SEC-Two: Secure Estimation Over Two Channels

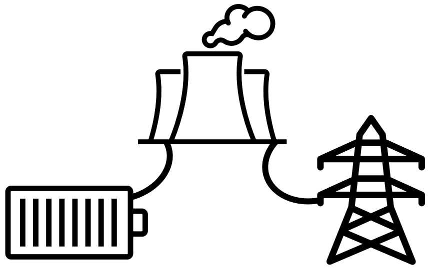
The 2026 American Control Conference

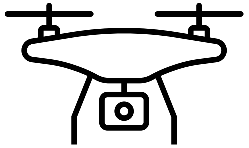
Jacopo Porzio[1], Aris Kanellopoulos[1], Rijad Alisic[2], György Dán[1], Henrik Sandberg[1]

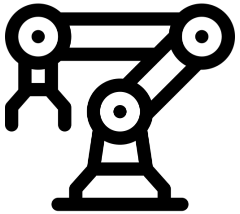
[1]KTH Royal Institute of Technology, Sweden. [2]MIT Massachusetts Institute of Technology, USA.

Motivation

Cyber-physical systems integrate sensing, computation, and control of physical processes.



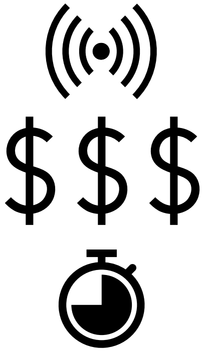




Such systems can combine two types of sensing:

Vulnerable

Low-cost sensors
noisy, high-rate measurements



Often authenticated

High-cost sensors
accurate, *sparse* measurements

Motivation

Vulnerable

Low-cost sensors
noisy, high-rate measurements

High-cost sensors
accurate, *sparse* measurements

Often authenticated

Getting inspiration from works on sensor scheduling:

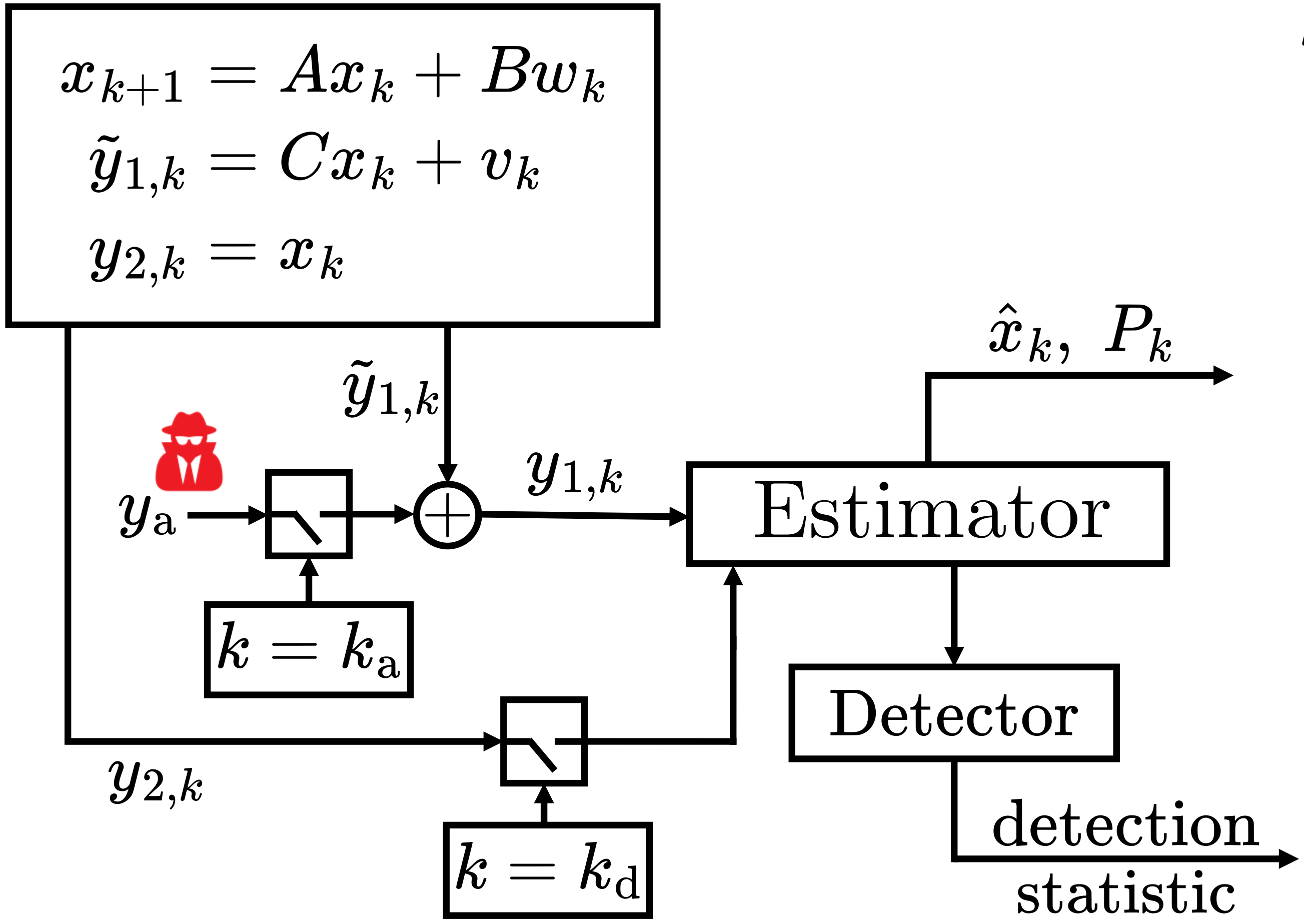
Shi et al., *Sensor data scheduling for optimal state estimation with communication energy constraint* (2011)
Sandberg et al., *Estimation over heterogeneous sensor networks* (2008)
Trimpe et al., *Event-based state estimation with variance-based triggering* (2014)
Leong et al., *Sensor scheduling in variance-based event triggered estimation with packet drops* (2016)

The Plan: Exploit the *sparse* accurate readings to reduce the impact of tampering of the low-cost sensors.

Problem Layout

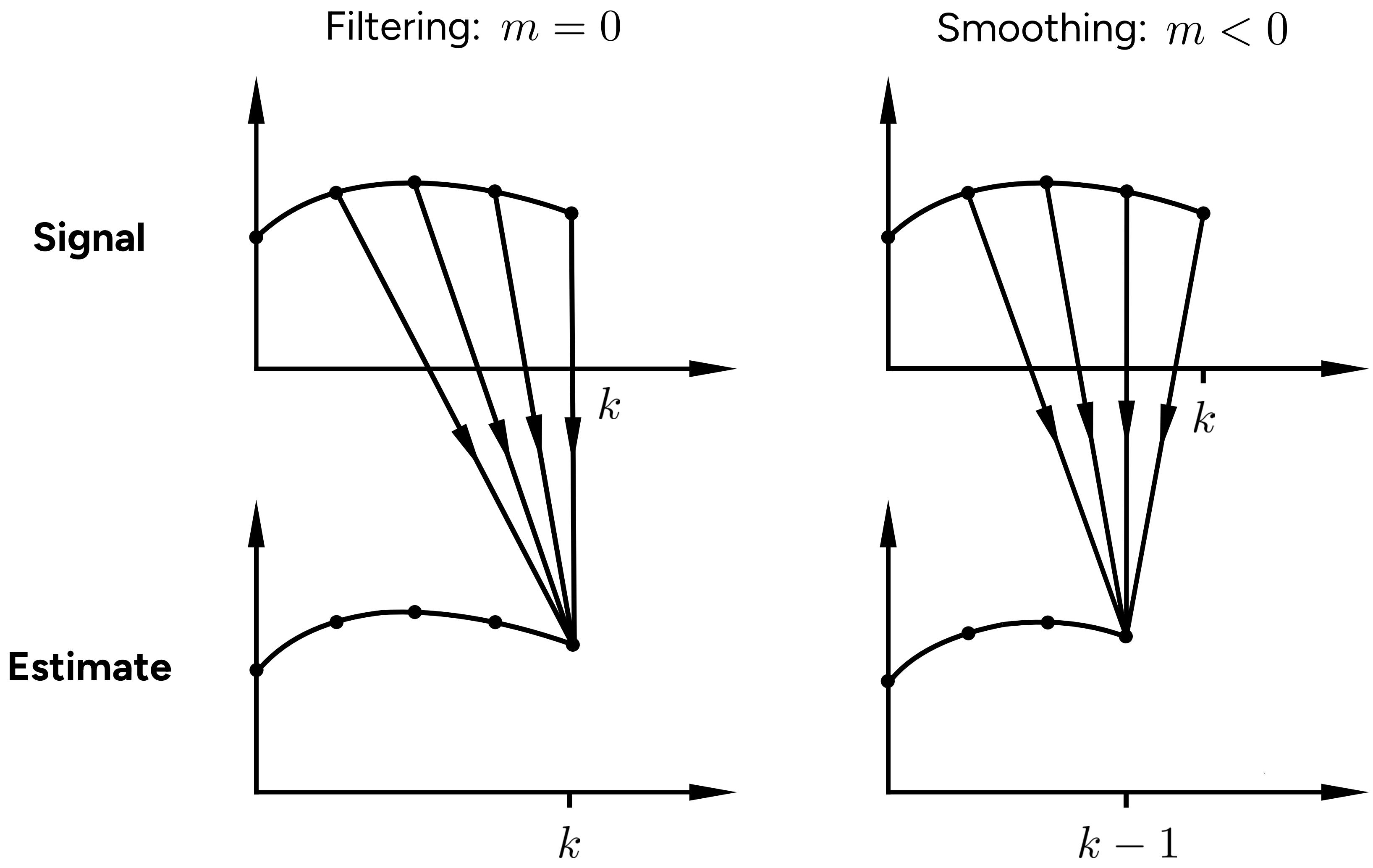
We consider state estimation for a discrete-time **finite-dimensional** linear time-invariant system under **adversarial action**.

