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

Marina Krotofil, Alvaro Cardenas, Bradley Manning, Jason Larsen

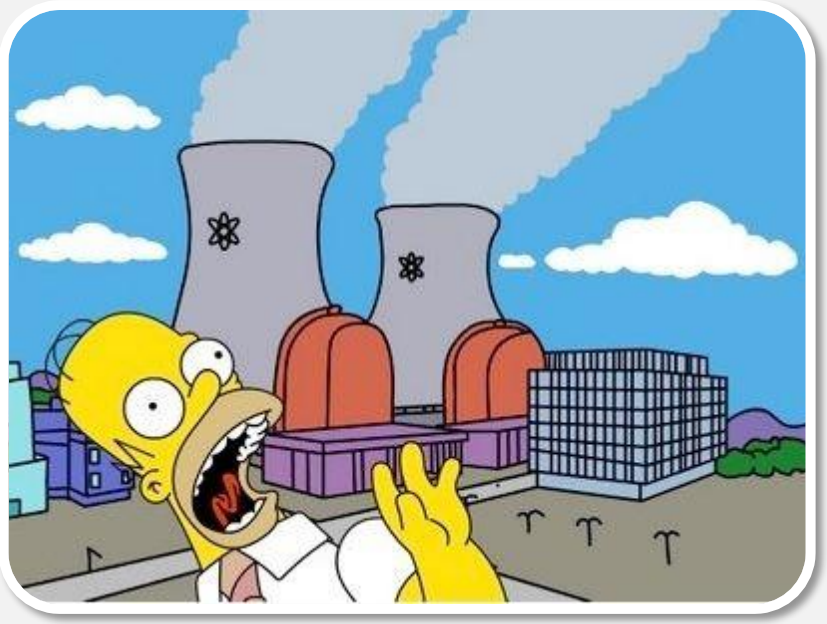
Hamburg University of Technology, Germany
University of Texas in Dallas, USA
Autolive GmbH, Germany
IOActive Ltd., USA

30th Annual Computer Security Applications Conference, New Orleans, USA **11.12.14**

Cyber-physical security

- **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

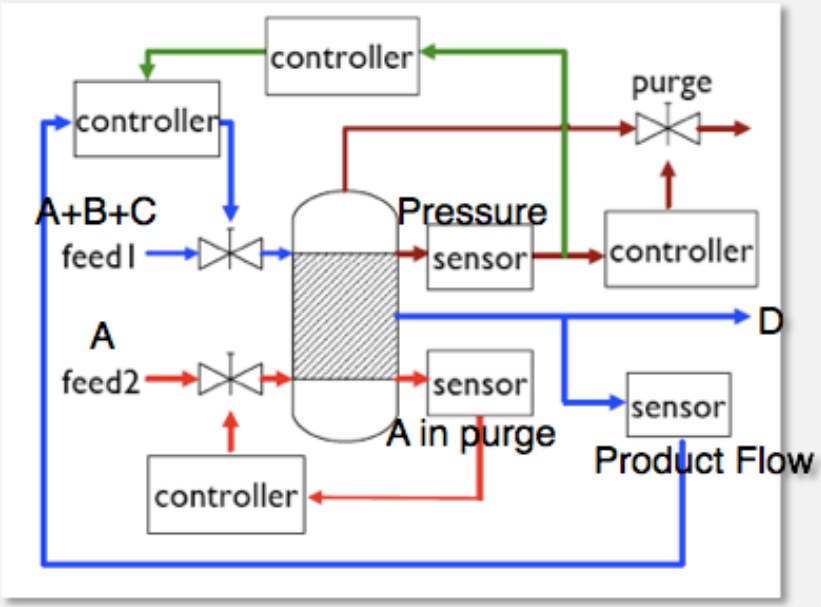
Digital Perl Harbor

010011011011101

Missing peace of knowledge

Secure control

- Traditional IT security requirements: confidentiality, integrity, availability
- What are the requirements for secure control?

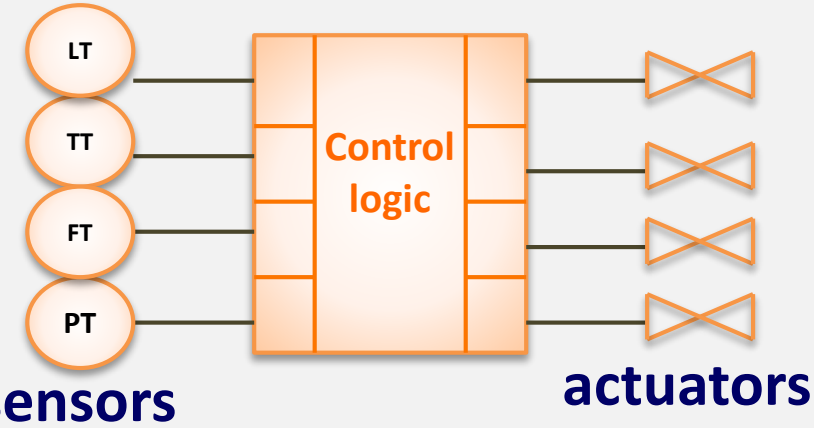


- **Safety constraint:**
  - Pressure < 3000kPa

- **Operational requirement:**
  - Minimize cost

$$\text{Cost} = \frac{F_3}{F_4}(2.206_{yA3} + 6.177_{yC3})$$

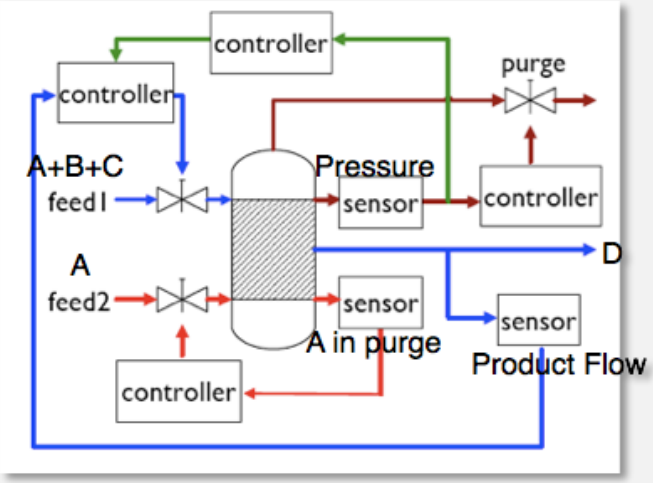
Stale Data attack

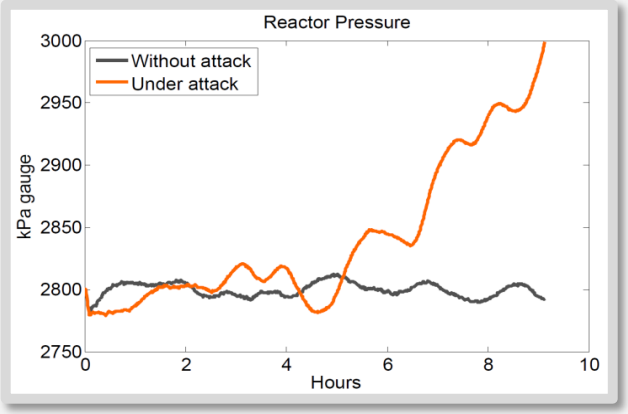


43	45	47	45	43	43	44	43	43
90	89	88	91	91	90	89	90	91
13	15	17	15	13	13	14	13	13
17	15	12	**15**	12	12	12	12	12

