Privacy-Preserving AIS for Network Security

Karthik S
Chandan Yeshwanth

April 5, 2016

Recap

- Affinity function : privacy-preserving r contiguous bits (R-CONT)
- Tolerization/Maturation of detectors using R-CONT

LISYS Overview

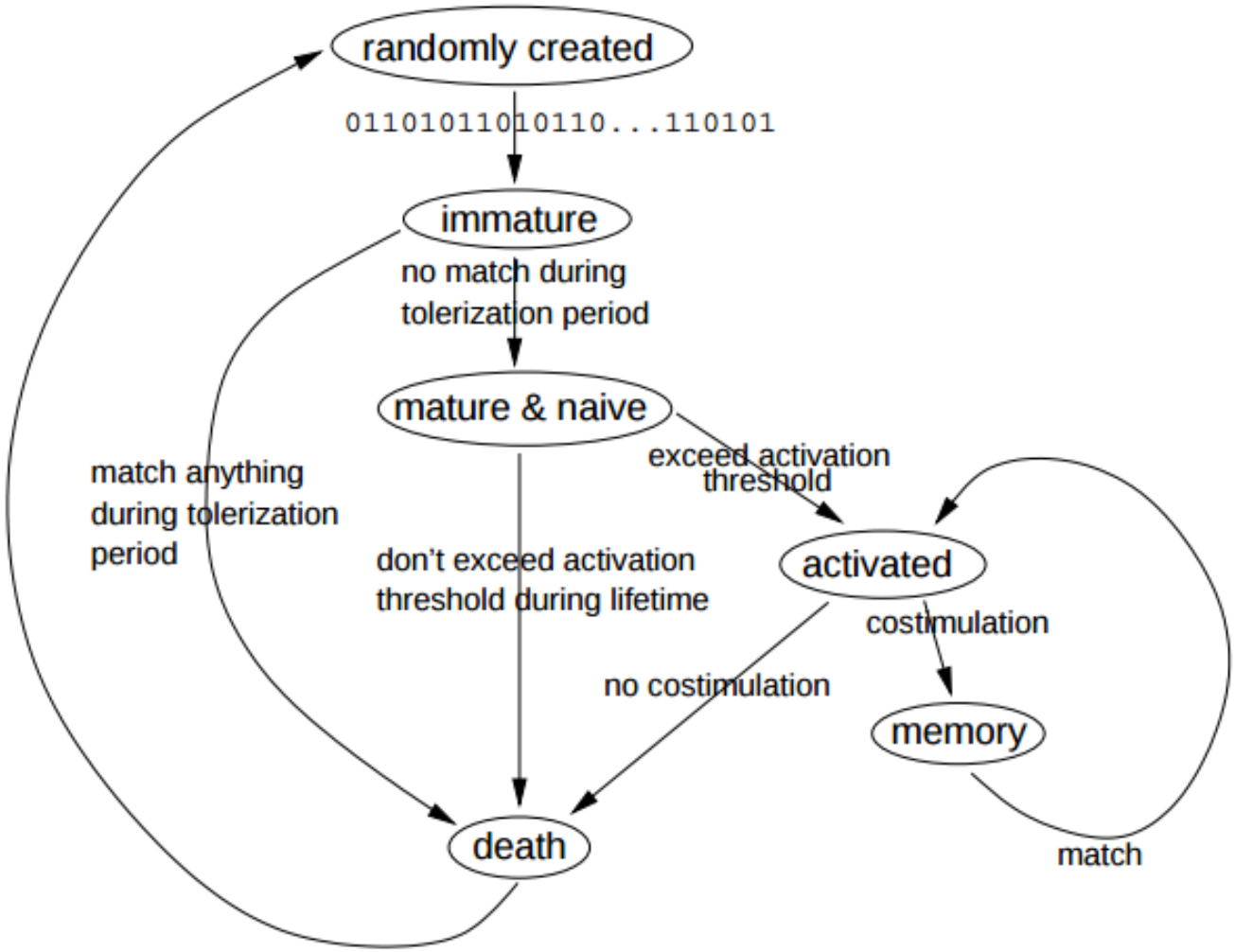

Figure : Detector lifecycle[1]

Intrusion Detection

- For a normal (non-memory) detector, if number of matches is greater than a threshold within a given timeframe, then the following happens:
  - the detector gets added to the memory set
  - any subsequent connections that it matches are classified as intrusive
- For memory detectors, the threshold is 1
- The number of matches of a given detector $d_i$is given by $d_i.matches$

Intrusion detection

Algorithm 4 DETECT$([D], [M], [c], COUNT)$

for $i = 1$ to $|D|$ **do**
  $[u_i] = R - CONT([c], [d_i])$
  $u_i = RECONSTRUCT([u_i])$
  $COUNT[i] += u_i$
  if $COUNT[i] \geq \tau$ **then**
    $[M].add([d_i])$
    return 1
  end if
end for
for $i = 1$ to $|M|$ **do**
  $[u_i] = R - CONT([c], [d_i])$
  $u_i = RECONSTRUCT([u_i])$
  if u_i **then**
    return 1
  end if
end for
return 0

Memory Set

- The detectors are replaced in the memory set using the least-recently-used (LRU) policy
- Detectors that are removed from the memory set are added back to the normal detector set (with threshold τ)
- Memory detector set is stored between sessions

Decay And Death

- The match count for a detector d_i, $COUNT[i]$ decreases by 1 with probability γ_{match} at each timestep
- The probability of a detector dying at a timestep is given by p_{death}
- The detector is replaced by a new one which is subsequently tolerized and added to the detector set
- The dynamic nature of the detector set allows the system to adapt to new threats and self-connections


Steven A Hofmeyr and Stephanie Forrest.
Architecture for an artificial immune system.
Evolutionary computation, 8(4):443–473, 2000.