$$k \in \{0, 1, \ldots, N\}$$



Filtering and Smoothing — Concepts Review

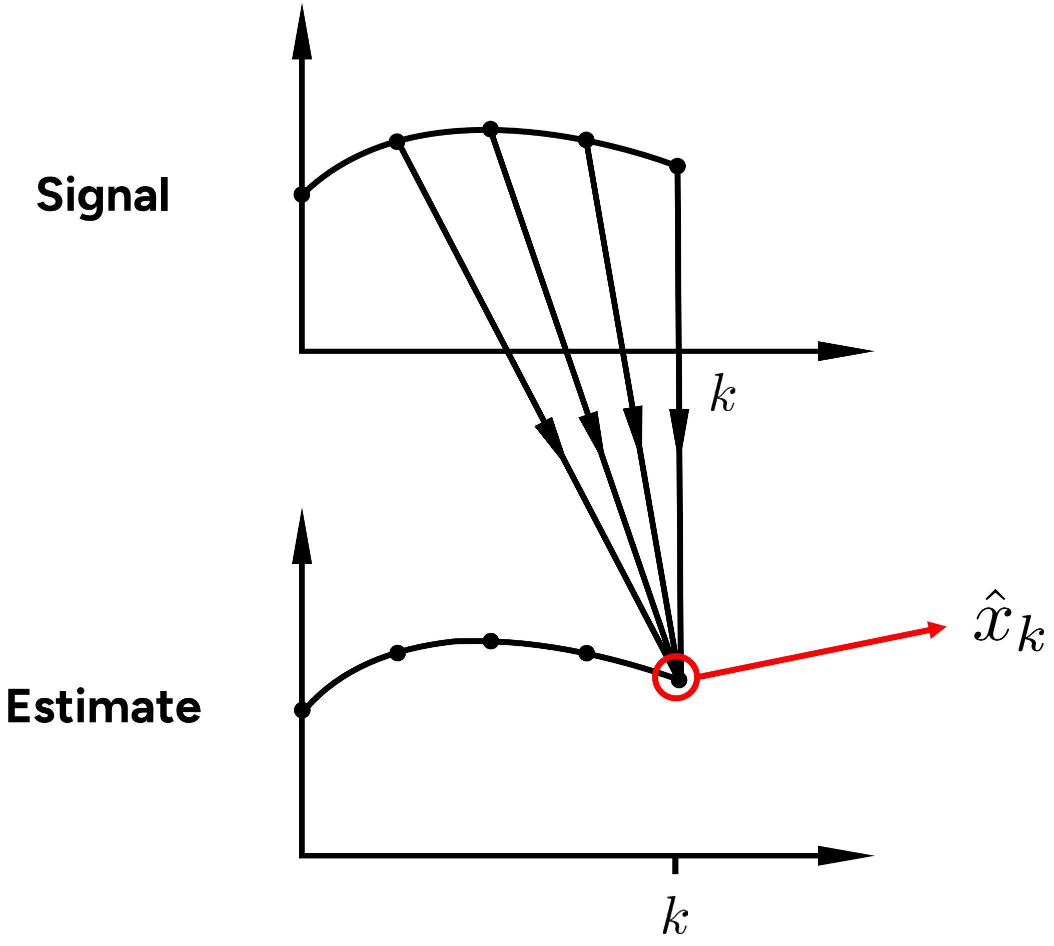
Estimate $x(k+m)$ given $\{y(i) \mid i \leq k\}$.



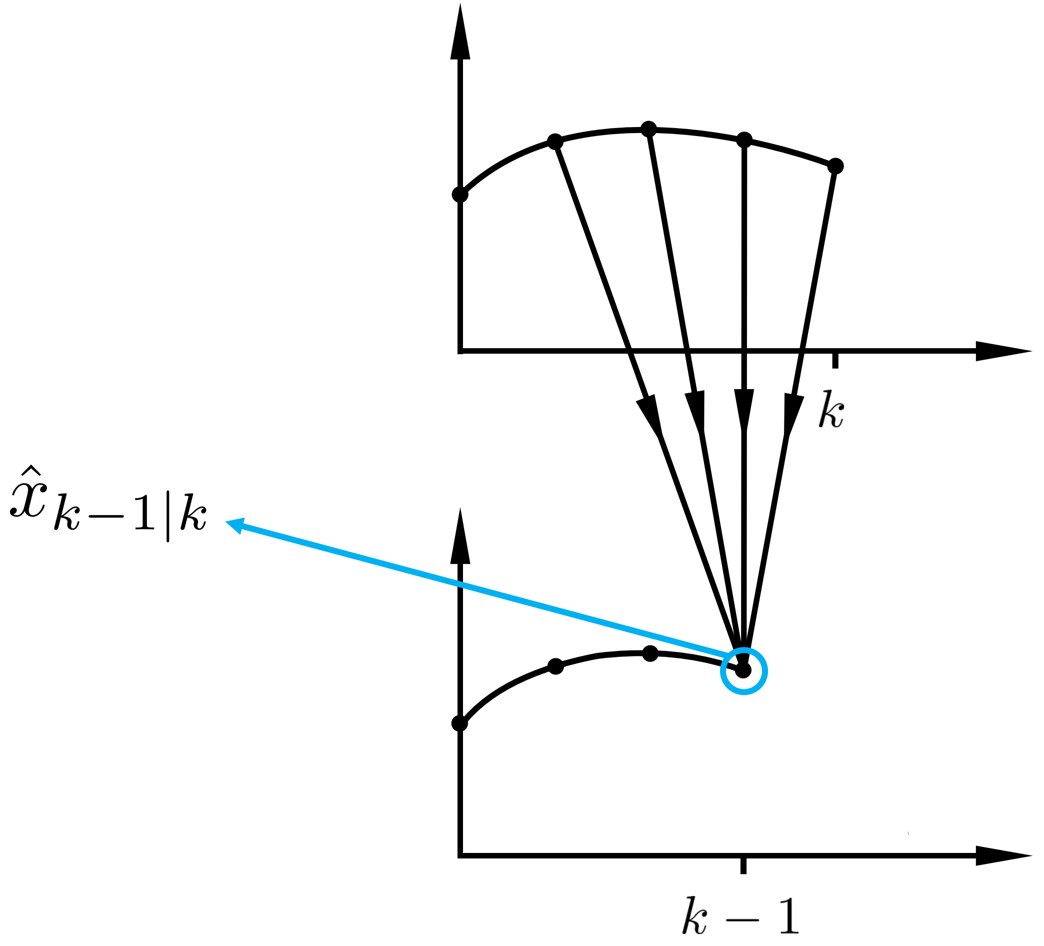
Filtering and Smoothing — Notation

Estimate $x(k+m)$ given $\{y(i) \mid i \leq k\}$.