Attack time

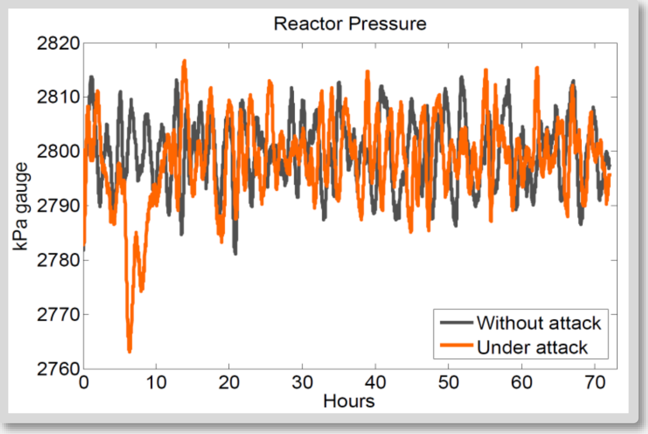
Attack duration

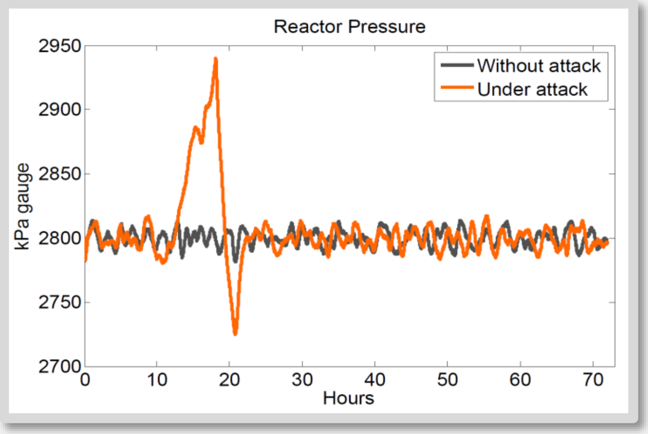


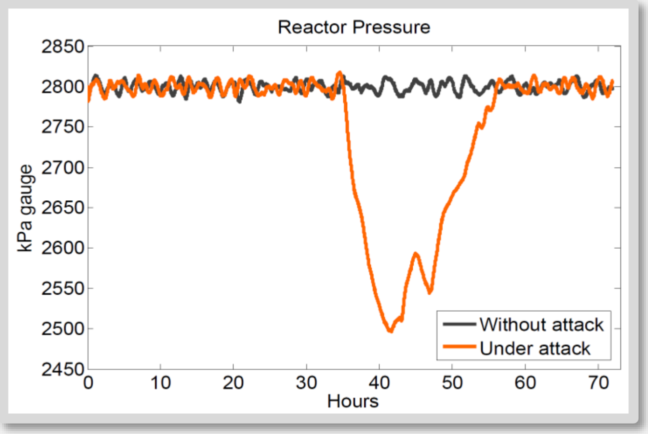


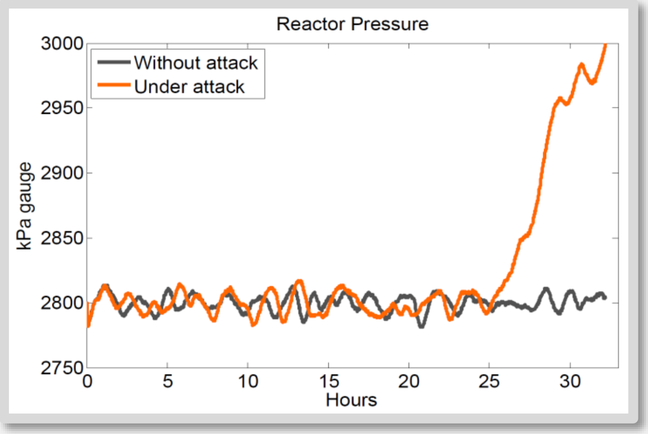
- DoS attacks are similar to data integrity attack, in which the attacker have control over **start of the attack** and its **duration**

