Is it a good time?
Deciding when to Launch Attacks on Process Control Systems

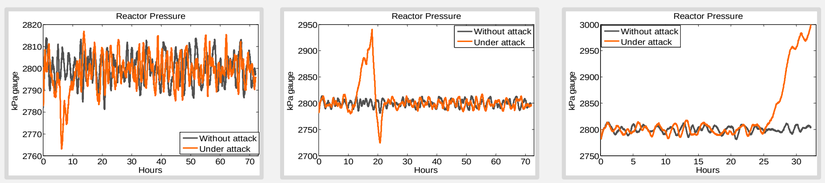
Marina Krotofil†, Álvaro Cárdenas‡

†Hamburg University of Technology, Germany

‡University of Texas at Dallas, USA

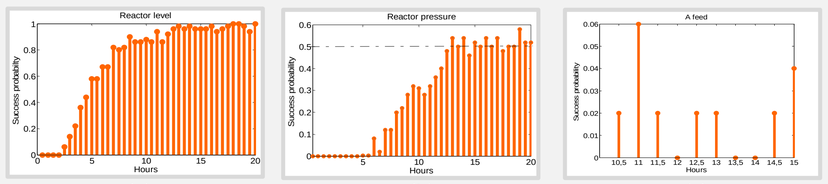
MOTIVATION

We consider an adversary whose goal is to force a plant into an unsafe state causing its shutdown. An attacker can read sensor signals for a given process variable (PV), and then launches a DoS attack on the communication channel which will freeze certain PV in the controller's memory [3] depending on the time of attack. As a result, the controller will select control commands based on a value that is not being updated.



(a) (b) (c)

- If the timing of a DoS attack is not chosen correctly, the attack has limited impact (a) or terminates as a near miss (b). But if chosen carefully, the attack has higher chance to succeed (c).
- The attacker faces a real-time decision problem to select the optimal time to attack. She also wants to achieve the result as soon as possible to avoid detection and operator's response.



(a) (b) (c)

- Evaluation of the effectiveness of the DoS attack at a random time demonstrates that it would take the attacker a long time to achieve her goal reliably (a). In certain cases without strategic decision making it is not even possible to achieve process shutdown (b,c).

SECRETARY PROBLEM

- There is only **one** position available.
- The number of applicants, ***N*, is finite** and known to the decision maker (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 without ties. The decision to either accept or reject an applicant is **based only on the ranks of those applicants interviewed so far**.
- Once rejected, an **an applicant cannot later be recalled.**
- The DM is satisfied with nothing but the **best**.

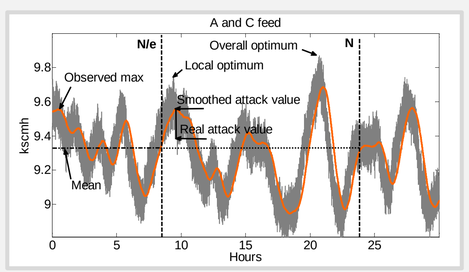
- The max probability to select the best candidate is ***1/e*** [2].

STRATEGY

- Do not make any offer to first ***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 condition** the learning window can be cut to ***N/log(N)*** [4].

EXPERIMENTAL APPROACH

- With the beginning of the attack period *N*, the assaulter starts smoothing the signal and conducts the selection process in real time. She sets the aspiration level (reference value) based on the greatest value of the smoothed signal observed in the learning period *N/e*.
- Upon completion of the learning phase the attacker sequentially inspects every sample of the smoothed signal until she finds a sample whose value exceeds the reference value. After that, she applies forward looking analysis. In particular, the adversary incorporates expectations about upward trend of the physical phenomena into her decision process.



The choice between stopping at the current sample or continuing to search is determined not only by the aspiration value but also by the difference between the stopping value and the continuation value. An alternative approach is to use the theory of quickest change detection based on CUmulative SUM or CUSUM test (future work).

