Intrusion Detection

- Signature based
- **Anomaly based**
- Host based
- **Network based**

Anomaly based Network Intrusion Detection (A-NIDS)

- Statistical based
    - Univariate
    - Multivariate
- Knowledge based
- **Machine learning based**

Exploiting Communication Regularities

- Learn the normal sequences of messages on a network
- Build a model describing these sequences

Machine Learning

- Bayesian networks
- **Markov models**
- Neural networks
- Fuzzy logic
- Genetic algorithm
- Etc.

Hidden Markov Model

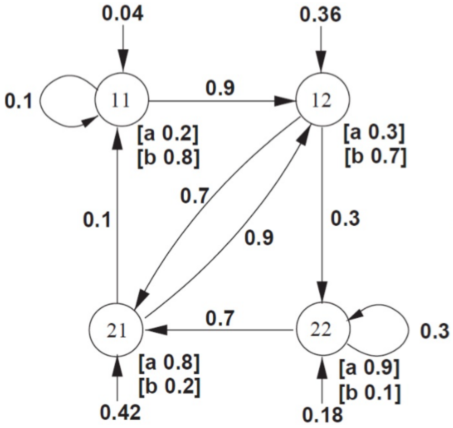


Figure : PAutomaC: a PFA/HMM Learning Competition, Sicco Verwer et al., 2012

Hidden Markov Model - Urn and Ball

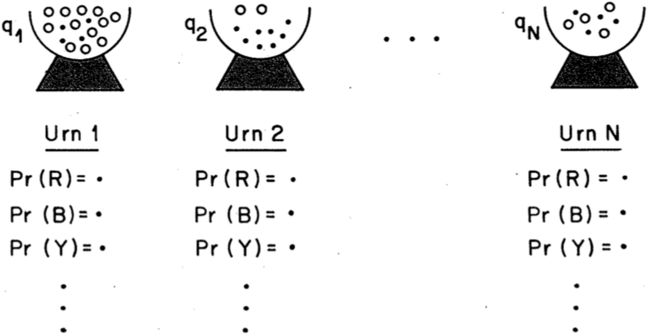
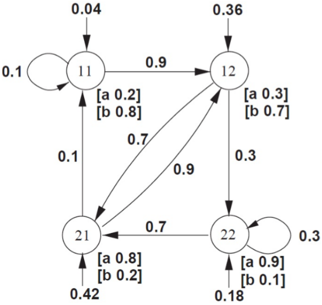


Figure : An Introduction to Hidden Markov Models, L. R. Rabiner B. H. juang, 1986

Hidden Markov Model

- T = length of observation sequence
- N = number of states in the model
- M = number of observation symbols
- $Q = \{q_1, q_2, ..., q_N\}$, states
- $V = \{v_1, v_2, ..., v_M\}$, observation symbols
- $A = \{a_{ij}\}$, $a_{ij} = Pr(q_j \text{ at } t+1 | q_i \text{ at } t)$, state transition probability distribution
- $B = \{b_j(k)\}$, $b_j(k) = Pr(v_k \text{ at } t | q_j \text{ at } t)$, observation symbol probability distribution
- $\pi = \{\pi_i\}$, $\pi_i = Pr(q_i \text{ at } t = 1)$, initial state distribution
- $\lambda = (A, B, \pi)$, the HMM


0.04
0.36
0.1
11
0.9
12
[a 0.2]
[b 0.8]
[a 0.3]
[b 0.7]
0.7
0.1
0.9
0.3
21
0.7
22
0.3
[a 0.8]
[b 0.2]
[a 0.9]
[b 0.1]
0.42
0.18