Timing of the DoS attack



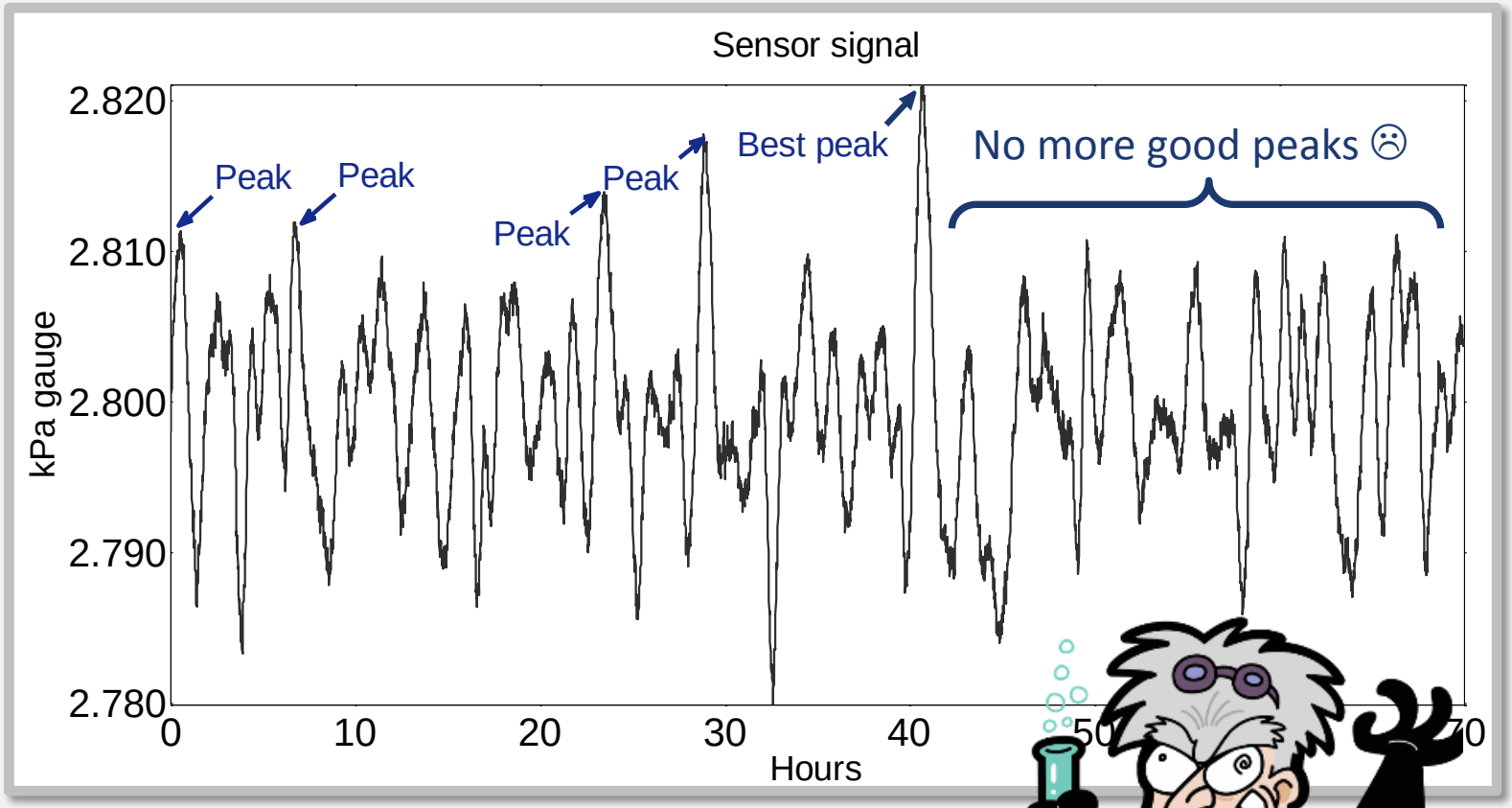






- Impact of 8h long DoS attacks on reactor pressure sensor at random time

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 an applicant cannot later be recalled - think of dating problem ☺**
- The DM is satisfied with nothing but the **best**.

