CPS: Driving Cyber-Physical Systems to Unsafe Operating Conditions by Timing DoS Attacks on Sensor Signals

Marina Krotofil, Alvaro Cardenas, Bradley Manning, Jason Larsen

Hamburg University of Technology, Germany
University of Texas in Dallas, USA
Autolive GmbH, Germany
IOActive Ltd., USA

30th Annual Computer Security Applications Conference, New Orleans, USA
Cyber-physical systems are IT systems “embedded” in an application in the physical world

Attacker’s goals:
- Get the system in a state desired by the attacker
- Make the system perform actions desired by the attacker
Motivation

- Best Choice Problem
- Experimental results
- Interesting issues
- Conclusion
Typical understanding of SCADA hacking

Breaking into system != breaking the system

Digital Perl Harbor

010011011011101

Missing peace of knowledge
Traditional IT security requirements: confidentiality, integrity, availability

What are the requirements for secure control?

Safety constraint:
- Pressure < 3000kPa

Operational requirement:
- Minimize cost

\[ \text{Cost} = \frac{F_3}{F_4} (2.206y_{A3} + 6.177y_{C3}) \]
DoS attacks are similar to data integrity attack, in which the attacker have control over **start of the attack** and its **duration**.
Impact of 8h long DoS attacks on reactor pressure sensor at random time
Quest for the peak

- REAL TIME decision making problem
- Searching for the “BEST” peak
- Achieving results within some time horizon
Motivation

Best Choice Problem

Experimental results

Interesting issues

Conclusions
Secretary Problem (SP)

- There is only one position available.
- The number of applicants, $N$, is finite and known to the DM.
- The $N$ applicants are interviewed sequentially, one at a time, in a random order.
- The DM can rank all the $N$ applicants from best to worst. The decision to either accept or reject an applicant is based only on the ranks of those applicants interviewed so far.
- Once rejected, an applicant cannot later be recalled - think of dating problem 😊
- The DM is satisfied with nothing but the best.
The max probability to select the best candidate is $\frac{1}{e}$

**Strategy**

- Do not make any offer to first $\frac{N}{e}$ candidates (*learning window*)
- After that select the **first** candidate whose rank exceeds the highest rank in the observation window (*aspiration level*) or the **last candidate**
- For order of candidates which satisfies **hazard rate solution** the learning window can be cut to $\frac{N}{\log(N)}$
Secretary Problem: sensor signal
Use cases: peak detection and heuristics

**SP Enhancement: Peak detection**

- Forward looking search
- Non-parametric CUSUM (change detection)

\[ S_i^+ = \max(0, |X_{i-1} - X_i| + S_{i-1}^+) \]
\[ S_i^- = \max(0, |X_i - X_{i-1}| + S_{i-1}^-) \]

**SP alternative: Heuristics**

- Normal distribution: \( \mu \) and \( \sigma \)
- Outlier detection (Outlier Test - OT)
Evaluation metrics

- **Shutdown time (SDT)** == Safety time
- **Error** in selecting the highest/lowest value in time series, in %
- Number of **non-selections** (NS) - last sample is taken

- **Time to select (TTS)**
- **Time to attack (TTA)**
Motivation

Best Choice Problem

Experimental results

Interesting issues

Conclusion
Simulation testbed

Tennessee Eastman (TE) test process
TE: types of sensor signals

A feed

Reactor pressure

A and C feed

D feed

Raw signal
Smoothed signal
Simulation results: risk assessment

- Unfeasible optimum (attack at best peak)
- Risk assessment based on the sensitivity of control loops
- Secretary problem delivers superior results among approaches

<table>
<thead>
<tr>
<th>XMEAS</th>
<th>Variable name</th>
<th>Optimum SDT,h</th>
<th>Secretary, n/e SDT,h</th>
<th>Secretary, n/log(n) SDT,h</th>
<th>Outlier Test, σ = 2.0 SDT,h</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>A-feed rate</td>
<td>22.22</td>
<td>13.96</td>
<td>40</td>
<td>42.85</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>18.74</td>
</tr>
<tr>
<td>(2)</td>
<td>D-feed rate</td>
<td>5.15</td>
<td>8.52</td>
<td>26</td>
<td>19.57</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>42.93</td>
</tr>
<tr>
<td>(3)</td>
<td>E-feed rate</td>
<td>4.29</td>
<td>8.13</td>
<td>38</td>
<td>17.65</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>44.87</td>
</tr>
<tr>
<td>(4)</td>
<td>C-feed rate</td>
<td>1.05</td>
<td>12.44</td>
<td>34</td>
<td>35.80</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>29.15</td>
</tr>
<tr>
<td>(5)</td>
<td>Recycle flow</td>
<td>4.39</td>
<td>17.12</td>
<td>32</td>
<td>39.17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>28.92</td>
</tr>
<tr>
<td>(7)</td>
<td>Reactor pressure</td>
<td>8.56</td>
<td>23.41</td>
<td>34</td>
<td>39.20</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>25.93</td>
</tr>
<tr>
<td>(8)</td>
<td>Reactor level</td>
<td>2.37</td>
<td>14.57</td>
<td>34</td>
<td>30.05</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>44.98</td>
</tr>
<tr>
<td>(9)</td>
<td>Reactor temper.</td>
<td>1.34</td>
<td>4.06</td>
<td>30</td>
<td>13.54</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>45.25</td>
</tr>
</tbody>
</table>

Note: Filled cells indicate key results.
Results: peak detection

Type 1

Secretary

Forward looking search

CUSUM

Type 3

Secretary

Forward looking search

CUSUM

Type 1: Hours vs. Number of Simulations

Type 2: Type 2: Hours vs. Number of Simulations

Type 3: Hours vs. Number of Simulations
Motivation

Best Choice Problem

Experimental Results

Interesting issues

Conclusion
Use case: detection of plant state change

- Step change in the reactant A feed
- Need to “re-learn” aspiration value
- Use CUSUM algorithm to detect changes in plant state
Use case: chaining attacks

- Chain two DoS attacks
- Attack on $F_{sep}$ (flow)
- After 30 min the separator level $L_{sep}$ reaches 30%
- Use CUSUM to detect change
  - SDT in **3.43 h** in comparison to **12.03 h** in case of direct attack
Success parameter: sampling frequency

- Sampling frequency changes noise profile
- Lower sampling frequency -> longer SDT

- Important knowledge to attacker to plan concealing activities
Motivation

Best Choice Problem

Experimental Results

Interesting issues

Conclusion
Good control vs. good crypto

- Security specialists define required security protections
  - Signatures for authentication and integrity protection
  - Encryption for confidentiality

- Mathematicians do their magic and come up with strong cryptographic primitives and algorithms

- It is no different with secure controls
  - Specify the problem and a desired outcome
  - Let control guys do what they do best
Thank you