Filtering: $m = 0$

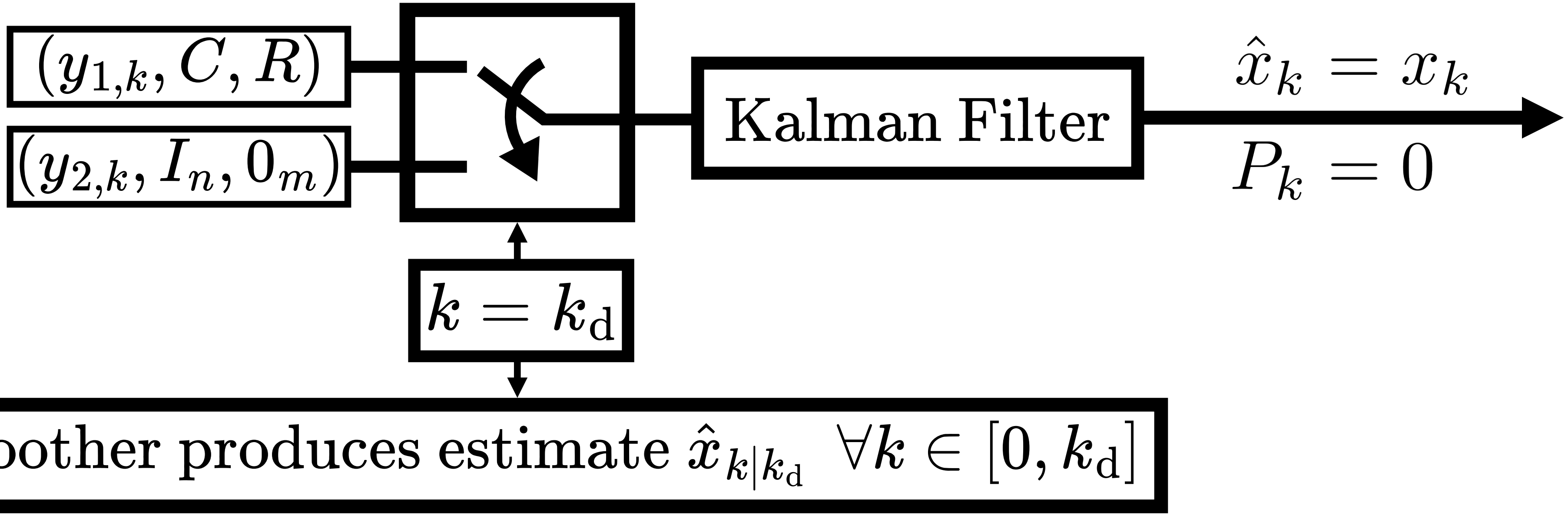


Smoothing: $m < 0$



Use of the Perfect Measurement

When the perfect measurement is received, it replaces the noisy one in the Kalman update and the smoother retrospectively refines the previous estimates.



How the Detector Works — The Principles

At each time step, the detector must decide decide between two hypotheses

$$\begin{aligned} H_0 &: \ \text{no attack} \\ H_1 &: \ \text{the attack has happened} \end{aligned}$$

according to a decision rule: if $g_k \geq \eta$, it rejects H_0 in favor of H_1.

Different statistics g_k are calculated based on *different inputs* depending on k:

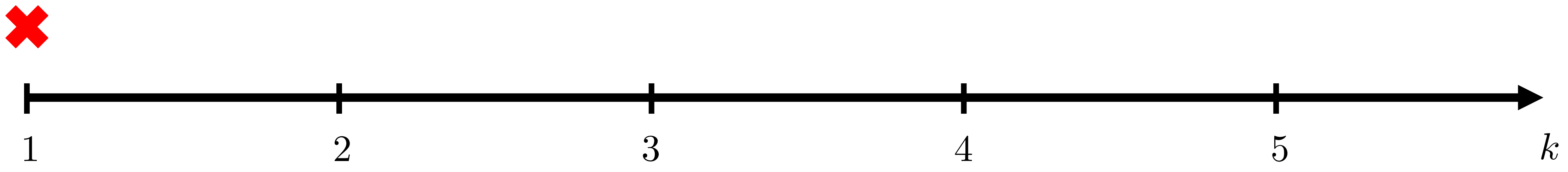
Innovation (residual)	*Both measurements*	*Smoothed innovation*
$z_k := y_{1,k} - C\hat{x}_k^-$	$y_{1,k},\, y_{2,k}$	$z_{k\vert k_\mathrm{d}} := y_{1,k} - C\hat{x}_{k\vert k_\mathrm{d}}$
P_{z_k}	R	$P_{z_{k\vert k_\mathrm{d}}}$

How the Detector Works — An Intuition

Real time: $k = 1$

$z_k^\top P_{z_k}^{-1} z_k \geq \eta?$

Online



On χ^2-square testing for security:
Mo and Sinopoli, *On the performance degradation of cyber-physical systems under stealthy integrity attacks* (2015)
Murguia and Ruths, *CUSUM and Chi-squared Attack Detection of Compromised Sensors* (2016)
...

How the Detector Works — An Intuition

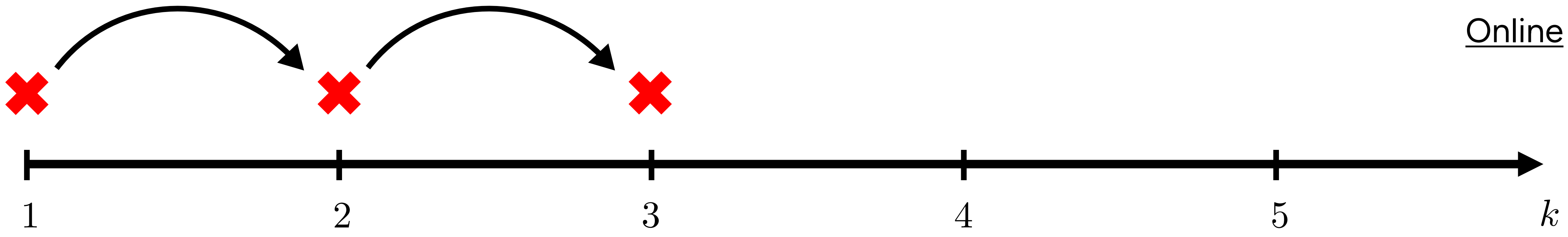
Real time: $k = 2$

✖ $z_k^\top P_{z_k}^{-1} z_k \geq \eta$?

How the Detector Works — An Intuition

Real time: $k = 3$

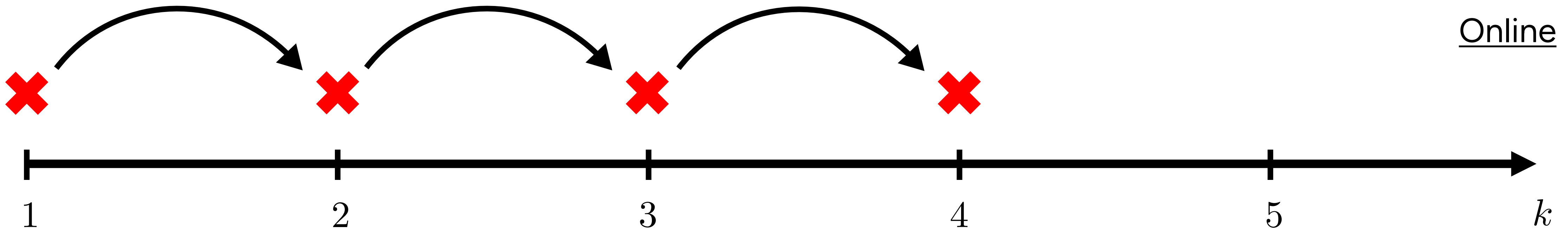
$z_k^\top P_{z_k}^{-1} z_k \geq \eta$?