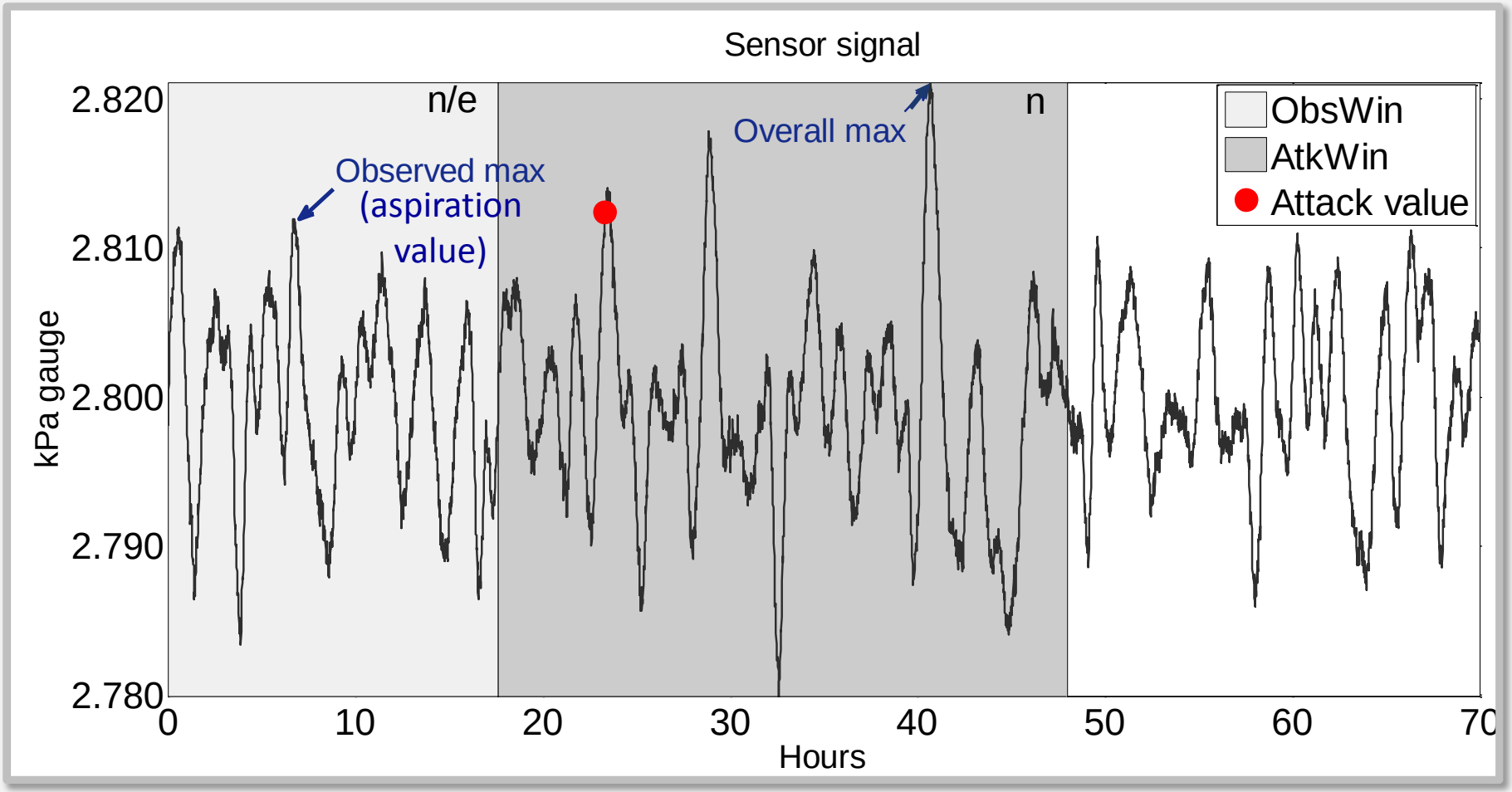
Secretary Problem: solution

- The max probability to select the best candidate is **1/e**

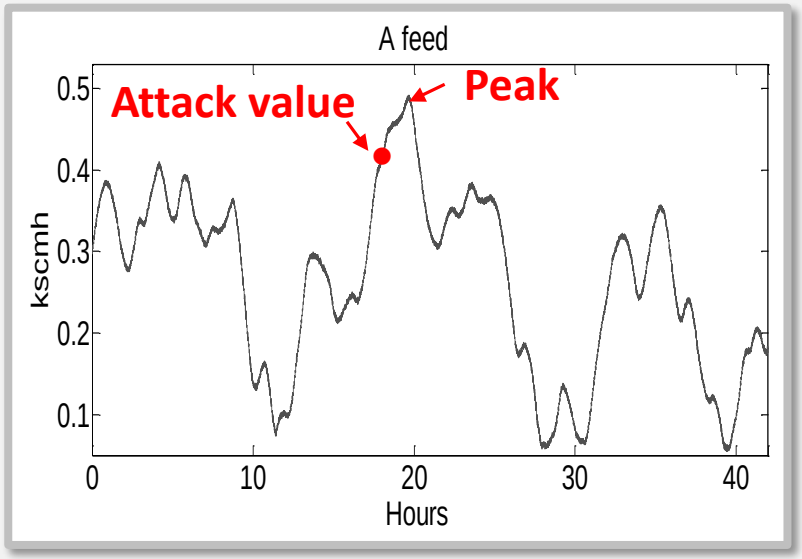
Strategy

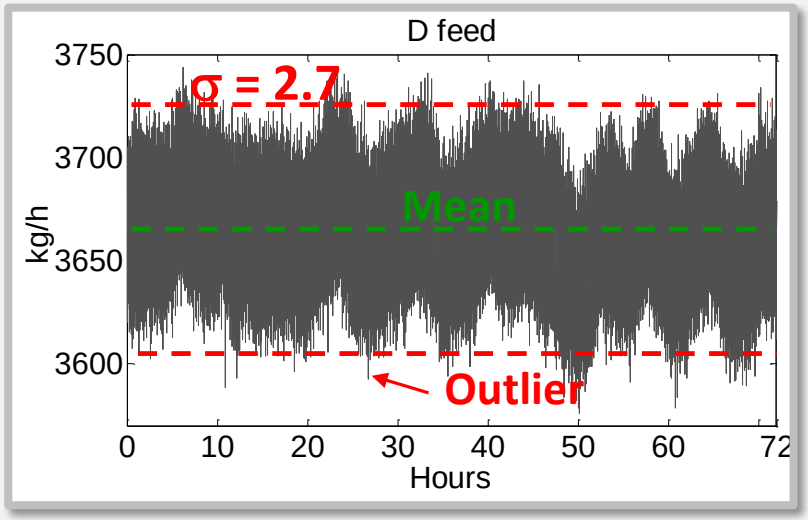
- Do not make any offer to first **N/e** candidates **(learning window)**
- After that select the **first** candidate whose rank exceeds the highest rank in the observation window **(aspiration level)** or the **last candidate**
- For order of candidates which satisfies **hazard rate solution** the learning window can be cut to **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)

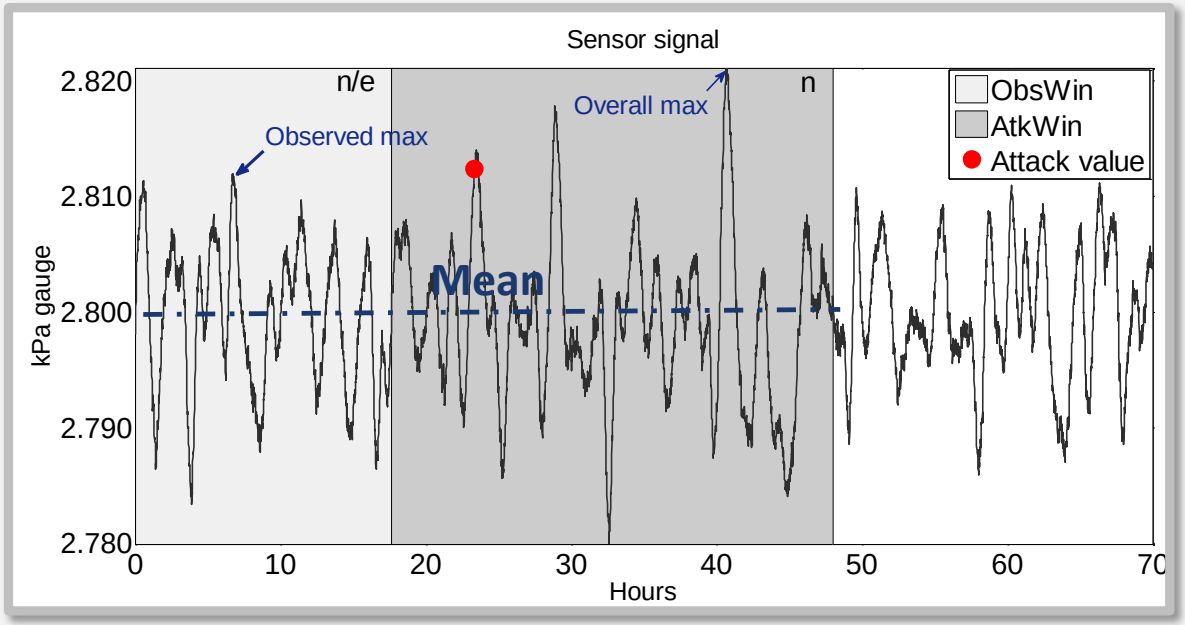
$$S_i^+ = \max(0, |X_{i-1} - X_i| + S_{i-1}^+)$$
$$S_i^- = \max(0, |X_i - X_{i-1}| + S_{i-1}^-)$$

SP alternative: Heuristics

- Normal distribution: **μ** and **σ**
- 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