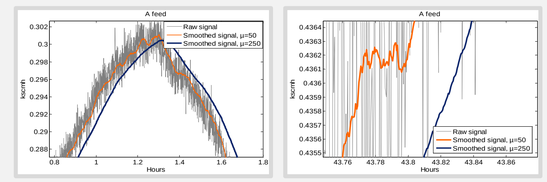
We evaluate the performance of our approach based on following metrics:

- Fractional error in identifying the peak, in %.
- Fractional error in selecting the highest value in a time series, in %.
- Number of non-selections (last sample is selected).

PROBLEM DESCRIPTION

- The shortest shutdown time (SDT) is achieved when striking at the signal peak – high or low (Table 1)*.
- During the assault, the adversary is presented with a time-series of sensor signal samples which exhibit a sequence of peaks. How should the attacker select one of peaks to launch her attack? We formulate the challenge as the Optimal Stopping Problem. In particular we use the Best Choice Problem (also „Secretary Problem") solution to identify optimal stopping criterion.

Because Secretary Problem theory assumes non-correlated time measurements, the attacker has to add an additional stopping criteria to identify when the sensor signal has reached its peak. As sensor measurements tend to be noisy and have sudden fluctuations we use a low-pass filter in form of signal smoothing (μ – smoothing parameter) to remove short-term fluctuations (a). Apart, we use additional condition to account for remaining noise on the slope of the ascending signal trend (b).

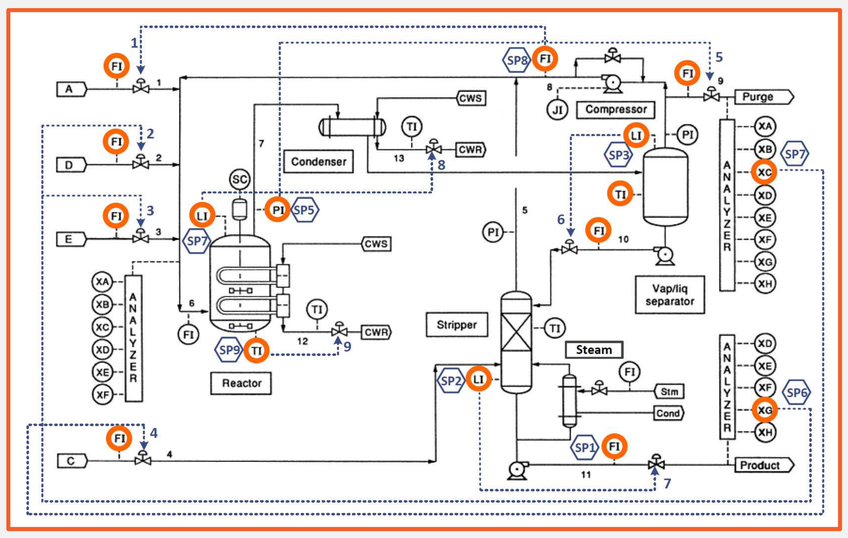


(a) (b)

*The plant is resilient to certain instances of DoS attacks. Hence the attacker might not succeed even if striking at signal pick.

Table 1: Simulation results for shortest shutdown time for TE plant.

XMEAS	Variable name	Units	Min Max	SDT(h)	Conf. Interval(95%)
(1)	A-feed	kscmh	0.0487 0.7466	12.12 -	(4.919;19.31) -
(2)	D-feed	kgh^{-1}	3556 3750	3.840 3.489	(3.641;4.040) (3.387;3.590)
(3)	E-feed	kgh^{-1}	4322 4553	4.120 2.672	(3.916;4.427) (2.517;2.879)
(4)	C-feed	kscmh	8.524 9.825	0.284 0.920	(0.263;0.305) (0.826;1.026)
(7)	Reactor pressure	kPa	2771 2829	8.3 -	(7.811;8.638) -
(8)	Reactor level	%	60.73 68.27	1.877 2.363	(1.778;1.976) (2.100;2.482)



Tennessee Eastman (TE) test process [1] under control based on [5].

