudates): Yellow blots

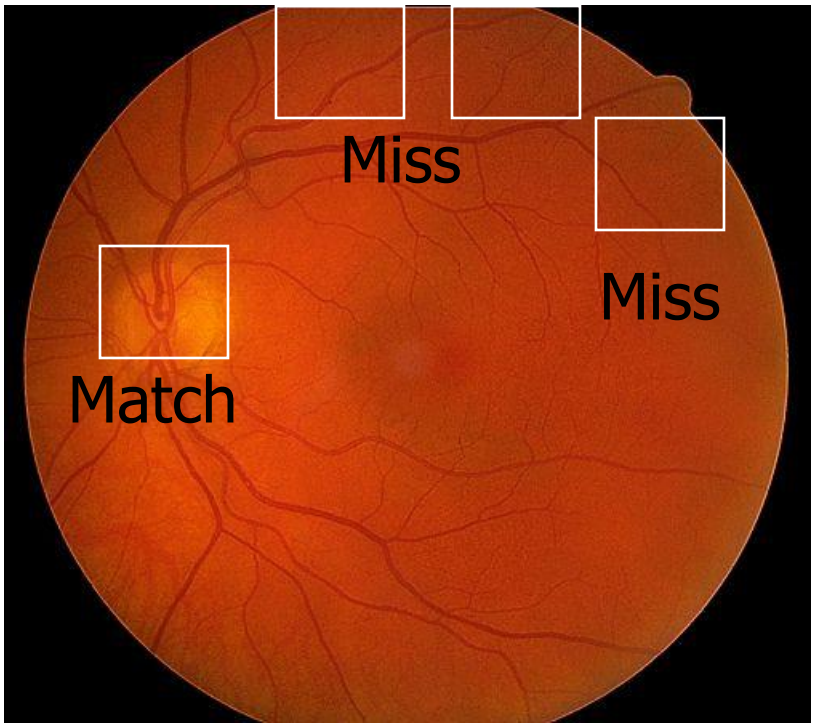
Example

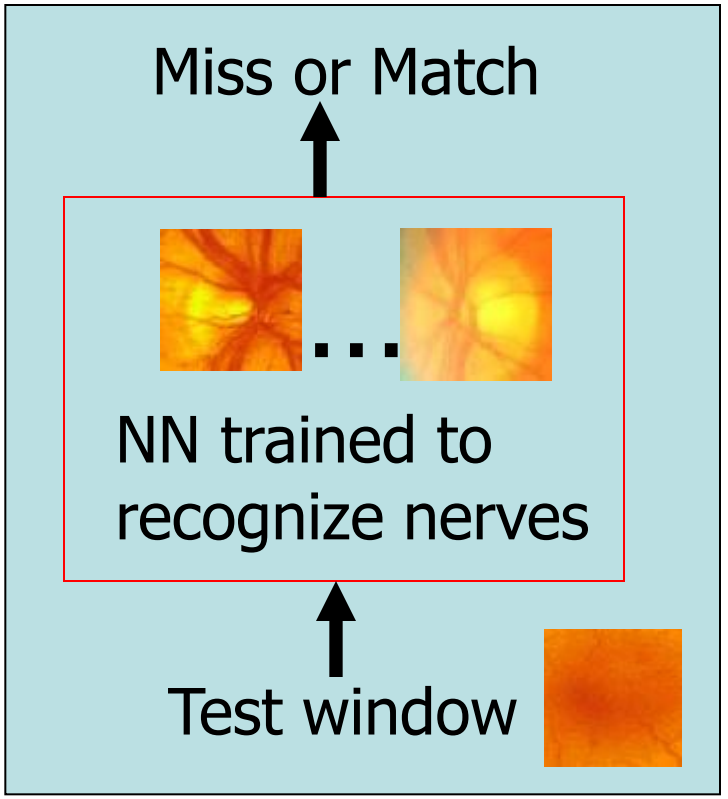
- Cotton Spots:



Approach

- A moving window searches for the matching pattern





Possible Quiz

What can vary in a backpropagation system?

What is misuse detection?

What is backpropagated during training?

SUMMARY

- Backpropagation Training

- Applications
  - IDS
  - Eyes