How the Detector Works — An Intuition

Real time: $k = 4$

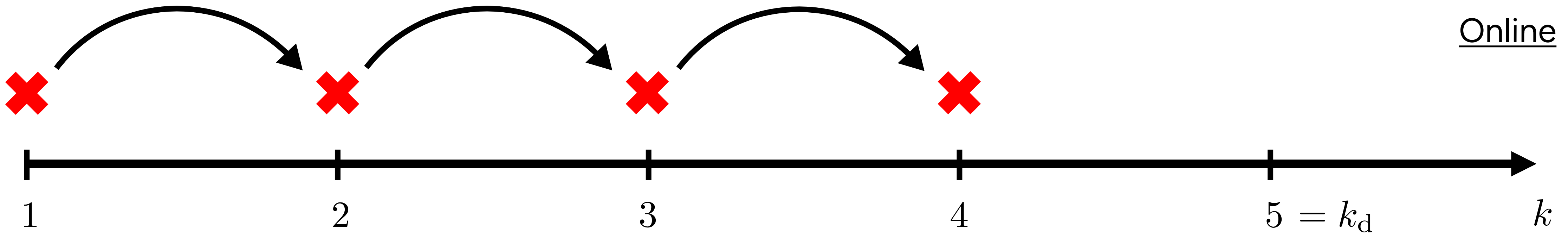
$z_k^\top P_{z_k}^{-1} z_k \geq \eta?$



How the Detector Works — An Intuition

Real time: $k = 5$

✖ $z_k^\top P_{z_k}^{-1} z_k \geq \eta?$

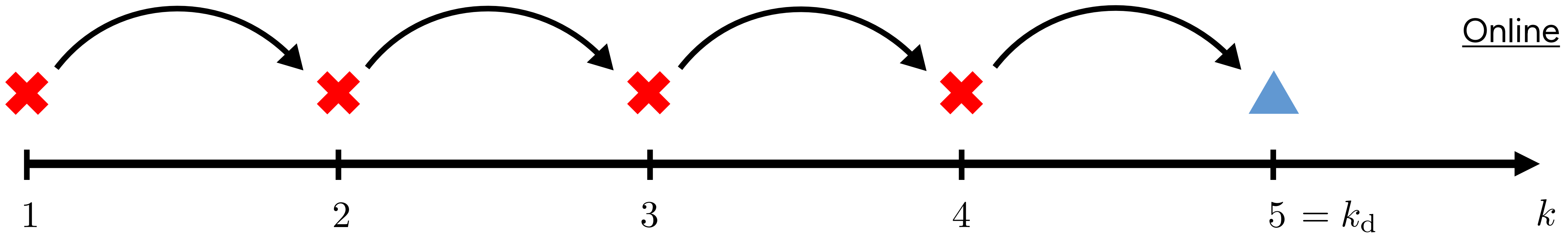


How the Detector Works — An Intuition

Real time: $k = 5$

$z_k^\top P_{z_k}^{-1} z_k \geq \eta?$

$(y_{1,k} - C y_{2,k})^\top R^{-1} (y_{1,k} - C y_{2,k}) \geq \eta?$



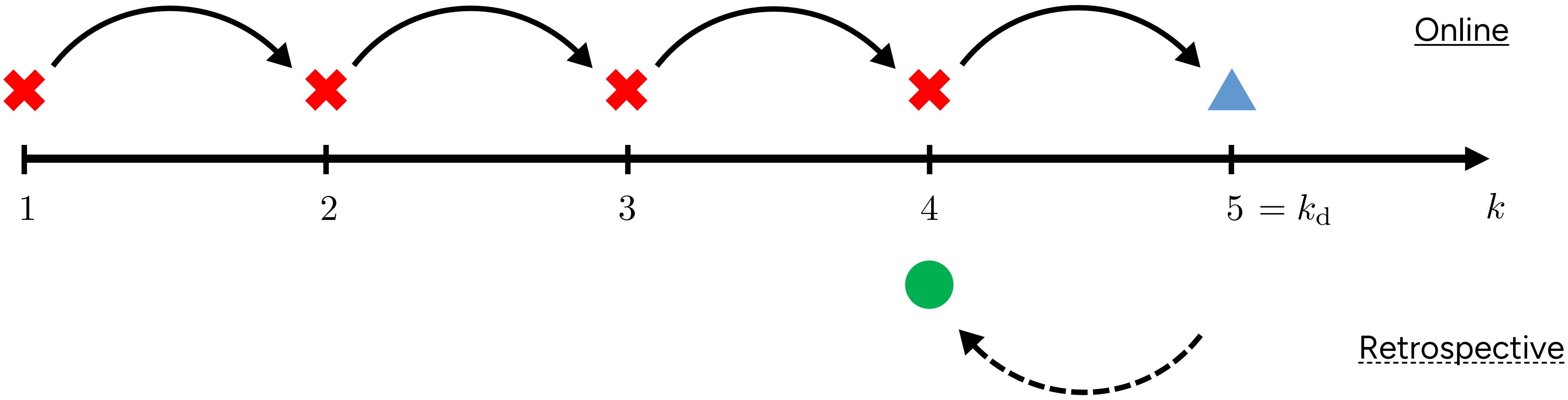
How the Detector Works — An Intuition

Real time: $k = 5$

$z_k^\top P_{z_k}^{-1} z_k \geq \eta?$

$(y_{1,k} - Cy_{2,k})^\top R^{-1} (y_{1,k} - Cy_{2,k}) \geq \eta?$

$z_{k|k_\mathrm{d}}^\top P_{z_{k|k_\mathrm{d}}}^{-1} z_{k|k_\mathrm{d}} \geq \eta?$



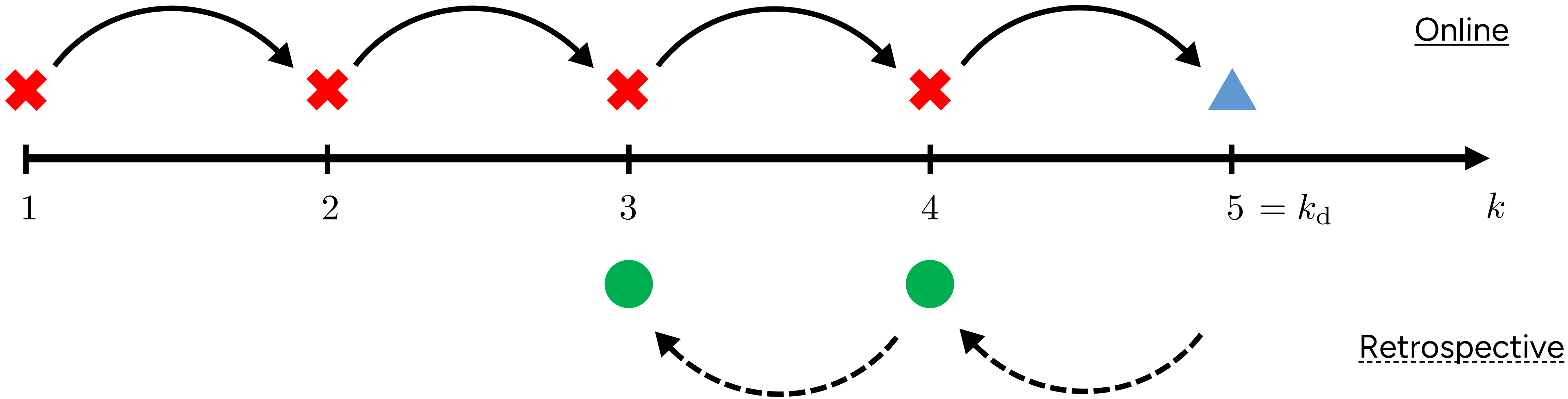
How the Detector Works — An Intuition

Real time: $k = 5$

$z_k^\top P_{z_k}^{-1} z_k \geq \eta?$

$(y_{1,k} - Cy_{2,k})^\top R^{-1}(y_{1,k} - Cy_{2,k}) \geq \eta?$

$z_{k|k_\mathrm{d}}^\top P_{z_{k|k_\mathrm{d}}}^{-1} z_{k|k_\mathrm{d}} \geq \eta?$