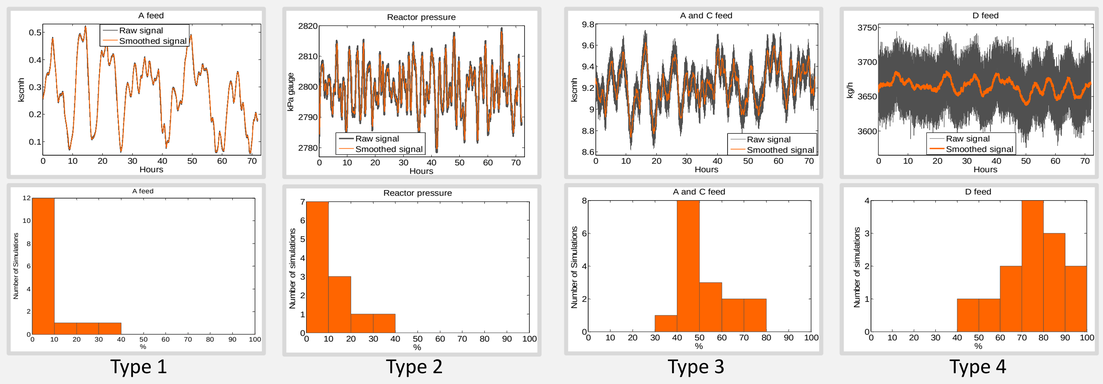
Table 2: Simulation results for Secretary Problem solution for XMEAS1.

N/e	N/log(N)
μ =50	
• 0.62 (0.25; 0.28) • 35.78 (20.36;51.2) • 6 (98.46)	• 0.84 (0.58;1.09) • 66.16 (50.76;81.55) • 0
μ =150	
• 0.84 (0.55;1.14) • 22.47 (9.73;35.2) • 5 (35.39)	• 1.00 (0.52;1.47) • 33.6 (18.77;48.42) • 0
μ =250	
• 0.80 (0.22;1.38) • 6.33 (0.18;12.49) • 7 (90.38)	• 0.78 (0.43;1.12) • 28.33 (13.42;43.25) • 0

RESULTS

In TE plant sensor signals can be roughly divided into 4 types. Type 1 is characterized by few distinct peaks and a low noise level. Type 2 is distinguished by multiple noisy signal peaks. Type 3 can be described as a very noisy variation of Type 2 signal. Type 4 signal exhibits a slow signal amplitude change with high amplitude noise.

- Experimental results show that to succeed, the attacker has to take into account type of the signal she is dealing with. The histograms of the distribution of the fractional error in selecting the highest possible value in the time series shows that our approach is not well suited for conduction attacks on noisy signals.



Type 1 Type 2 Type 3 Type 4

- Further, our results confirm that the learning period can be indeed cut down to *N/log(N)* while achieving results comparable to the *N/e* strategy. Because of the learning phase being short, the number of non-selections is reduced substantially (almost to zero). For the same reason the fractional error in selecting the highest possible peak increases as the attacker has less time to achieve sufficient aspiration level (Table 2).

[1] J. J. Downs and E. F. Vogel. A plant-wide industrial process control problem. Computers & Chemical Engineering, 17(3):245-255, 1993.

[2] P. Freeman. The secretary problem and its extensions: A review. International Statistical Review/RevueInternationale de Statistique, pp. 189-206, 1983.

[3] M. Krotofil and A. A. Cárdenas. Resilience of Process Control Systems to Cyber-Physical Attacks. In NordSec'14, Secure IT-Systems, vol. 8208 of LNCS, pp. 166-182, 2013.

[4] M. Mahdian, R. P. McAfee, and D. Pennock. The secretary problem with a hazard rate condition. In nternet and Network Economics, pp. 708-715. 2008.

[5] N. L. Ricker. Tennessee Eastman Challenge Archive. http://depts.washington.edu/control/LARRY/TE/download.html. retrieved: May, 2013.