A Machine Learning Evaluation of an Artificial Immune System

Matthew Glickman, Justin Balthrop and Stephanie Forrest

Presenter: Zheng Dong
zhdong@indiana.edu
Artificial Immune System
Sensor Life Cycles

- Immature
- Mature
- Activated
- Memory
- Death
Life Cycles

Start

Immature

Death

Random regeneration

Match

No activation in finite period

Naive, mature

Exceeds activation threshold

Memory Detector

Activated

Costimulated
• Instance-based ML algorithm

\[ \text{Output Value} = f (\text{example}, D(\text{input}, \text{example})) \]

• Inductive bias
  • the notion of distance
  • how distance is used
  • which training examples are retained

• Negative Detectors
Data Set

- **Data Source**
  - Internal network of a research lab
  - 62 days

- **Normal Data**
  - 415,274 TCP SYN packets
  - roughly 55% of this is web traffic.
  - 6,700 packets/day during normal period

- **Attack Data – 8 attacks**
  - Denial of service, Firewall, FTP
  - SSH
  - TCP SYN scan
  - Two Nmap scans
- Identified attacks that had taken place.
- isolated packets corresponding to each attack.
- reinserted into the normal data stream at well-controlled locations.

![Attack Data Diagram]
- 50 nodes
- own randomly generated substring-hash
- 100 detectors per node
- 120 runs

<table>
<thead>
<tr>
<th>Attack</th>
<th>Total # of attack packets</th>
<th>Fraction of runs in which at least one attack packet was flagged</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>12 (out of 12 total)</td>
<td>1/120</td>
</tr>
<tr>
<td>“Useless Services”</td>
<td>27 (out of 27 total)</td>
<td>99/120</td>
</tr>
<tr>
<td>ssh</td>
<td>56 out of 60 (total)</td>
<td>83/120</td>
</tr>
<tr>
<td>D.O.S.</td>
<td>284 (out of 301 total)</td>
<td>119/120</td>
</tr>
<tr>
<td>ftp</td>
<td>576 (out of 664 total)</td>
<td>109/120</td>
</tr>
</tbody>
</table>

Performance
Adding Activation Thresholds
Adding co-stimulation
False/True Positive
120 Runs
• Extend the empirical evaluation of LISYS’ performance to new and more challenging data sets
• Deepen our understanding of the contributions made by each component of LISYS to its overall performance
• Connect LISYS with the broader context of machine learning
Possible Discussions

- Positive detection possible to achieve such performance?
- False Positive vs. False Negative, which is more important?
- What do you think of the overall performance of LISYS?