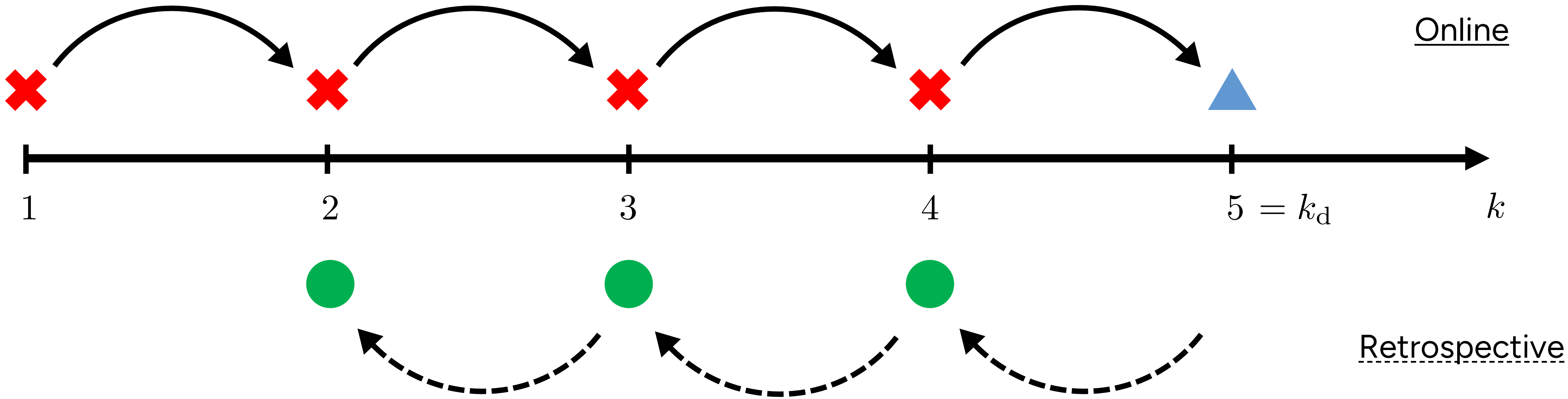
How the Detector Works — An Intuition

Real time: $k = 5$

$z_k^\top P_{z_k}^{-1} z_k \geq \eta?$

$(y_{1,k} - C y_{2,k})^\top R^{-1} (y_{1,k} - C y_{2,k}) \geq \eta?$

$z_{k|k_\mathrm{d}}^\top P_{z_{k|k_\mathrm{d}}}^{-1} z_{k|k_\mathrm{d}} \geq \eta?$



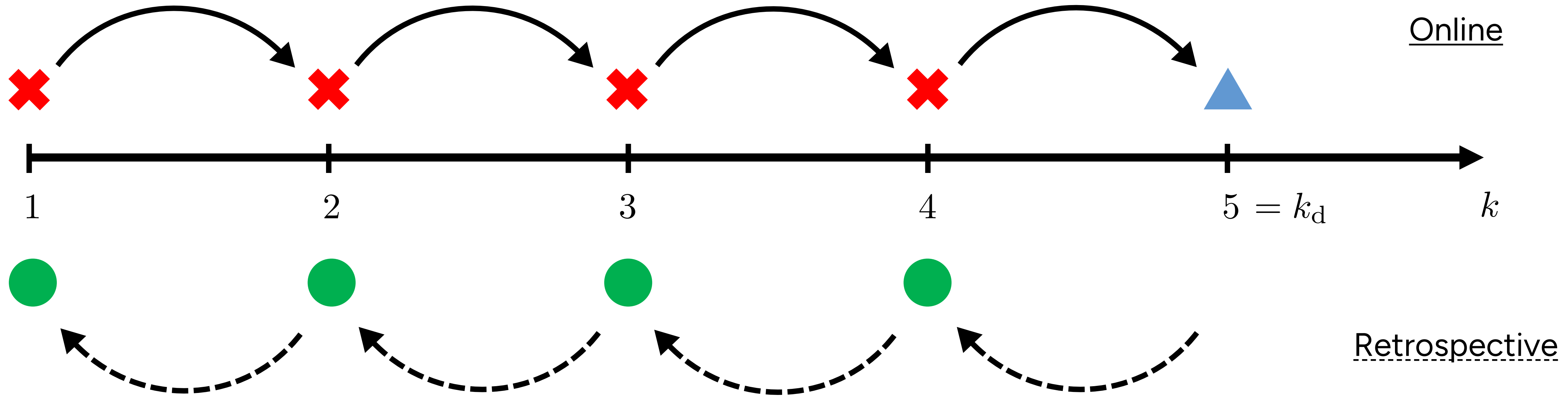
How the Detector Works — An Intuition

Real time: $k = 5$

$$z_k^\top P_{z_k}^{-1} z_k \geq \eta?$$

$$(y_{1,k} - C y_{2,k})^\top R^{-1} (y_{1,k} - C y_{2,k}) \geq \eta?$$

$$z_{k|k_\mathrm{d}}^\top P_{z_{k|k_\mathrm{d}}}^{-1} z_{k|k_\mathrm{d}} \geq \eta?$$



Attack Impact

We define the impact $\mathcal{E}_k$ of the attack through the Mean Squared Error (MSE):

$$\mathrm{MSE}_k = \mathbb{E}\left[\left(x_k - \hat{x}_k^{H_1}\right)^\top \left(x_k - \hat{x}_k^{H_1}\right)\right] = \mathrm{Tr}(P_k) + \mathcal{E}_k.$$

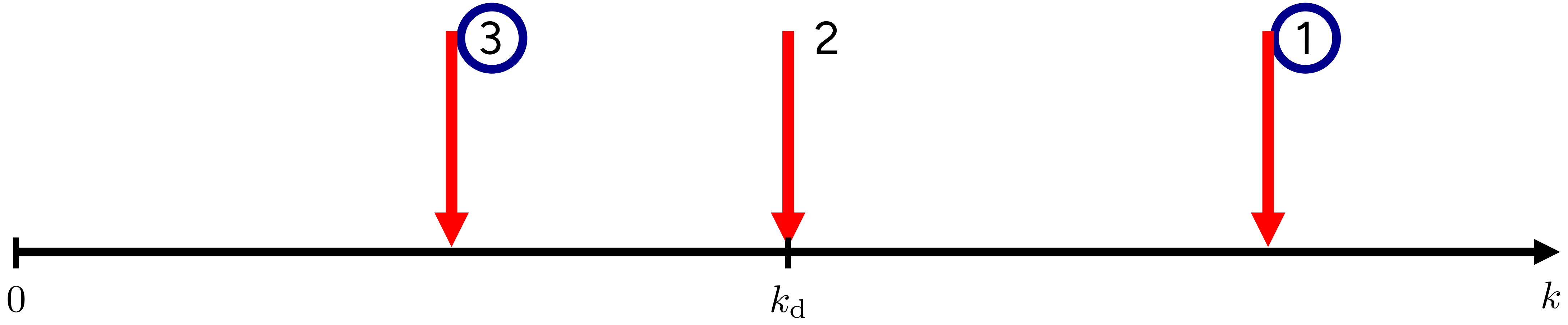
Posterior state estimation error covariance from KF

It depends on the Kalman gain at k_a, the attack amplitude y_a and the KF dynamics

Results

In the paper we analyze how the perfect measurement affects attack impact and detectability for three different scenarios:

1. $k_{\mathrm{a}} > k_{\mathrm{d}}$ (attack after);
2. $k_{\mathrm{a}} = k_{\mathrm{d}}$ (attack simultaneous);
3. $k_{\mathrm{a}} < k_{\mathrm{d}}$ (attack before).



Perfect measurement time

Attack *Following* the Perfect Measurement Change on Impact and Detectability

Considering an attack of magnitude y_{a} happening at $k_{\mathrm{a}} > k_{\mathrm{d}}$ and a *nominal process* using only noisy measurements, we prove that:

Theorem 1 (scalar case)

$$\mathcal{E}_{k_{\mathrm{a}}} \leq \mathcal{E}_{k_{\mathrm{a}},\mathrm{nom}} \; \forall k_{\mathrm{a}} > k_{\mathrm{d}}$$

Theorem 2 (vector case)