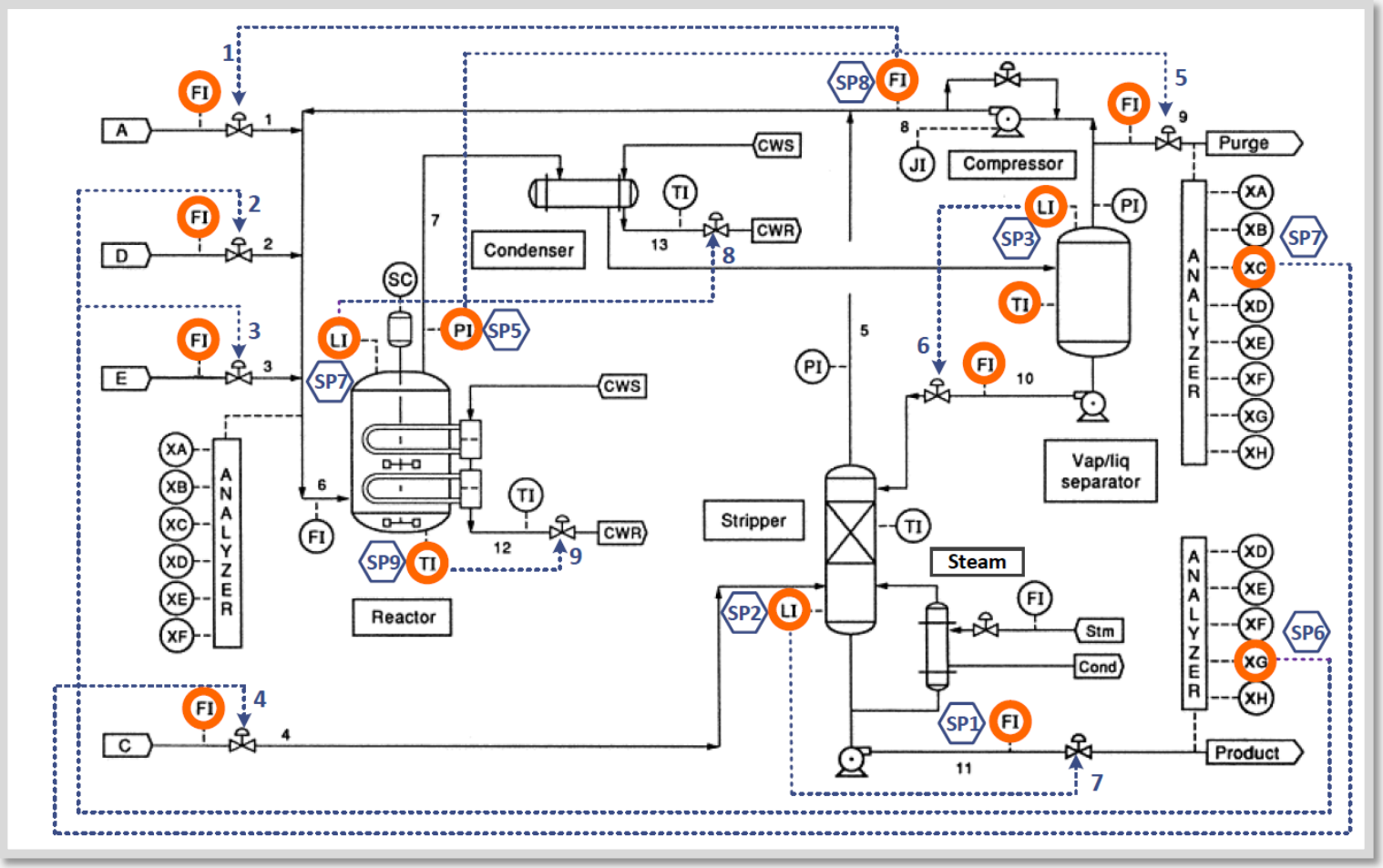


- Time to select (TTS)
- Time to attack (TTA)

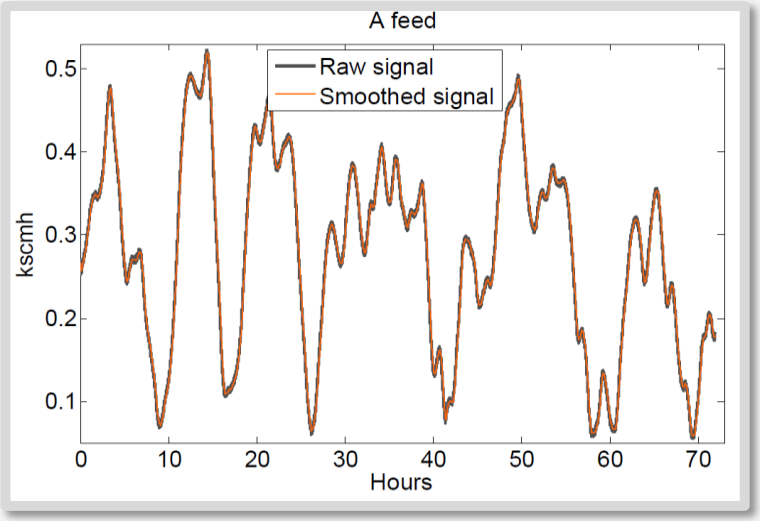
- Motivation
- Best Choice Problem
- **Experimental results**
- Interesting issues
- Conclusion

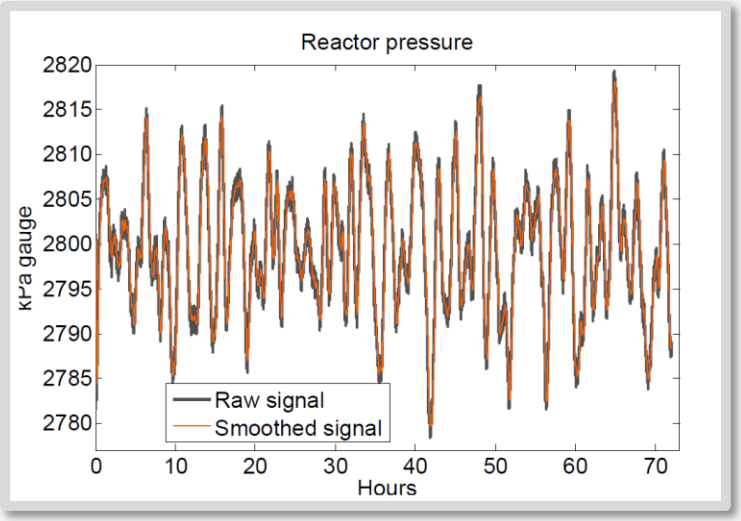
Simulation testbed

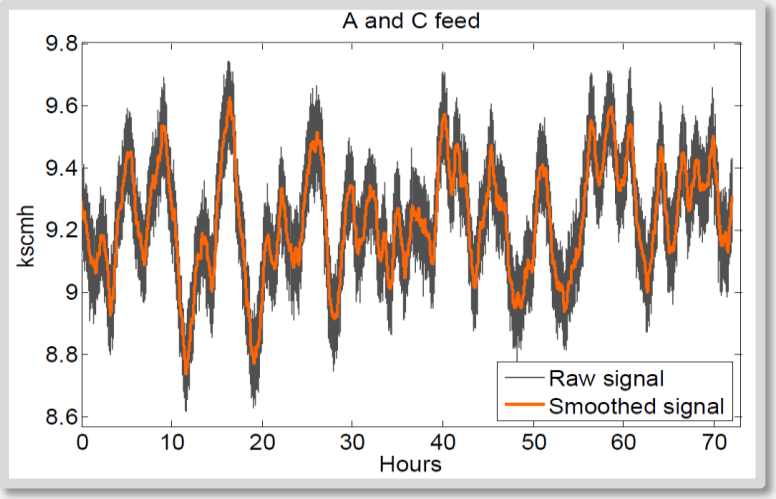
Tennessee Eastman (TE) test process

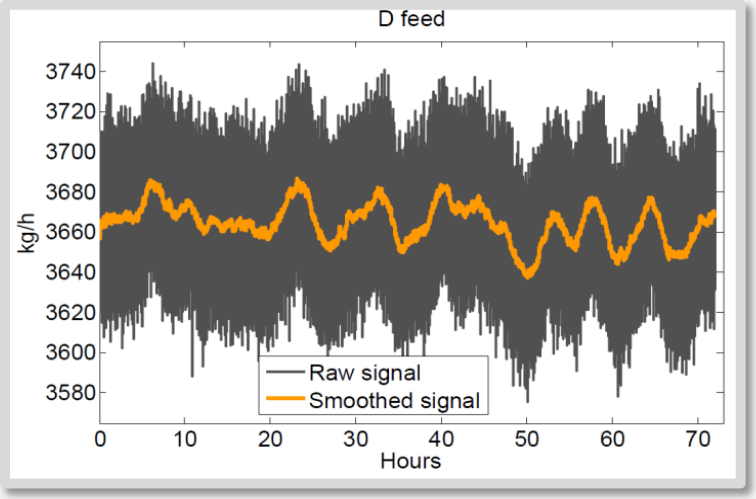


TE: types of sensor signals







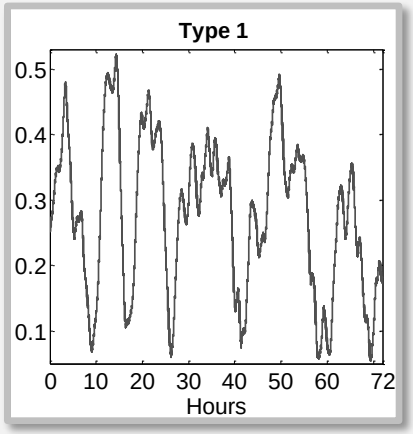


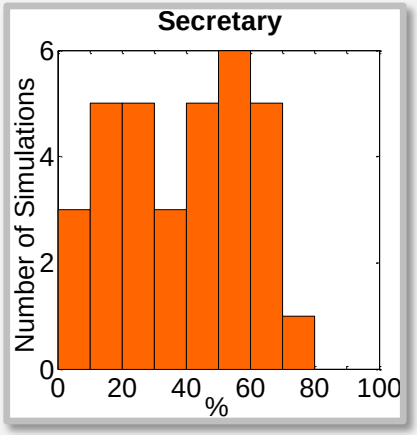
Simulation results: risk assessment

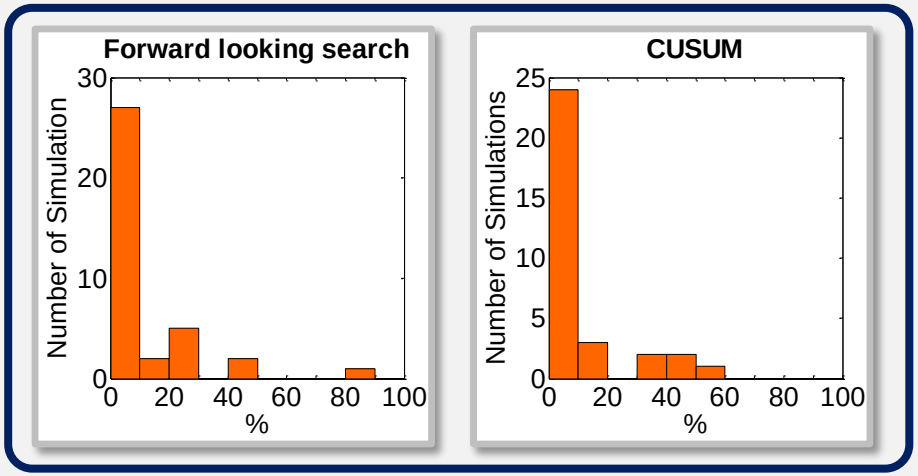
XMEAS		Variable name	Optimum	Secretary, n/e			Secretary, n/log(n)			Outlier Test, $\sigma = 2.0$		
			SDT,h	SDT,h	Error,%	NS,%	SDT,h	Error,%	NS,%	SDT,h	Error,%	NS,%
(1)	min	A-feed	22.22	-	13.96	40	-	42.85	12	-	18.74	70
	max	rate										
(2)	min	D-feed	5.15	5.93	8.52	26	6.05	19.57	0	6.72	42.93	0
	max	rate	3.69	3.85	6.38	20	4.27	13.64	4	6.36	42.15	0
(3)	min	E-feed	4.29	4.46	8.13	38	4.55	17.65	2	5.26	44.87	0
	max	rate	2.83	3.51	7.82	36	3.32	19.43	2	4.44	45.18	0
(4)	min	C-feed	1.05	1.78	12.44	34	1.99	35.80	4	2.07	29.15	12
	max	rate	1.78	2.38	18.83	44	1.93	34.45	8	2.20	28.44	6
(5)	min	Recycle	4.39	5.44	17.12	32	8.73	39.17	2	6.77	28.92	14
	max	flow	9.17	9.90	25.12	40	10.11	42.66	0	10.17	35.44	12
(7)	min	Reactor	8.56	8.2	23.41	34	8.21	39.20	8	8.51	25.93	8
	max	pressure										
(8)	min	Reactor	2.37	2.90	14.57	34	3.31	30.05	2	3.96	44.98	0
	max	level	2.73	3.08	11.13	32	3.40	24.20	0	3.71	37.69	0
(9)	min	Reactor	1.34	1.39	4.06	30	1.45	13.54	8	1.75	45.25	0
	max	temper.	0.65	0.69	3.74	40	0.70	13.56	6	3.71	37.69	0

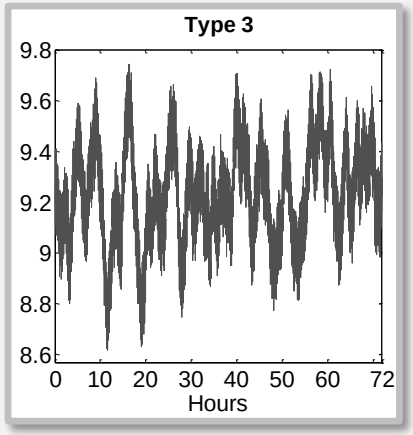
- Unfeasible optimum (attack at best peak)
- Risk assessment based on the sensitivity of control loops
- Secretary problem delivers superior results among approaches