$$g_k := z_k^\top P_{z_k}^{-1} z_k$$

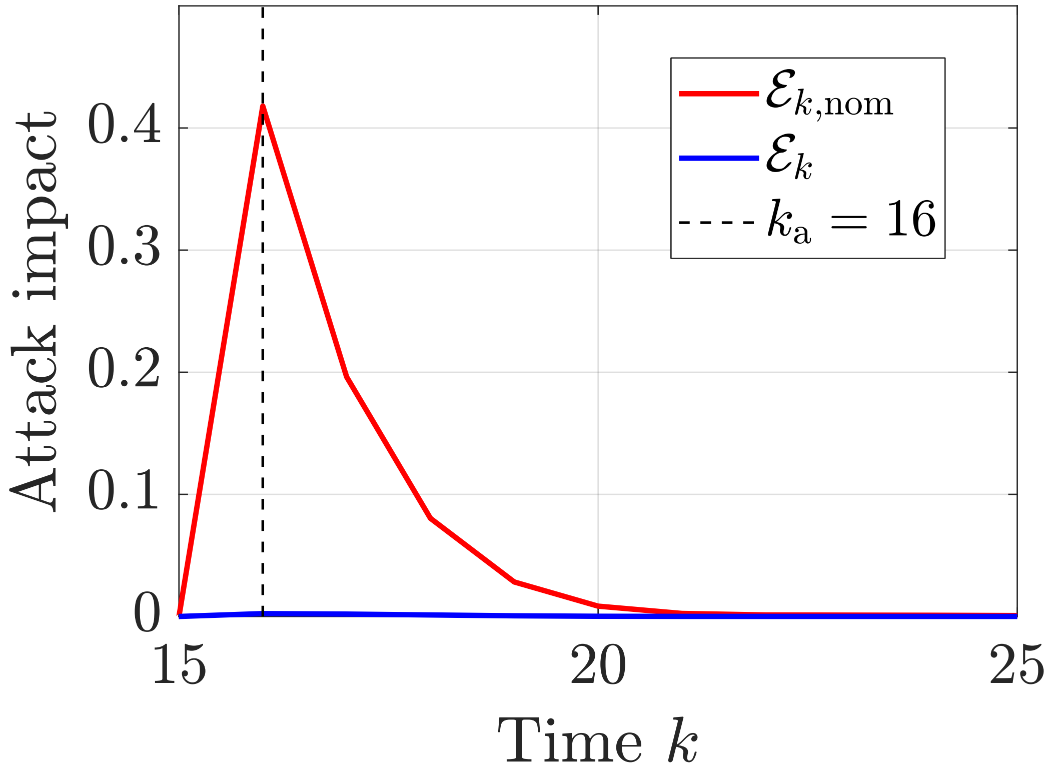
$$\mathbb{P}\left(g_{k_{\mathrm{a}}} \geq \eta \mid H_1\right) \geq \mathbb{P}\left(g_{k_{\mathrm{a}},\mathrm{nom}} \geq \eta \mid H_1\right) \; \forall k_{\mathrm{a}} > k_{\mathrm{d}}$$

The perfect measurement makes the attack less impactful while making it easier to detect it.

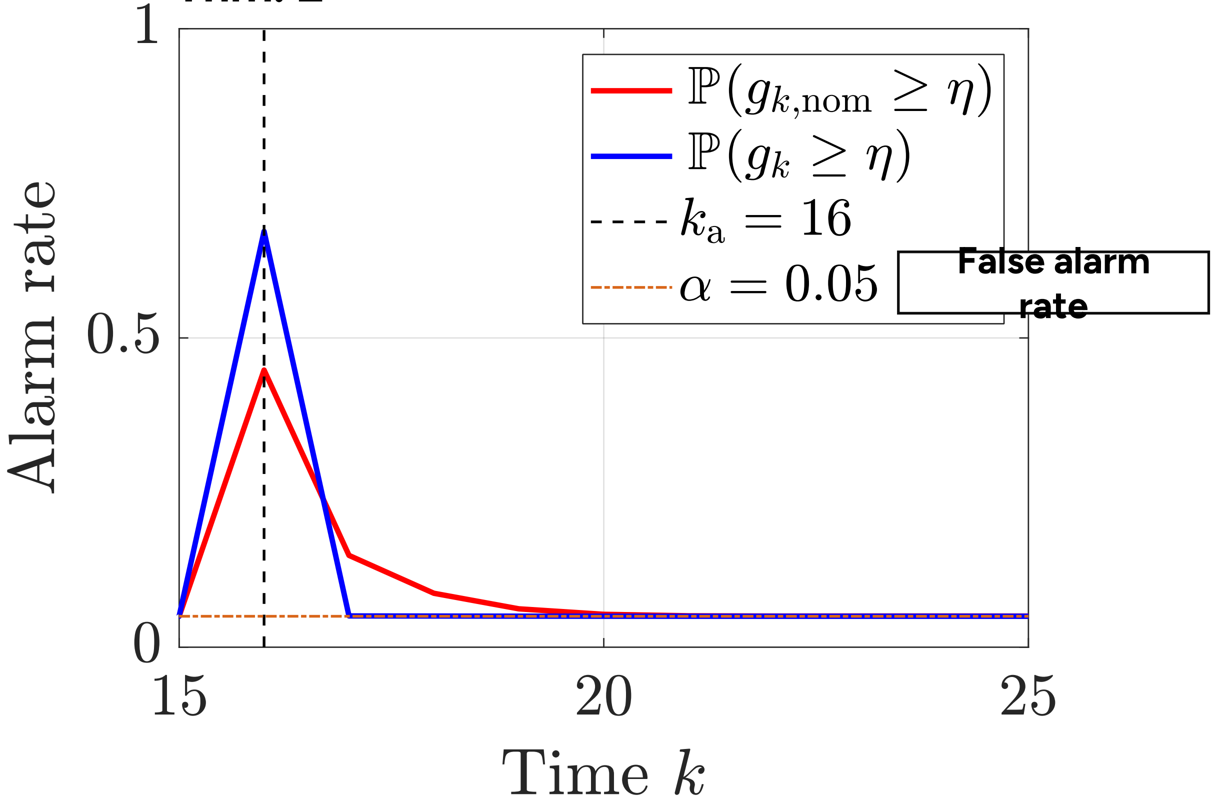
Attack *Following* the Perfect Measurement Change on Impact and Detectability — MD Example

Attack at $k_{\mathrm{a}} = 16$.
Perfect measurement at $k_{\mathrm{d}} = 15$.

Thm. 1



Thm. 2



$$N = 25,\ A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix},\ B = I_n,\ C = I_n,\ Q = 0.01 I_n,\ R = 0.3 I_m,\ y_{\mathrm{a}} = \begin{bmatrix} 0 \\ 1.5 \end{bmatrix},\ \eta \approx 6.$$

Attack *Preceding* Perfect Measurement Change on Detectability

Considering an attack of magnitude y_a happening at $k_\mathrm{a} < k_\mathrm{d}$ and comparing the unsmoothed detection statistic