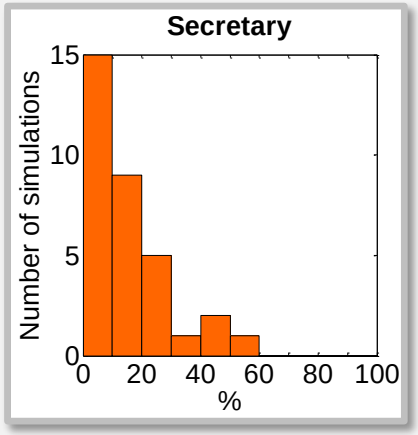
Results: peak detection

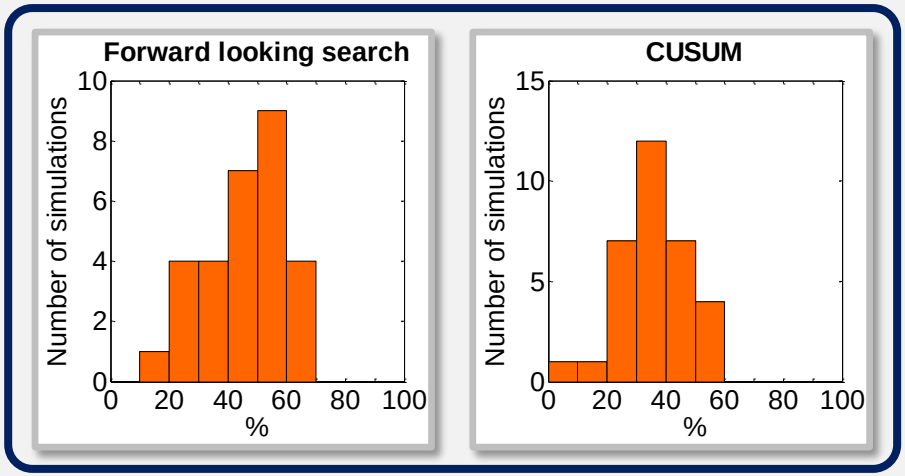








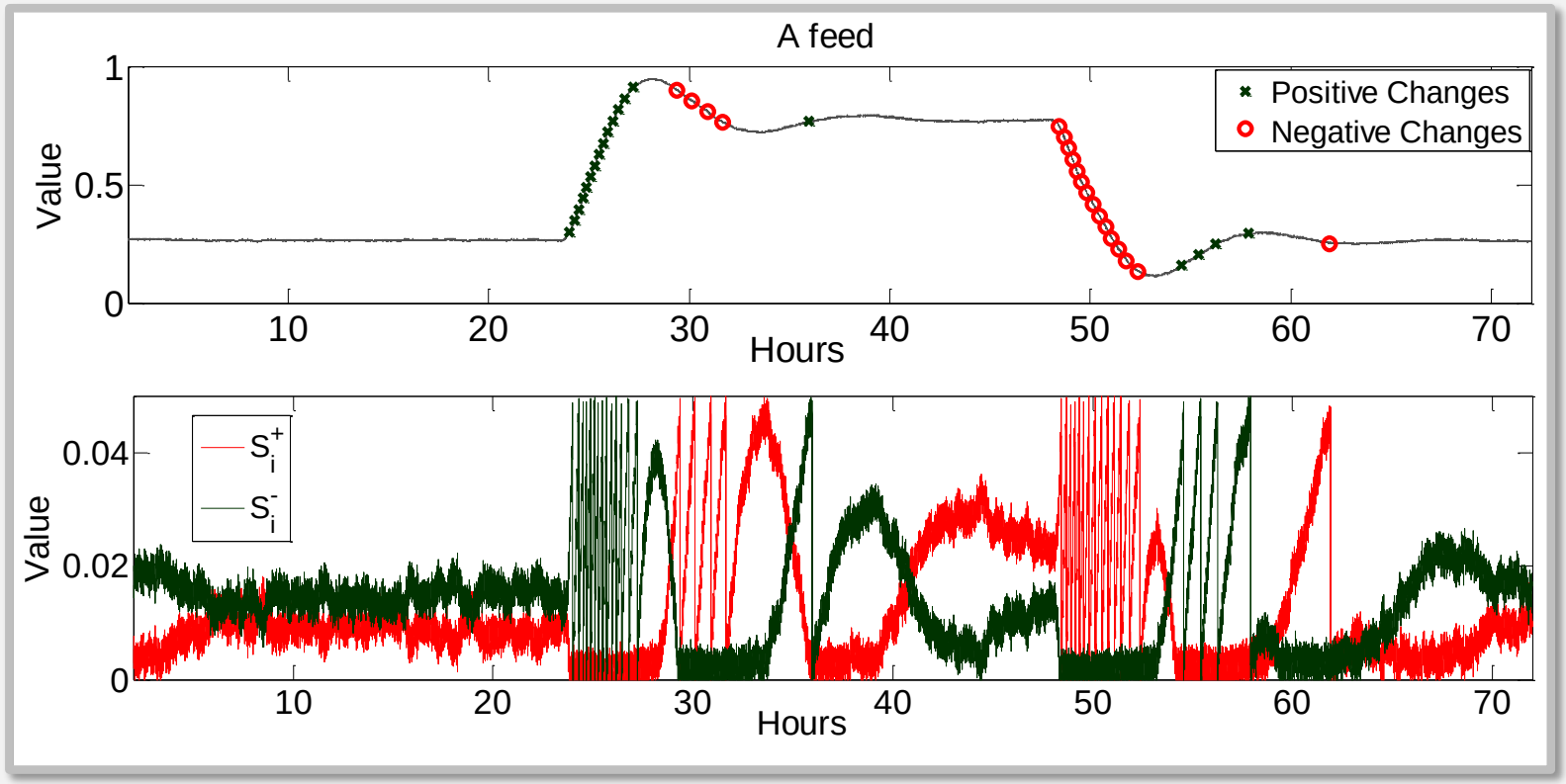




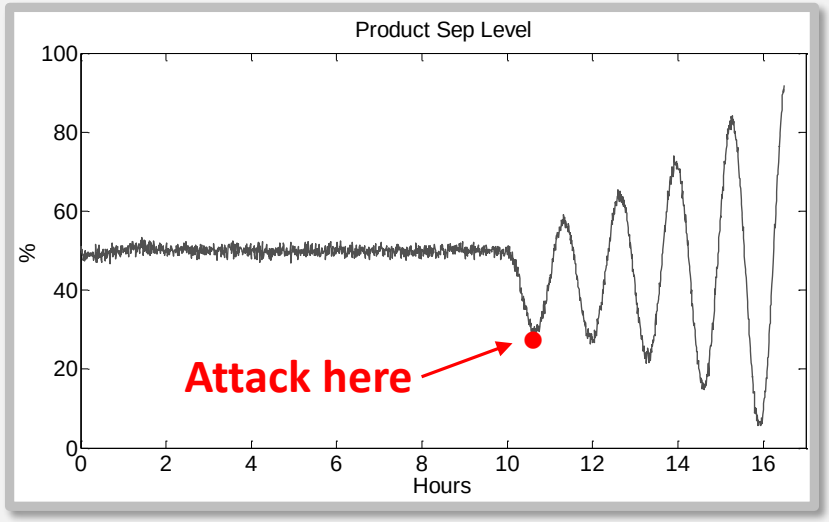
- Motivation
- Best Choice Problem
- Experimental Results
- **Interesting issues**
- Conclusion

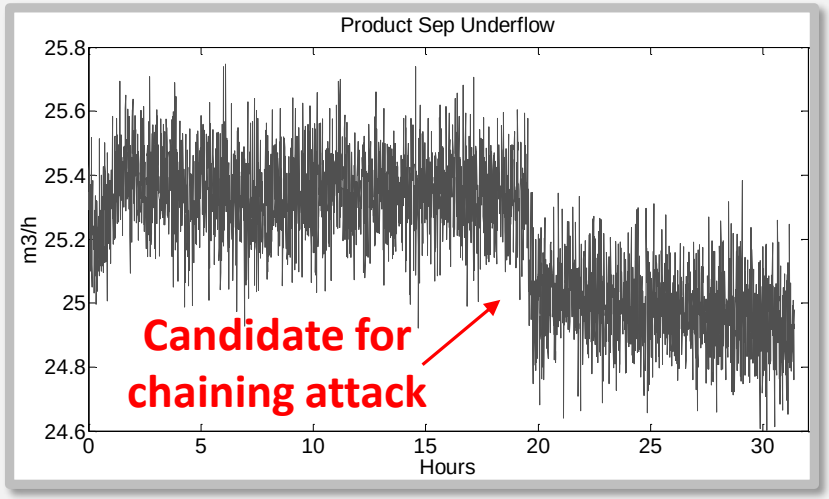
Use case: detection of plant state change

- Step change in the reactant *A* feed
- **Need to "re-learn" aspiration value**
- Use CUSUM algorithm to detect changes in plant state



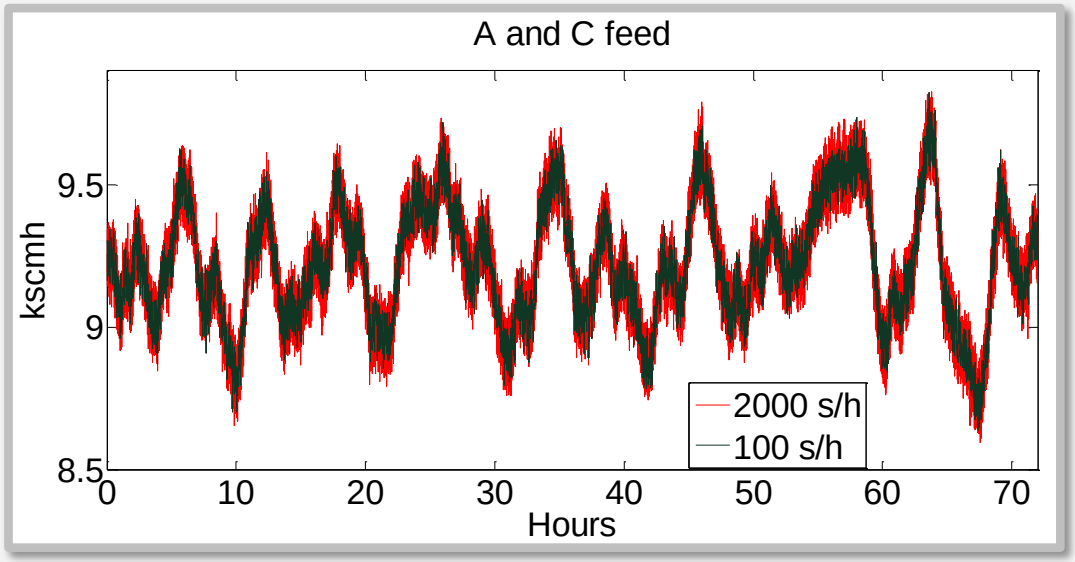
Use case: chaining attacks





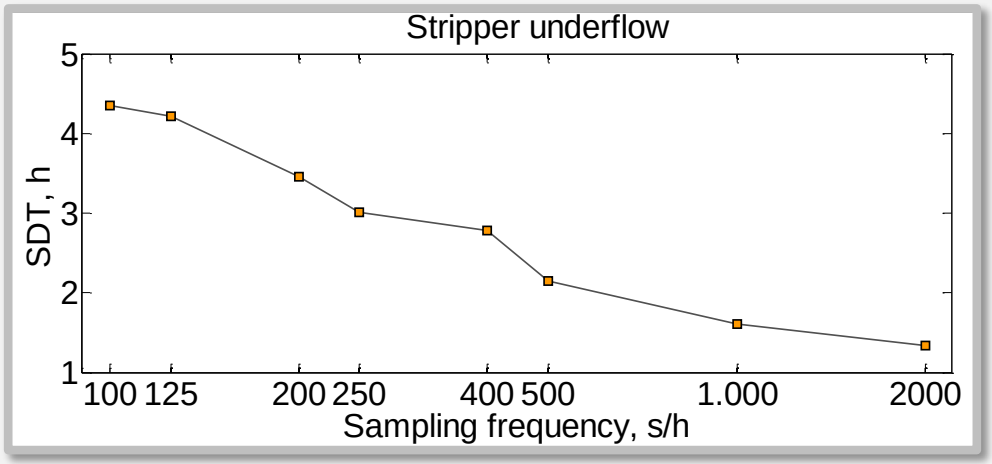
- **Chain two DoS attacks**
- Attack on F_{sep} (flow)
- After 30 min the separator level L_{sep} reaches 30%
- Use CUSUM to detect change
  - SDT in **3.43 h** in comparison to **12.03 h** in case of direct attack

Success parameter: sampling frequency



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

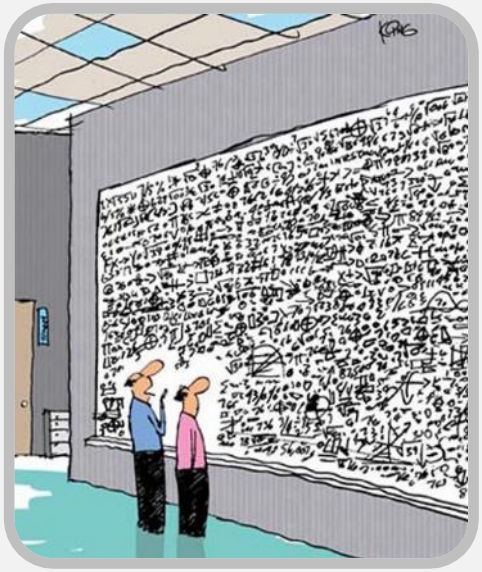
- Important knowledge to attacker to plan concealing activities



- 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