$$g_k := z_k^\top P_{z_k}^{-1} z_k$$

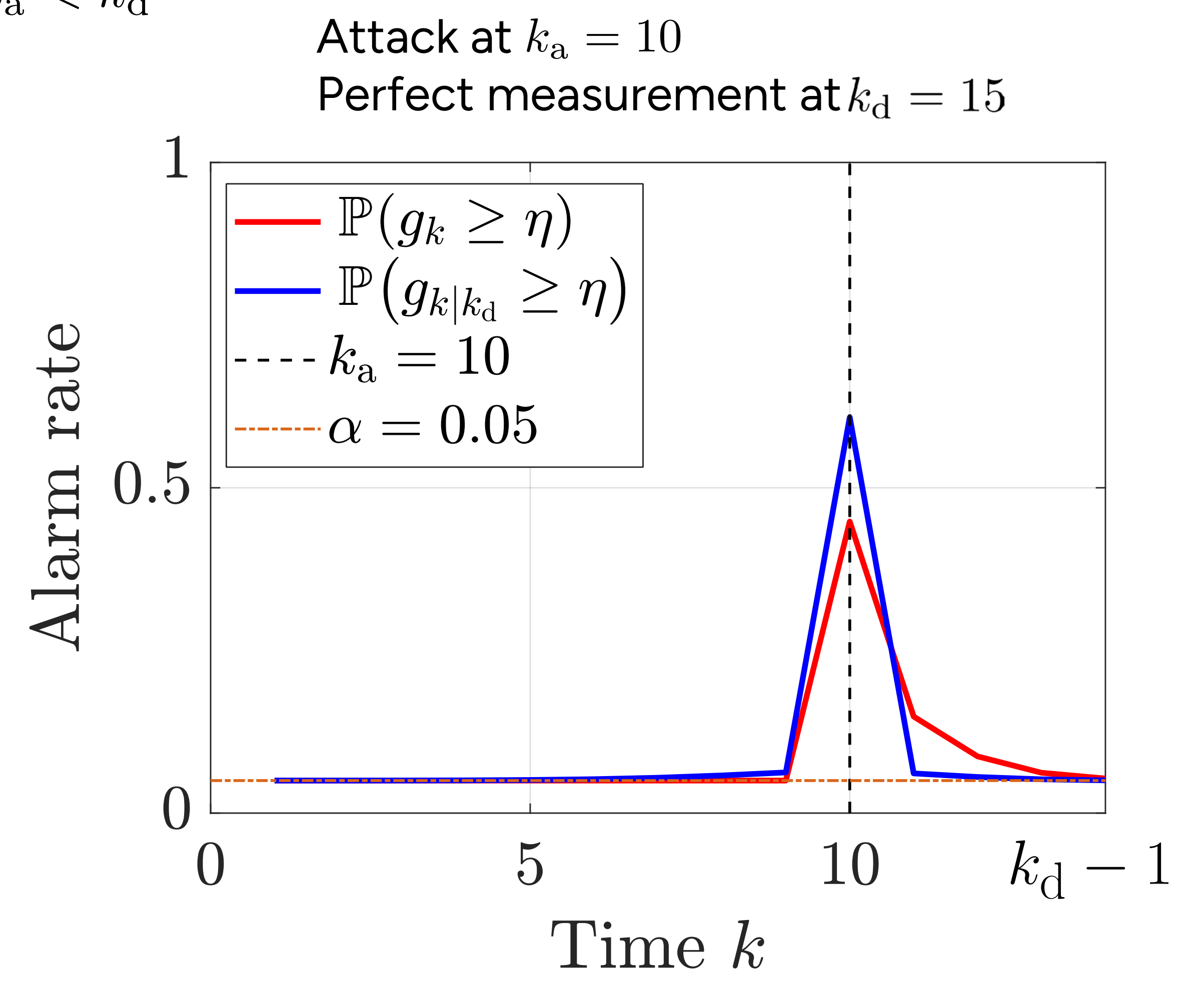
and the smoothed detection statistic

$$g_{k|k_\mathrm{d}} := z_{k|k_\mathrm{d}}^\top P_{z_{k|k_\mathrm{d}}}^{-1} z_{k|k_\mathrm{d}}$$

we proved that:

Theorem 3 (scalar case)

$$\begin{aligned}
&\mathbb{P}\left(g_{k|k_\mathrm{d}} \geq \eta \mid H_1\right) > \mathbb{P}\left(g_k \geq \eta \mid H_1\right) \quad \text{for } k < k_\mathrm{a}\\
&\mathbb{P}\left(g_{k|k_\mathrm{d}} \geq \eta \mid H_1\right) > \mathbb{P}\left(g_k \geq \eta \mid H_1\right) \quad \text{for } k = k_\mathrm{a}\\
&\mathbb{P}\left(g_{k|k_\mathrm{d}} \geq \eta \mid H_1\right) < \mathbb{P}\left(g_k \geq \eta \mid H_1\right) \quad \text{for } k > k_\mathrm{a}
\end{aligned}$$



$N = 25,\ A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix},\ B = I_n,\ C = I_n,\ Q = 0.01 I_n,\ R = 0.3 I_m,\ y_\mathrm{a} = \begin{bmatrix} 0 \\ 1.5 \end{bmatrix},\ \eta \approx 6.$

Summary

Contributions:

- new two-channel attack detector with *optimal smoothing* (*“retrospective”*) *capability*;
- value of sparse authenticated sensing in dynamical systems.

Additional results (in the paper):

- monotonic trends in impact and detectability;
- detection at perfect measurement time;
- different smoothing behavior with VS without perfect measurement.

Next steps:

- proofs in multi-dimensional case (simulations promising);
- multiple perfect measurements and attacks;
- game-theoretic analysis;
- hardware in-the-loop.

Thanks for listening!

Jacopo Porzio
porzio@kth.se

Decision and Control System
KTH Royal Institute of Technology
Stockholm, Sweden

https://www.kth.se/profile/porzio

Appendix

More on the Impact

$$\mathcal{E}_k = {y_\mathrm{a}}^\top \Delta(k, k_\mathrm{a})^\top \Delta(k, k_\mathrm{a}) y_\mathrm{a} \tag{1}$$

$$\Delta(k, k_\mathrm{a}) = \Big(\widetilde{\prod_{i=k}^{k_\mathrm{a}+1}} \big(I_n - K_i C_i\big) A \Big) K_{k_\mathrm{a}} \tag{2}$$

$$\widetilde{\prod_{i=m}^{j}} \mathcal{Z}_i = \begin{cases} \mathcal{Z}_m \mathcal{Z}_{m-1} \cdots \mathcal{Z}_{j+1} \mathcal{Z}_j, & m > j \\ \mathcal{Z}_j, & m = j \\ 1, & m = j-1 \\ 0, & m \leq j-2. \end{cases} \tag{3}$$

Attack *Following* the Perfect Measurement Monotonic Trends in Impact and Detectability

Considering an attack of magnitude y_a happening at $k_\mathrm{a} > k_\mathrm{d}$, we prove that:

Proposition 1 (scalar case)

$\mathcal{E}_{k_\mathrm{a}}$ is non-decreasing in k_a $(k_\mathrm{a} > k_\mathrm{d})$ and upper-bounded.

Proposition 2

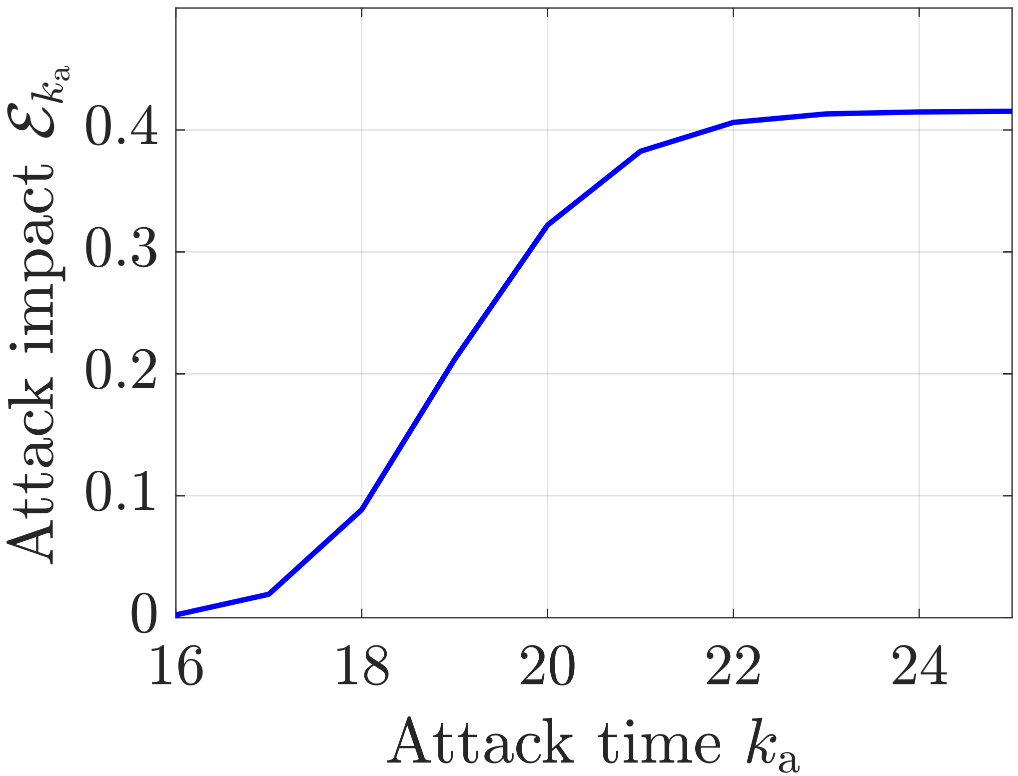
$\mathbb{P}\left(g_{k_\mathrm{a}} \geq \eta \mid H_1\right)$ is non-increasing in k_a $(k_\mathrm{a} > k_\mathrm{d})$ and lower-bounded.

The farther from the perfect measurement, the greater the impact and the lower the detectability.

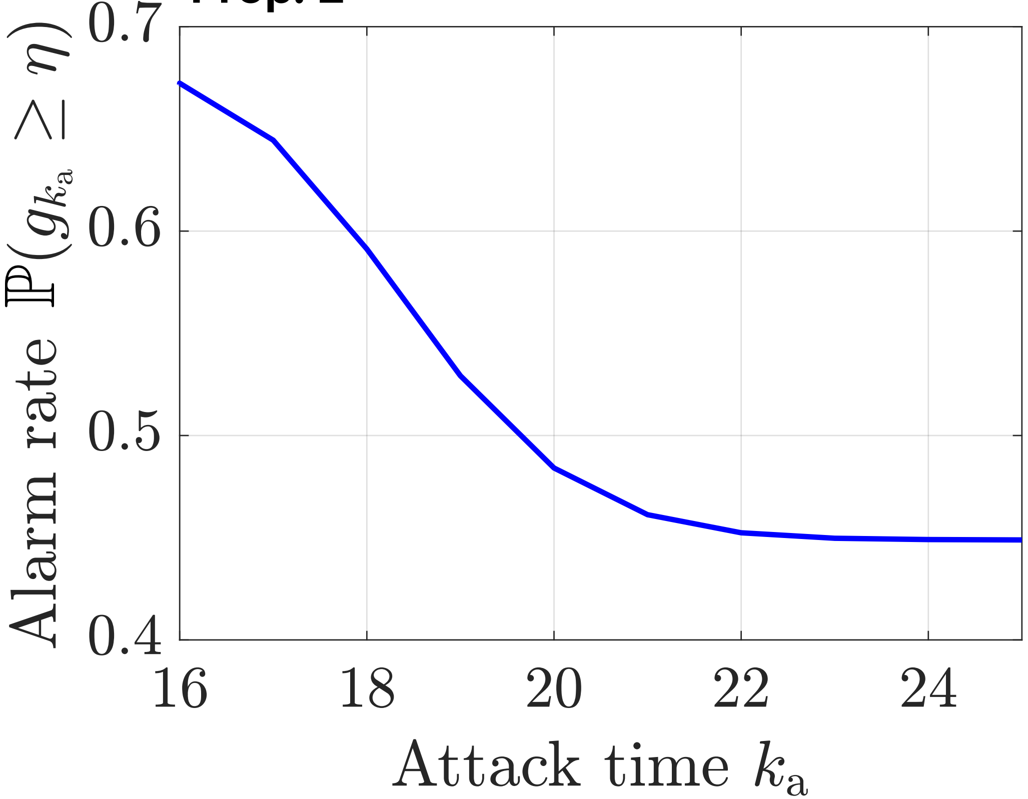
Attack *Following* the Perfect Measurement: Monotonic Trends in Impact and Detectability — Example

Perfect measurement at $k_\mathrm{d} = 15$.

Prop. 1



Prop. 2



$$N = 25,\ A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix},\ B = I_n,\ C = I_n,\ Q = 0.01 I_n,\ R = 0.3 I_m,\ y_\mathrm{a} = \begin{bmatrix} 0 \\ 1.5 \end{bmatrix},\ \eta \approx 6.$$

The Case for Smoothing is not Trivial

Which is larger between $g_k = z_k^\top P_{z_k}^{-1} z_k$ and $g_{k|k_\mathrm{d}} = z_{k|k_\mathrm{d}}^\top P_{z_{k|k_\mathrm{d}}}^{-1} z_{k|k_\mathrm{d}}$?

Smoothing removes unmodeled outliers such as the attack. Hence, it holds on average that

$$\begin{gathered}\|z_{k_\mathrm{a}}\| = \|C(x_{k_\mathrm{a}} - \hat{x}_{k_\mathrm{a}|k_\mathrm{a}-1}) + v_k + y_\mathrm{a}\| \\ \vee \\ \|z_{k_\mathrm{a}|k_\mathrm{d}}\| = \|C(x_{k_\mathrm{a}} - \hat{x}_{k_\mathrm{a}|k_\mathrm{d}}) + v_k + |\Delta| y_\mathrm{a}\|, \quad |\Delta| < 1.\end{gathered}$$

For the same reason, smoothing reduces uncertainty:

$$P_{z_k} \succ P_{z_{k|k_\mathrm{d}}} \iff P_{z_k}^{-1} \prec P_{z_{k|k_\mathrm{d}}}^{-1}$$

Therefore, it is not easy to conclude whether

$$g_k \lessgtr g_{k|k_\mathrm{d}}.$$

Attack *Preceding* Perfect Measurement Smoothing: Perfect vs Noisy

Two smoothing setups:

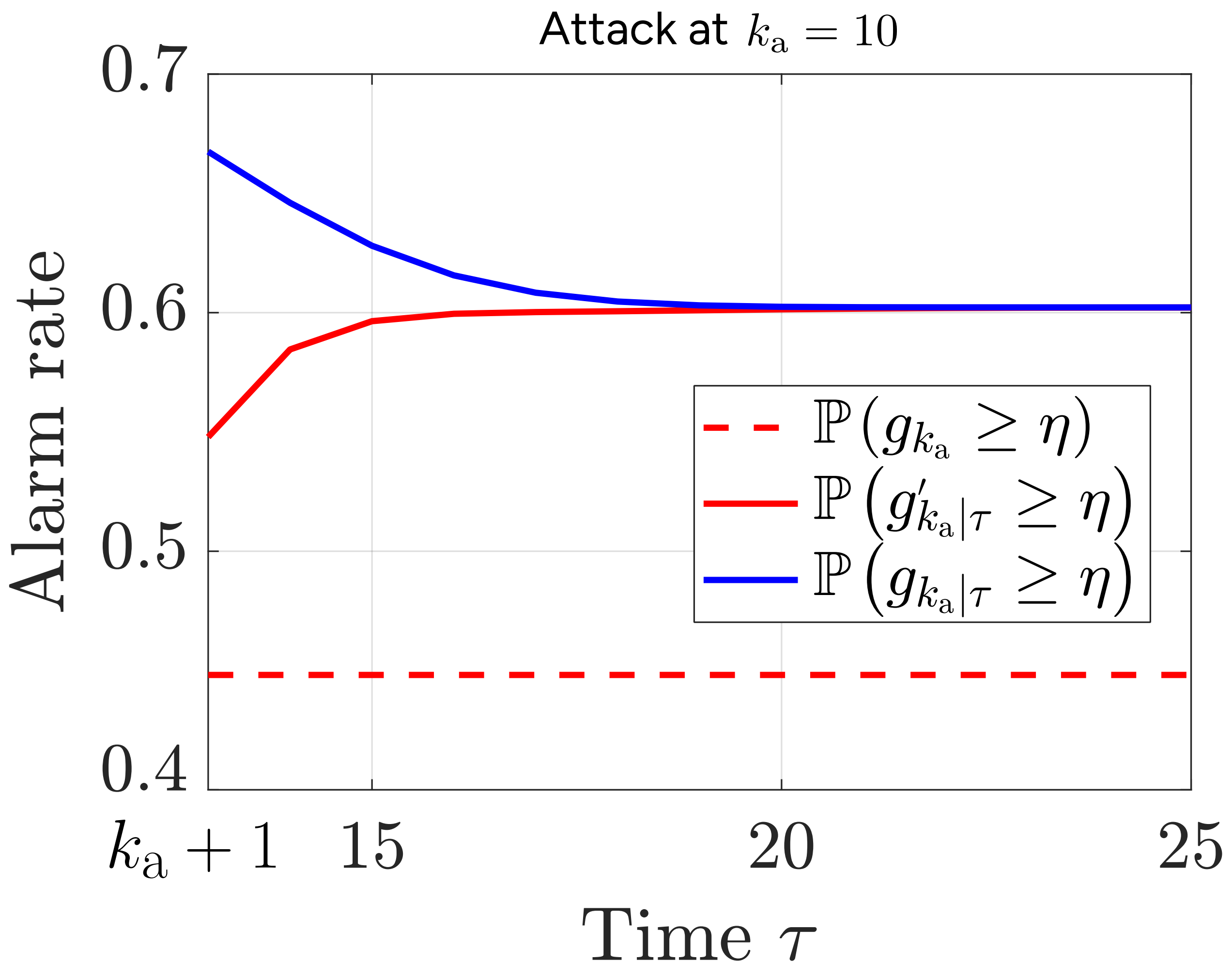
i. perfect measurement at time τ $(g_{k|\tau})$;

ii. noisy measurement at time τ $(g'_{k|\tau})$.

We proved in scalar case that:

Proposition 4

$$\begin{array}{ccc} \mathbb{P}\left(g_{k_{\mathrm{a}}|\tau+1} \geq \eta \mid H_1\right) & < & \mathbb{P}\left(g_{k_{\mathrm{a}}|\tau} \geq \eta \mid H_1\right) \\ \vee & & \vee \\ \mathbb{P}\left(g'_{k_{\mathrm{a}}|\tau+1} \geq \eta \mid H_1\right) & > & \mathbb{P}\left(g'_{k_{\mathrm{a}}|\tau} \geq \eta \mid H_1\right) \end{array}$$



$$N = 25,\ A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix},\ B = I_n,\ C = I_n,\ Q = 0.01 I_n,\ R = 0.3 I_m,\ y_{\mathrm{a}} = \begin{bmatrix} 0 \\ 1.5 \end{bmatrix},\ \eta \approx 6.$$